

Mastering Microsoft 365



Eleventh Edition (2025)

Office 365 for IT Pros

The Ultimate Guide to Planning, Deploying, and Managing the Microsoft 365 Cloud Productivity Ecosystem covering:

Teams, Exchange Online, SharePoint Online

OneDrive for Business, Entra ID, Planner

Microsoft Purview Compliance Solutions

Editor: Tony Redmond

Lead Author: Paul Robichaux

**with Brian Desmond, Michel de Rooij, Christina Wheeler,
Juan Carlos González, and Ben Lee**

Office 365 for IT Pros (2025 Edition)

Mastering Microsoft 365 Office Applications

Published by Tony Redmond (<https://office365itpros.com>)

© Copyright 2015-2024 by Tony Redmond.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means without the written permission of Tony Redmond.

The example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, people, domain name, email address, logo, person, place, or event is intended or should be inferred. The book expresses the views and opinions of the authors. The information presented in the book is provided without any express, statutory, or implied warranties. The authors cannot be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

Although some of the authors are members of Microsoft's Most Valuable Professional (MVP) program, the content of this book solely represents their views and opinions about Office 365 and any other technologies mentioned in the text and is not endorsed in any way by Microsoft Corporation.

Please be respectful of the rights of the authors and do not make and distribute copies of this eBook available to others.

Eleventh (2025) edition. Previous editions appeared under the following titles:

- Office 365 for Exchange Professionals (May 2015 and September 2015).
- Office 365 for IT Pros (3rd edition – June 2016).
- Office 365 for IT Pros (4th edition – June 2017).
- Office 365 for IT Pros (5th edition – July 2018).
- Office 365 for IT Pros (6th edition – July 2019).
- Office 365 for IT Pros (7th edition – July 2020).
- Office 365 for IT Pros (8th edition – July 2021).
- Office 365 for IT Pros (9th edition – July 2022).
- Office 365 for IT Pros (10th edition – July 2023).

The authors issue regular updates for this eBook until they publish a new edition, usually after a year. People who buy the book through gumroad.com can use their accounts to download updates as they become available (the View content link in your receipt always accesses the latest available files). Information about how to access updated files is in our [FAQ](#).

This is the first update for the 2025 edition published on **1 October 2024** (monthly update #112). You can find information about the changes made in updates in [our change log](#) or through our [Facebook page](#).

Tony Redmond took the photo used on the front cover in Orlando, Florida in March 2024.

Table of Contents

Introduction	xi
What We Cover.....	xi
The Colored Boxes.....	xii
Book Updates.....	xiii
The Author Team	xiii
Thanks to Our Microsoft Contacts.....	xiv
Our Sponsor.....	xiv
Comments and feedback.....	xiv
Chapter 1: The Microsoft 365 Ecosystem and Office 365	15
Microsoft 365: More than Office 365.....	16
Microsoft 365 Architecture and Infrastructure.....	17
Microsoft 365 Products and Licenses	36
Microsoft 365 Copilot	42
Preparing Yourself for the Cloud.....	45
The Commercial Success of the Microsoft Cloud	52
Leveraging the Breadth of Office 365.....	54
Chapter 2: Managing Identities.....	56
The Role of Entra ID	56
Identity Architectures	59
Hybrid Identity Authentication Infrastructure	60
Alternate Login ID.....	64
Understanding Authentication in Entra ID.....	65
Customizing the Tenant Sign-In Page.....	69
Joining Computers to Entra ID	71
Guest Access with Entra ID Collaboration	72
Protecting Identities.....	81
Controlling Access	91
User Settings.....	104
App Registrations and Permissions	104
Connecting to LinkedIn	107
PowerShell and Entra ID	108
Chapter 3: Tenant Management.....	109

Office 365 for IT Pros

Cloud versus On-Premises Management.....	109
Tenant and Workload Management.....	111
Miscellaneous Administration Tasks	126
Managing Licenses, Plans, and Billing	136
Managing Network Connectivity.....	138
Monitoring.....	140
Service Requests.....	149
Protecting Data with Encryption.....	153
Reporting	155
Backing Up Office 365	160
Chapter 4: Managing User Accounts.....	169
Managing User Accounts in the Microsoft 365 Admin Center.....	169
Managing User License Assignments	172
Managing User Role Assignments	178
Managing Privileged Accounts.....	185
Managing Exchange Online Mailboxes.....	186
Administrator Access to User Mailbox Settings.....	197
Securing the Data of Ex-employees	198
Managing User Pronouns.....	208
Managing User Settings for Viva Insights.....	208
Managing User Access to Microsoft Bookings	209
Chapter 5: Managing Exchange Online	210
Exchange Online.....	210
Native Data Protection	212
Managing Mailboxes.....	214
Autodiscover.....	242
Recovering Deleted Mailboxes.....	242
Inactive Mailboxes.....	243
Automatic Mailbox Maintenance	251
Archive Mailboxes.....	258
Shared Mailboxes	268
Mail Contacts and Mail Users	280
Recipient Moderation	281
Blocking Basic Authentication	283

Office 365 for IT Pros

Chapter 6: Mail Flow.....	285
Configuring Mail Flow.....	285
Managing Connectors	302
Mail Flow Rules	305
Remote Domains	313
Fallback Domains.....	314
Device and App Mail Relay to Exchange Online	314
High Volume Email (HVE)	315
Exchange Online Protection (EOP).....	317
Microsoft Defender for Office 365 (MDO).....	349
Attack Simulation Training	354
Investigations	360
Threat Explorer.....	361
Monitoring and Troubleshooting Mail Flow	363
Transport Limits.....	378
Chapter 7: Managing SharePoint and OneDrive for Business	381
SharePoint Online.....	381
Sharing	399
SharePoint Online Extensibility Options	408
Additional Features and Settings in SharePoint Online	414
OneDrive for Business.....	419
Microsoft Loop.....	430
Migrating to SharePoint Online and OneDrive for Business	431
Microsoft Lists	434
Microsoft Search	436
How Microsoft Viva and Microsoft Syntex Bring AI to SharePoint	442
Other Services Using SharePoint Online and OneDrive for Business	447
Chapter 8: Planner and Tasks	449
Planner Architecture and Management.....	449
Using the Planner Web Client.....	460
Using Planner in Teams.....	476
Using Planner Premium.....	478
Chapter 9: Managing Video	479
Stream Architecture and Management.....	479

Office 365 for IT Pros

Using Stream	487
Chapter 10: Managing Groups	497
An Identity and Membership Service.....	497
Group Components	501
Implementing Groups	506
Entra ID Groups Policy	507
Creating Microsoft 365 Groups.....	517
Managing Groups with Outlook Clients	524
Guest Access to Microsoft 365 Groups.....	526
Controlling Guest Access to Groups	533
Removing and Recovering Groups.....	539
Group Expiration Policy	542
Dynamic Microsoft 365 Groups	546
Groups and Compliance.....	551
Viva Engage and Groups.....	552
Evaluating Viva Engage, Groups, and Teams.....	556
Distribution Lists.....	557
Dynamic Distribution Lists.....	568
Migration from Email Distribution Lists	573
Comparing Groups, Distribution Lists, and Shared Mailboxes	576
Chapter 11: Teams Basics.....	577
Workgroup Collaboration	577
The Structure of Teams	586
Maintaining Team Membership.....	596
Teams Messaging	602
Personal (1:1) and Group Chats	615
Teams Meetings	625
Teams Calling	650
Viewing Organizational Information	651
Presence and Status.....	652
Files: Linking Teams and SharePoint Online	654
Teams for Frontline Workers.....	659
Can Teams Replace Email?	660
Teams and Email Interaction	663

Office 365 for IT Pros

Chapter 12: Managing Teams.....	668
Keeping Teams in Good Shape.....	668
Creating a Deployment Plan for Teams.....	668
Teams Management.....	669
Creating Teams.....	684
Dynamic Teams.....	693
Hiding Teams from Exchange Online	693
Using a Team-Enabled Group as a Distribution List.....	694
Deleting (and Restoring) Channels and Teams.....	695
Channel Moderation.....	697
Managing Settings for a Team.....	698
Guest Access for Teams.....	700
Email Integration for Teams Channels.....	704
Teams and Compliance	707
Auditing Teams.....	719
Teams and the Groups Expiration Policy.....	720
Archiving Teams	720
Reporting Teams Usage	722
Extending Teams	724
Teams App Setup Policies	728
Managing Access to Apps	730
Teams App Store.....	731
Teams and Bots	731
Office Connectors and Teams.....	732
Teams Approvals.....	732
Debugging Teams Clients	733
Migration to Teams.....	734
Chapter 13: Managing Teams Calling and Devices.....	736
Teams Calling Fundamentals	736
Teams Meeting Enhancements	749
Teams Phone	753
Teams Devices.....	773
Troubleshooting and Monitoring Calls.....	787
Chapter 14: Managing Clients	800

Office 365 for IT Pros

Many Clients, One Service.....	800
Managing the Microsoft 365 Apps Suite.....	803
Using the Microsoft Apps Admin Center	812
Managing the Outlook Client Family.....	818
Managing Client Access and Protocols.....	827
Managing Teams Clients.....	832
Managing OneDrive for Business Clients.....	840
Managing Microsoft Authenticator	841
Optimizing Microsoft 365 Client Network Access	844
Chapter 15: Managing Devices.....	847
Comparing the Three Solutions	847
Getting Started with Intune	848
Managing Apps	851
Managing Devices	858
Security by Compliance	861
Intune Management.....	864
Chapter 16: Managing Data Governance and Compliance	868
Data Governance.....	868
Principles of Data Governance	871
Compliance Permissions	873
Optical Character Recognition.....	874
Retention Policies and Publishing Label Policies	874
Rules or Principles of Retention.....	876
Retention Policies	877
Retention and Sensitivity Labels	898
Creating New Retention Labels.....	900
Using Retention Labels.....	906
Auto-Label Retention Policies.....	913
Records Management.....	918
Processing Manual Dispositions	922
Event-based Retention	926
Removing Retention Labels.....	927
Data Classification Dashboard.....	927
Ingesting Items for Review from External Sources.....	930

Office 365 for IT Pros

Using PowerShell with Retention Labels and Policies.....	931
Moving Data Between Tenants	941
Understanding the Exchange Mailbox Lifecycle.....	942
Exchange Mailbox Retention Policies	947
Communication Compliance.....	951
Information Barriers.....	961
Chapter 17: Managing eDiscovery	971
Content Searches.....	971
Creating and Running a Content Search.....	974
Auditing of Search Activities	990
Microsoft Purview eDiscovery.....	991
Premium eDiscovery.....	997
Data Search Cases	999
Using PowerShell with Content Searches	1001
Using PowerShell to Manage eDiscovery Cases.....	1008
In-place Holds and Litigation Holds.....	1011
Chapter 18: Managing Data Loss Prevention	1013
Leak Prevention with Software.....	1013
Microsoft Purview Data Loss Prevention.....	1015
Sensitive Information Types	1015
Microsoft Purview DLP Policies	1017
DLP and Insider Risk Management.....	1030
Endpoint DLP	1031
Creating Custom Sensitive Information Types.....	1032
Document Fingerprinting	1037
Chapter 19: Managing Information Protection	1039
The Need to Protect Data.....	1039
Rights Management	1040
Enabling Rights Management for a Tenant.....	1044
Sensitivity Labels	1046
Protecting SharePoint Online and OneDrive for Business.....	1078
Protecting Email	1084
Managing Microsoft Purview Message Encryption.....	1094
Hybrid Protection.....	1103

Office 365 for IT Pros

Protecting Windows Files	1103
Managing Sensitivity Labels with PowerShell.....	1106
Azure Rights Management PowerShell.....	1115
Using Microsoft Defender for Cloud Apps to Protect Office 365 Content.....	1120
Microsoft Information Protection Auditing	1121
Cloud Exit for Encrypted Content.....	1122
Chapter 20: Managing Auditing and Reporting	1124
Microsoft 365 Audit Framework	1124
Activity Alerts and Alert Policies	1146
Office 365 Cloud App Security	1151
Third-Party Auditing Alternatives.....	1156
Exchange Online Administrative Auditing	1157
Exchange Online Mailbox Auditing	1157
Reporting Workload Activity.....	1162
Chapter 21: Power Platform	1170
Building No-Code/Low-Code Solutions	1170
Power Platform Administration.....	1171
Power Automate	1181
Power Apps	1192
Power Platform Solutions	1208
Power BI.....	1211
AI Builder for the Power Platform	1218
Power Pages.....	1220
Copilot Studio	1221
Teams and the Power Platform.....	1225
Data Storage Comparison	1227
Chapter 22: Prepare Microsoft 365 Business for Copilot	1228
Your step-by-step guide to adopting Microsoft 365 Copilot with confidence	1228
CoreView's unique 7-step approach	1229
10 unique Copilot challenges (+ solutions)	1229
Five more advanced tips for Copilot adoption	1239
CoreView's Free Tools for Microsoft 365 Management	1240
Appendix	1243
Annualized Run Rate for the Microsoft Cloud	1243

Office 365 for IT Pros

Growth in Office 365 User Numbers	1244
Office 365 Quarterly Performance Against SLA.....	1245

Introduction

Welcome to the Eleventh (2025) edition of **Office 365 for IT Pros**, a book focused on the Microsoft 365 cloud productivity suite. The goal of this book is to help tenant administrators, architects, and technologists understand and exploit the capabilities available in the enterprise version of Office 365 and the surrounding Microsoft 365 ecosystem. We have seen enormous change since Microsoft released Office 365 in July 2011. It's been a blast tracking, analyzing, and documenting the evolution of Office 365 since we started to write *Office 365 for IT Pros* path in the summer of 2014.

Some accuse Microsoft of applying branding too liberally with the result that they confuse customers about just what Microsoft 365 means. In the context of this book, Office 365 means the enterprise Office services accessed by tenants via the internet, including Exchange Online, SharePoint Online, OneDrive for Business, Teams, Planner, and Viva Engage. We also cover the functionality available in the various administrative portals and how to use Power Automate to automate administrative processes. Although we cover clients like Outlook, we don't cover applications like Word, Excel, and PowerPoint except in passing.

This is not an official Microsoft publication and Microsoft endorses none of the opinions expressed here in any way. Instead, it's a collection of thoughts, ideas, and perspectives from a team of highly experienced MVPs (some of whom are members of the Microsoft Most Valuable Professional program).

What We Cover

This book helps you maximize your use of Office 365. The major topics include:

- Introducing Office 365 and how the Office 365 servers fit inside the overall Microsoft 365 ecosystem.
- Managing user identities with Entra ID, including synchronization with on-premises directories and different authentication methods.
- Managing the overall Office 365 framework.
- Understanding the two original core workloads: Exchange Online and SharePoint Online (including OneDrive for Business), including how mail flow works to bring messages into and out of your tenant.
- Working with Microsoft 365 Groups, including how to manage the membership and access service enabled by Groups.
- Understanding the architecture of Teams and how this popular application leverages so many parts of Microsoft 365 and Azure. With over 320 million monthly active users, no one can doubt the status of Teams as the third core workload.
- Understanding how to manage Teams within the enterprise.
- How Microsoft Stream organizes and manages video files.
- Using Microsoft Planner to organize team and group projects effectively.
- Managing desktop, mobile, and browser clients, with or without Intune.
- How data governance and compliance work, including how retention policies and retention labels work across Exchange Online, SharePoint Online, OneDrive for Business, and Teams.
- How workloads capture audit records for thousands of different events and how to use that audit data to answer questions about how people use (and sometimes abuse) the service.
- Using Power Automate and Power Apps to automate different user and administrative operations.
- Protecting documents and emails with data loss prevention policies and encryption (sensitivity labels).
- Artificial intelligence is all the rage these days. Because of the need for client apps to interact with Large Language Models through prompts, Microsoft 365 Copilot is largely a client-driven technology.

Office 365 for IT Pros

We cover the administrative aspects of Microsoft 365 Copilot where appropriate across the different chapters.

It's a lot of information to cover in a single book. In fact, our package is more like six individual books stitched together to form a cohesive view of Office 365:

- Microsoft Entra ID.
- Exchange Online.
- SharePoint Online and OneDrive for Business (what Microsoft calls ODSP).
- Teams.
- Microsoft Purview compliance solutions.
- Microsoft Information Protection.
- Automating Microsoft 365 with PowerShell.

We hope that you'll like what you find here and appreciate the effort we go through to publish the monthly updates to refresh the material and make sure it is as up-to-date as possible.

Cloud and On-Premises Products

This book is about Office 365, the cloud Office services within Microsoft 365. It follows that when we reference "Exchange" or "SharePoint," we mean the cloud version rather than the on-premises code. Where necessary, we are explicit. For instance, we say "Exchange Online" when we mean that a feature belongs to the cloud version. If we say "Exchange" or "SharePoint," the discussion applies to both cloud and on-premises versions. It's easier with applications like Teams and Planner because they don't exist on-premises (and never will).

Automating Microsoft 365 with PowerShell

Anyone involved with the administration of a Microsoft 365 tenant should have at least a passing acquaintance with PowerShell and the Microsoft Graph APIs. Until this edition, we included a chapter covering how to automate different aspects of Microsoft 365 tenants using PowerShell. The chapter in the tenth edition spanned 90 pages and was growing due to the influence of the Microsoft Graph and the growing support of Graph-based interaction through the Microsoft Graph PowerShell SDK. We decided to split off the chapter into a separate eBook, **Automating Microsoft 365 with PowerShell**, which is included in Office 365 for IT Pros subscriptions.

Even though we now have a separate eBook covering PowerShell, you'll find examples of using PowerShell throughout the book to emphasize the value of being able to automate operations. These examples are intended to illustrate a point in the context of the topic under discussion.

We use a [GitHub repository](#) (see [this article](#) for information) to store code. Referencing scripts in GitHub makes the book a little shorter and allows text to flow better on the page. Another advantage is that the code in GitHub is more likely to work because you can download a complete script instead of transcribing code from a book.

The Colored Boxes

From time to time, we want to draw your attention to something that we think is important. We use three colors to highlight information. The first type is a note.

Note: This is some additional information about a topic that we're discussing. We've included it because we think it adds some value.

We also have some warnings for things that you need to understand.

Warning: Warnings or other cautionary notes will appear like this. Try not to ignore these, the lessons were often learned the hard way and we'd hate to see you suffer the same pain.

And there are lots of real-world observations that we think will interest you.

Microsoft 365 Groups: Every group is represented as a group object in Entra ID...

Book Updates

Apart from the multi-platform nature of Microsoft 365, ever since we started working on Office 365 for IT Pros, we wanted to avoid the static nature that afflicts traditional technical books. Given that Microsoft issues updates for all workloads on a constant basis, it didn't seem to make much sense to say that any text was definitive. This feeling led us to the decision to create a book that changes to match what happens inside Office 365.

Due to the fast-changing nature of Office 365, some of the user interface elements illustrated in this book might have changed when you read this book. The same is true for details of how a feature works. Our tenants use the "Targeted Release" option to allow us to see new features before Microsoft releases them to general availability. We may cover something here that you might not see yet in your tenant. Coping with a fast-changing (or even ever-changing) environment is just one of the challenges faced by tenant administrators. New features appear, options move around, and options function in a slightly different manner. Things are just very different from the somewhat staid situation that often occurs inside a typical on-premises infrastructure.

Microsoft's documentation has improved dramatically since 2018 but is sometimes bypassed by recent developments. We do our best to keep an eye on what is happening and what changes, but please forgive us if we overlook some details recently revealed or updated by Microsoft. Think of this as an opportunity to demonstrate how good a detective you are in seeking the right answer based on the evidence presented in this book, on Microsoft's websites, and in the voluminous amount of text that you will find in blogs scattered around the web. Of course, blog authors are not seers either and their text begins to degrade as soon as it appears, so you must gather evidence and put it in context with what you see in your tenant at the time when you're trying to solve a problem or get something to work as you believe it should. Welcome to the world of cloud software!

We release updated versions of this book monthly (see [our FAQ](#) for information about downloading updates). Our policy is to fix errors as soon as we find them, or a reader tells us about a problem. We will update (patch) the version that is currently online to give subscribers the opportunity of always being able to fetch the latest content from where they bought the book (Gumroad or Amazon). It's just like fixing bugs in a software program.

The Author Team

The Office 365 for IT Pros writing team is:

- Tony Redmond.
- Paul Robichaux.
- Ben Lee.
- Brian Desmond.
- Juan Carlos González.
- Christina Wheeler.
- Michel de Rooij.

Office 365 for IT Pros

Our Technical Editor is Vasil Michev. For more information on the team, see [our online bios](#).

Microsoft MVP Program

Tony, Juan Carlos, Paul, Michel, Ben, and Vasil are proud members of Microsoft's Most Valuable Professional (MVP) program and Brian and Christina are MVP alumni. See [this page](#) for more information about the MVP Program. Christina and Brian are ex-MVPs, but we don't hold that against them.



Thanks to Our Microsoft Contacts

Many people at Microsoft helped us to understand some technical details or explain how an application works. The list of those who have helped is now too long to include here. We extend our thanks to everyone at Microsoft who answered our questions. We owe you a huge debt.

Speaking of Microsoft, we don't have a foreword for this edition. This isn't because we don't respect the forewords written for previous editions by luminaries such as [Jeffrey Snover](#) and [Jared Spataro](#). We greatly appreciate the sentiments expressed in these forewords but have concluded that forewords are not something that a constantly updated book should have. Please enjoy the online copies of the previous forewords.

Our Sponsor



It's hard to find the time to gather information, make sure that it's current, and write it up. Since 2014, the Office 365 for IT Pros team has dedicated an enormous amount of effort into the creation and updates of the eBook, including the many revisions and rewrites required for this edition. We could not undertake the task without the help and support of our sponsor, **CoreView**. We are very grateful for the support extended by CoreView and for the support given in the past by our previous sponsors (CodeTwo Software and Quest Software). Please read Chapter 22 or visit [CoreView's website](#) to learn more about their innovative and useful solutions.

Comments and feedback

Comments about the content as well as pointers to where little errors might have crept into the text are always welcome. Please send your comments, suggestions, and observations to BookComments@Office365ITPros.com or post to our [Facebook page](#).

Chapter 1: The Microsoft 365 Ecosystem and Office 365

Paul Robichaux

Microsoft launched Office 365 in June 2011. Much later, it introduced Microsoft 365 by combining Office 365, Windows 10 Enterprise, and the Enterprise and Mobility Suite. They have since updated the Office 365 plans for small to medium businesses to use Microsoft 365 branding and changed the name of the Office Pro Plus desktop application suite to "Microsoft 365 apps for enterprise." These changes may have made the marketing team happy, but each rebranding created a lot of confusion. Even today, the differentiation between Microsoft 365 and Office 365 can be unclear.

Despite that confusion, Office 365 has been wildly successful-- currently over 400 million people in more than one million customer organizations use it worldwide. Office 365 is the cornerstone of the Microsoft 365 ecosystem and consists of a set of cloud services, referred to as *workloads*. The three base Office 365 workloads are Exchange Online, SharePoint Online, and Teams. Exchange and SharePoint originated as on-premises servers, but the cloud products are very different from their on-premises counterparts, notably because of the engineering effort to manage data at a massive scale. Other workloads like Teams and Planner are cloud-only and have no allegiance to any on-premises technology. Indeed, the way that cloud-only workloads consume other cloud services and microservices (services built for a specific purpose, like Azure Key Vault) mean that they will never appear on-premises.

The basic idea behind cloud services is that customers transfer the responsibility for running workloads to a cloud provider, who then charges a fixed fee based on some unit of work, such as a user account or mailbox. Customers either start from scratch with a cloud provider or migrate their data across the internet to the cloud provider, which is meant to offer enough computing, network, and operational capacity to handle the work generated by hundreds of thousands of companies. The value proposition is that the massive economy of scale allows cloud providers to deliver the same or better functionality as self-hosted applications at a lower cost. Another factor is that moving data into the cloud makes it available for sophisticated processing that cannot be done (because it is too costly or complex) by on-premises servers. Features that use artificial intelligence, like auto-suggested replies, are now in many client apps. This functionality depends on access to user data stored in Exchange Online, SharePoint Online, OneDrive for Business, and Teams.

It's best to think of Microsoft 365 not as just one application or workload, but as a complex ecosystem made of multiple moving parts, connected via components like the Microsoft 365 substrate. This ecosystem takes advantage of shared services like Search and machine learning and offers standardized programming interfaces in the Microsoft Graph APIs. The ecosystem did not develop overnight and is the product of over twenty years of engineering effort.

It's challenging to keep any book about technology completely up to date. We do not claim that the coverage here is perfect because Microsoft 365 continues to evolve to keep its cloud services "evergreen." A cloud service that stays static is less attractive to its users than one where changes and updates appear all the time. To set some achievable boundaries, this book covers Office 365 in-depth and the remainder of the Microsoft 365 ecosystem when appropriate.

Microsoft 365: More than Office 365

Microsoft calls Microsoft 365 “the world’s productivity cloud,” saying that it represents their vision for the future of productivity tools spanning an integrated set of apps and services. The upshot of this marketing activity is that Microsoft liberally applies the Microsoft 365 moniker to a wide range of products offered to consumers and the enterprise. To be clear, this book covers Microsoft 365 as it affects Office 365 for enterprise customers and does not deal with packages offered to consumers or small businesses. Table 1-1 lists the Microsoft 365 packages for the enterprise.

Variant	Target market	Components
Microsoft 365 Enterprise	Companies with more than 300 users.	Windows 11 Enterprise Office 365 (E3 or E5) EMS
Microsoft 365 Business	Small to medium companies (up to 300 users).	Windows 11 Business Microsoft 365 Business Standard EMS
Microsoft 365 Frontline	Customer service and support workers.	Windows 11 Enterprise Office 365 F3 EMS
Microsoft 365 Education	Educational establishments.	Same offerings as for Enterprise, Business, and Frontline
Microsoft 365 Non-Profit	Non-profit organizations.	Same as Microsoft 365 Business
Microsoft 365 Government	U.S. government and state agencies.	Same as Microsoft 365 Enterprise (E3 and E5 bundles)

Table 1-1: Microsoft 365 products

Although the enterprise Microsoft 365 plans include Office 365, customers can still buy Office 365 licenses separately. There’s no functional difference between the application functionality of Exchange Online, SharePoint Online, and Teams in the Microsoft 365 plans versus the Office 365 plans. The differences exist in areas like device and identity management and advanced compliance and data governance features.

Since the introduction of Microsoft 365, Microsoft has added a great deal of functionality in the Microsoft 365 plans, especially in the areas of compliance, data governance, and identity management. Two useful tools are available to help understand what’s available, and the costs involved:

- [PDFs with overviews](#) of the Office 365 and Microsoft 365 plans. The PDFs are not official Microsoft documentation. They are the creation of a Microsoft Australia employee.
- A [Microsoft comparison of the features available to each plan](#), including the costs of subscriptions and add-ons.

Over time, Microsoft introduced components that work across the suite instead of being restricted to individual workloads. Good examples of where this has happened are the management consoles like the Microsoft 365 admin center and the Microsoft Purview Compliance portal. Looking back, the progress to integrate applications enabled Office 365 to progress from being a loose collection of barely cloudified on-premises applications to evolving into an integrated ecosystem. That progression took the best part of six years; it’s happening more rapidly in Microsoft 365.

Evidence exists that an increasing percentage of the user base, particularly in medium to large enterprises (over one thousand seats), see their most cost-efficient licensing arrangement as one built around Microsoft 365. In April 2022, Microsoft said that 45% of Office 365 seats are part of Microsoft 365 plans. Many of these customers buy Microsoft 365 because they want to use Enterprise Mobility and Security and advanced

Microsoft Entra ID features. The influence of Microsoft's success in transitioning from Office 365 to the Microsoft 365 suite is seen in the steady growth of Enterprise Mobility and Security seats to 259 million monthly active users (October 2023).

Microsoft 365 Architecture and Infrastructure

Attention to detail and absolute adherence to well-defined procedures are the hallmarks of how Microsoft runs its cloud infrastructure. Without attention to detail enforced through automated processes and procedures, it would be impossible to manage a service for millions of tenants ranging from small to the very largest companies.

An indication of the scale of Microsoft's cloud businesses is its assertion (June 2019) that it serves [a billion users and twenty million businesses](#). The investment needed to buy land and build data centers, install computing resources, power, and cooling, and automate the management and security of applications and data at the scale of Microsoft 365 is massive. The ability to deliver services to customers at a competitive price is only possible for companies with very deep pockets. Microsoft is one of those companies. Google and Amazon are other examples. Let's look at some aspects of Microsoft's cloud infrastructure.

Data Sovereignty and Residency

There are two useful concepts you'll need when discussing cloud solutions:

- Residency is where data lives.
- Sovereignty "[refers to the concept that data is under the control of the customer](#) and governed by local law." For example, some countries have requirements for businesses operating in those countries may allow their data to be stored or who may process it, and virtually every government has a set of laws and regulations controlling when and whether law enforcement may obtain access to cloud data.

Microsoft's family of cloud solutions (including Azure, Office 365, Dynamics, and so on) provide various types of support for customer's residency and sovereignty requirements, many of which may derive from other regulatory or legal demands.

Data Residency

One important aspect of the cloud is that the service provider has ultimate control over where your data goes, just as you would if your data stayed on-premises. A growing number of countries have regulations that limit where data may be permanently stored—Microsoft says that between 2017 and 2022, the number of countries enforcing data residency restriction [increased from 35 countries to 62](#), with nearly double the number of regulations. Microsoft has tried to keep up with these restrictions by building data centers and locating services in various regions—for example, the advent of the European Union's GDPR spurred Microsoft to build out their Microsoft 365 and Azure data center offerings in Europe to allow European customers to keep their data within the EU. Microsoft also offers [multi-geo capacity](#) for some workloads so that the tenant owner can control exactly which regions SharePoint, OneDrive, and Exchange Online content for specific users is stored in.

Teams has always been an outlier, since many of its capabilities were only hosted in specific regions (so that a Teams chat between someone in Denmark and two people in Ukraine might result in data going to North America because that's where one or more Teams microservices were hosted). Over time Microsoft has moved Teams services around the globe. Microsoft [now promises](#) that "Teams core customer data, consisting of Teams chat messages (including private messages, channel messages, meeting messages, and associated images), and meeting recordings, present in the tenant, will be stored at rest in local datacenter regions." They

have also announced an add-on package called [Advanced Data Residency](#) (ADR), which gives customers some additional migration capabilities and data storage at rest commitments for additional workloads. ADR currently covers Exchange, SharePoint, OneDrive, Teams, Copilot, Viva Connections, Viva Topics, and most of the Purview features. ADR is a good example of a service that will be intensely interesting to a fraction of Microsoft's customers and of no interest to the rest.

Data Centers and Regions

Microsoft 365 tenants share a single large logical infrastructure composed of hundreds of thousands of servers spread across multiple Microsoft data centers. Figure 1-1 shows Office 365 data centers in June 2022. This map is only of historical interest; Microsoft no longer updates it, preferring instead to provide a [large set of tables](#) showing exactly which services are available in which regions. In addition, this map doesn't show the deep investment made to create "edge" network termination points set up by Microsoft to bring user traffic quickly into its data centers from all around the world or the internal network that transports tenant data between data centers. In total, the [Microsoft Cloud](#) (Microsoft 365 and Azure) spans well over 200 data centers. Not every Microsoft Cloud data center delivers Office 365 services to customers, but the number of local data centers delivering Office 365 is growing over time.

Microsoft organizes its data centers into *regions*. The data center region selected to host the data for new tenants is based on the country (location) selected by the tenant. Since launching Office 365, Microsoft has gradually built out the data center infrastructure. In many cases, new data centers are launched to keep data local ("[in-geo data residency](#)") to accommodate customer choice and satisfy local regulations. Where large regional data centers such as the European Union used to be the focus for Office 365 service delivery, localized service is now available in many individual countries like Australia, France, Germany, Singapore, Poland, Mexico, Spain, Switzerland, and the U.K. Microsoft calls the country-level regions "Go Local," as in "Go Local Japan" or "Go Local Australia." This is an internal Microsoft notation that reflects the purpose of country-level regions.



Figure 1-1: 2022 map of Office 365 data center locations (source: Microsoft)

A big advantage gained by segmenting tenant workload across multiple data center regions is that a fault that affects users in one region seldom spreads to other regions. Known single points of failure that can affect multiple regions do exist, but in general, outages don't affect more than a single workload running in a single

region, such as a failure affecting mailboxes running in a single Exchange Online Forest or sites served by a single SharePoint Online farm.

Apart from the ability to serve large customer populations, natural and economic advantages such as ambient temperature (to reduce the need for cooling) or availability of cheap hydroelectric power influence data center placement. Security is of prime concern and Microsoft pays great attention to the physical security of the buildings (you will not find large signs proclaiming Microsoft's ownership anywhere) as well as cyber-security for the data contained within the buildings.

Co-Location of Consumer and Business Services

In addition to its enterprise cloud applications, Microsoft hosts over 400 million Outlook.com users in the same data centers. Outlook.com mailboxes run on the same Exchange Online server, storage, and network infrastructure, giving consumer accounts the same advantage of features like Native Data Protection and Exchange Online Protection, and the same clients are available for both services. Of course, many Exchange Online features aren't available in the free Outlook.com service even though the same engineering teams support the two services. Microsoft introduces some functionality into one service before they decide to do the same for the other. For example, "Sweep" rules first appeared in Outlook.com and are now available in OWA, while the calendar and calendar sharing features now available in Outlook.com originated in Exchange Online. Taken together, the infrastructure shared by Exchange Online and Outlook.com delivers email to billions of mailboxes (not all the mailboxes belong to humans). Microsoft uses the same shared infrastructure approach with OneDrive for Business and the consumer version of OneDrive.

Number of Servers

As you'd expect, the infrastructure is also massive if looked at in terms of the number of individual servers running different workloads. The last public figure for Exchange Online is 300,000 mailbox servers (September 2022) while that for SharePoint Online is 180,000 servers (May 2019). Add in the servers used for Teams, Planner, Microsoft Entra ID, other Azure services, and supporting services, the number deployed to run Office 365 workloads comfortably surpasses one million physical servers.

Even with so many resources, demand flowing from an event can exert enormous pressure on an online service when user numbers grow dramatically over a short period. During the Covid-19 pandemic, Microsoft onboarded tens of millions of new users. In the case of Teams, the number of daily active users increased from 20 million in November 2019 to 75 million in April 2020, creating a surge in user demand that also impacted SharePoint Online, OneDrive for Business, Exchange Online, and other services. To maintain responsiveness for end-users, Microsoft trimmed the functionality of different applications. Background processes didn't run as often and Microsoft adjusted some features to reduce demand, such as dropping the resolution of Teams meeting recordings from 1080p to 720p. Although some interruptions happened, generally Office 365 remained online and handled the swelling load. After Microsoft had the chance to commission new server and storage resources in the data centers, they reversed the feature adjustments.

Data Residency and Workloads

Instead of focusing on the location of physical data centers, Microsoft prefers to discuss data residency. The [definitions and terms page](#) explains how Microsoft approaches data residency while the [data locations page](#) gives guidance about how a tenant can find out the storage location for their data used with individual workloads.

Generally, all Microsoft 365 data centers deliver core services (Exchange Online, SharePoint Online, and OneDrive for Business). Other services, like Teams and Project Online, might also run in the same data centers. In some cases, other data centers within the region deliver specific services, as in North America, where the

Planner service runs from data centers in California and Virginia. Microsoft Entra ID is another service that can come from another region. For instance, the U.K. region accesses Microsoft Entra ID from the EMEA and U.S. data centers.

The point of delivery for services changes over time and if you are concerned about data residency, you should confirm with Microsoft to understand exactly where your data are for all applicable applications.

New Data Centers

Once a new data center comes online, a sophisticated migration process moves tenants from other data centers to the new location. The same is true when Microsoft creates a new region. For instance, after the United Kingdom data centers came online, some tenants asked to move their work to those data centers to keep their data "in country;" the same happened in France or when Australian and New Zealand tenants moved to the Australian data centers. This work happens behind the scenes to make the eventual switchover is fast and painless. Microsoft has [a documented process](#) to help tenants with specific data residency requirements to request a move for their core data to a new region after it comes online.

The creation of a new data center region normally means that the data center first delivers the base workloads to tenants. It can take some time before the full range of service capabilities is available, including applications (like Teams or Planner) and utilities. Microsoft is currently developing several new regional data centers.

Workloads Running Within Data Center Regions

Microsoft distributes work across all data centers within a region to protect data against failure. For instance, the active-active design for Exchange Online Database Availability Groups (DAGs) means that mailbox database copies exist in at least two data centers within a region. In addition, as Microsoft adds data centers to a region, the opportunity exists to spread database copies to those data centers. For instance, new DAGs built for use by Exchange Online in the European Union region might include databases spread across the Amsterdam, Dublin, Helsinki, and Vienna data centers. Spreading data across so many data centers reduces the risk that any individual outage will affect a sizeable number of users. It is a deployment strategy that the average on-premises administrator could never contemplate because of the investment needed to build out the underlying data centers and network.

Another way to understand what data center region supports data for your tenant is to access the Organization Profile (in the Org Settings section of the Microsoft 365 admin center). Go to the Data Location section and you will see the region for some, but not all, of the workloads used by the tenant (Figure 1-2). Microsoft complies with what it calls the [EU data boundary](#), meaning that all services and data used by tenants based in the European Union will remain within the European Union.



Data location

As part of our transparency principles, we publish the location where Microsoft stores your customer data, see [Where your Microsoft 365 customer data is stored](#).

Service	Geography
Microsoft Exchange	European Union
SharePoint	European Union
Microsoft Teams	European Union

Figure 1-2: Data locations for a tenant

Although Microsoft Entra ID holds most of the information for tenant accounts and configurations in the same data center region as a tenant's data, an exception exists in that Microsoft stores five user-related

attributes including the User Principal Name and password hash for tenant accounts in the U.S. This is to make sure that authentication can happen as quickly as possible, no matter where in the world a user is located. For more information on this topic, see Microsoft's [support article on the situation](#) for European customers.

Sovereign Clouds for Government Use

Most of the time, we think of Office 365 as a single cloud service delivered worldwide by Microsoft. It's more than that, of course; there are the other Microsoft cloud services consumed by Office 365, such as Entra ID, but there are also multiple independent instances of Office 365 offering what appear to be very similar services, but for specific regions or markets. These are generally known as *sovereign clouds*.

Let's start by saying that the primary Office 365 cloud we all think of first may be referred to as "Office 365 Commercial". Microsoft's Richard Wakeman [defines three useful principles](#) around which Commercial was built:

1. The directory service is shared and globally accessible, meaning that directory authentication and processing may happen in any Microsoft data center or region, even if directory data is restricted to a specific geography.
2. The network is global. At least in theory, any of the Office 365 Commercial endpoints (which all end in .com, at least for now) can resolve to any worldwide instance of the endpoint. That is, if your tenant's in the US, and you're visiting Ireland and go to outlook.office.com, your connection will probably be resolved to a Microsoft front door in Ireland.
3. The support system is global. When you file a ticket, or when an outage occurs, the people who handle it may be anywhere in the world.

New domains for the cloud: Microsoft is gradually moving some of its services to the ".microsoft" domain. For example, instead of *outlook.office.com*, users will eventually go to *outlook.cloud.microsoft*. For now, they're starting slowly. Copilot, along with the PowerPoint, Excel, Word, Planner, Loop, Mesh, Sway, and Viva applications are there now (e.g. *copilot.cloud.microsoft* is the URL for the Copilot business chat homepage), as are the service status page (*status.cloud.microsoft*) and the Microsoft 365 admin center (*admin.cloud.microsoft*). Other services will follow; for example, in September 2024 Microsoft announced the forthcoming movement Purview message encryption to the new *static.microsoft* domain. They've promised to give at least 30 days of advance notice before changing existing service URLs.

Microsoft also sells a family of Office 365 solutions that they call the Government Community Cloud, or GCC. [Microsoft describes GCC](#) as dedicated for use for "United States Federal, State, Local, and Tribal governments, as well as contractors holding or processing data on behalf of the US Government." GCC is a data enclave inside the Office 365 Commercial cloud (meaning it is not a physically separate cloud instance), and all GCC users of GCC share the enclave (thus the use of "community" in the name). Although it isn't clear from the name, GCC is only meant for unclassified information, although it is approved for use with various types of other sensitive information, including tax and financial data and certain types of sensitive law-enforcement-related information. Some of the approvals required to process certain data types (such as [the CJIS certification](#) required for law enforcement use) require special configuration, which of course Microsoft will assist with as part of a consulting engagement.

Defense-related agencies and businesses can instead use GCC High, a separate GCC instance with additional security controls. GCC High isn't allowed to contain or process classified data. However, GCC High can be used for a type of information known as "controlled unclassified information," or CUI. Agencies or companies that need to do so can use the Office 365 Government Secret cloud, approved for processing certain types of classified information. As you might guess, this instance of the cloud provides a service labeled as "Office 365

Secret,” which includes many (but not all) of the familiar features from the commercial version. It is available for use by US government agencies and a limited subset of industrial contractors.

Microsoft operates a specially-built version of Office 365 for the [US Department of Defense \(DoD\)](#). This offering is *only* for the US DoD and their approved vendors or agencies and is hosted in its own logically and physically separated cloud from the commercial Office 365 services. Microsoft is rebranding this offering as “Microsoft 365 DoD” so you may see both the Office 365 and Microsoft 365 brands referenced. The only way to get access to this service, whatever its name, is to be part of the US DoD. A similar environment was built for the UK’s Ministry of Defense.

Besides these services, Microsoft has several sovereign Azure offerings. Azure Government is a separate instance of Azure for government use; according to Microsoft it is “based on the same underlying technologies as global Azure” but not necessarily an exact replica. Azure Government is referred to by Microsoft as “US sovereign,” meaning that the directory services and network only operate in the US. Their data is not stored or processed anywhere outside the US, and all the Azure Government endpoints are in the .us or .mil domains. Furthermore, all the people who support Azure Government are US citizens or permanent residents who have passed security screening checks. Access to Azure Government is limited to US federal agencies, state and local governments, and partners or solution providers that support them.

To support Office 365 Government Secret, Microsoft also built what they call the Microsoft Classified Cloud (for Secret and [Top Secret](#) data). They even have their own [website touting their value to the intelligence community!](#). Figure 1-3 shows the current set of publicly acknowledged Office 365 clouds for government use.

Office 365 Government:

Meeting the full spectrum of government data needs

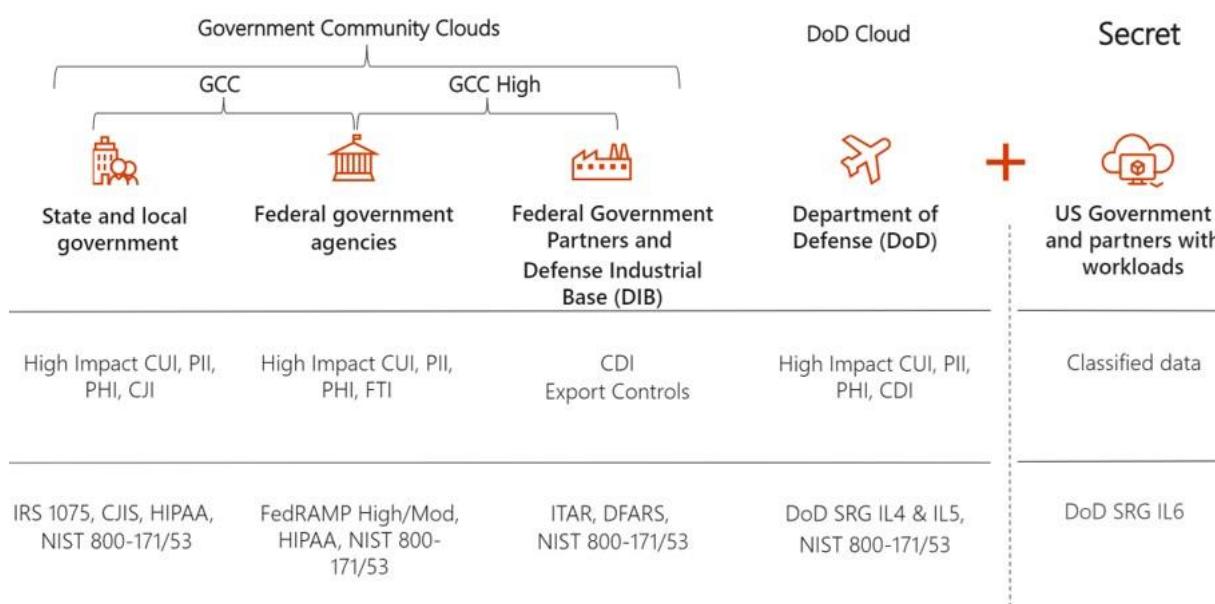


Figure 1-3: Microsoft’s government clouds for Office 365 (late-2023)

The Chinese government requires that most cloud services doing business in China have local instances that are logically separate from their overseas counterparts. These instances must be maintained by Chinese citizens in Chinese data centers. In the case of Office 365, this service is known as “[Office 365 operated by 21Vianet](#)” (21Vianet being the Chinese company that runs the service for Microsoft). Microsoft carefully emphasizes that they don’t operate or manage this service. There used to be a similar service for German customers known as Office 365 Germany, too, but as Microsoft added data centers in Germany, that variant

went away. It's interesting to wonder about how much work Microsoft does to create a "containerized" version of the basic Office 365 services for deployment in a new country and to ask whether this will ever become a feature available to commercial customers.

Additional Cloud Offerings

"[Microsoft Cloud for Sovereignty](#)" offers a customized set of services intended for governments when hosting their own applications (whether newly built or ports of existing applications) in Azure to take advantage of government-friendly features such as [confidential computing](#) and various data protection and auditing controls. Cloud for Sovereignty is a development platform, not a productivity service.

There's also the "[Microsoft Cloud for Sustainability](#)," a set of tools based around the [Microsoft Sustainability Manager](#) for calculating the carbon footprint and environmental impact of your entire business operation. These calculations can be customized to reflect your business (e.g., a manufacturing business will have a very different emissions profile from an insurance agency) and can be as broadly inclusive of emissions and energy consumption as you wish. They've also added a [dashboard that shows the carbon emissions associated with your organization's use of Microsoft cloud services](#)—a courageous move given that it could potentially lead organizations to decide to reduce their cloud service usage. The Sustainability offerings are only available to customers that have enterprise license agreements with Microsoft.

Finally, Microsoft offers an [industry-specific cloud for healthcare](#), although this is more focused on providing a prebuilt set of tools (including data models for care providers and patients and connectors for various other healthcare software) and services targeted at the healthcare market.

Differences in Cloud Service Offerings

Each of the cloud services mentioned above has its own set of supported features. When Microsoft introduces a new feature into "the service," they're really introducing it into dozens of different environments. For example, as of September 2024, Office 365 in China doesn't support Microsoft Forms or Microsoft Planner, and they are still in the process of deploying the new Exchange admin center, well after its availability elsewhere. (It doesn't help that Microsoft's own documentation is inconsistent; it simultaneously [says](#) that Microsoft Booking is, and is not, available in the 21Vianet tenant!) Various Teams features available to commercial customers in North America are still rolling out to tenants based in other countries and Office 365 Education tenants; Viva Engage [isn't available in GCC High](#), nor are polls in Teams, and file sharing using SharePoint and OneDrive works differently in GCC High than in the lower-security GCC and commercial tenants.

Many third-party applications and services that work with the commercial Office 365 services may have incompatibilities, or not be supported, within some national cloud environments. Microsoft has an extensive [list of the API-level differences](#) between the different national clouds. One example: the common Graph *getMessage* call used to fetch Teams message data isn't available at all in the 21Vianet cloud and works differently between the worldwide commercial cloud and its national counterparts.

Even if your application works properly in these clouds, government customers can only run approved applications. There's a complex process to get this approval, and not every vendor submits to it. You may find that your preferred migration tool, management utility, or other application isn't approved, or that, when installed, it doesn't work properly. Be sure to check compatibility with your vendors before moving to one of these environments.

The bottom line for these differences is that if you are considering moving to anything other than the standard commercial service, you should take the time to research the differences in features and service

capabilities between the well-known baseline services in Office 365 and the specific version that you'll have access to.

Multi-Geo Microsoft 365

Organizations can choose to distribute Exchange Online, SharePoint Online, OneDrive for Business, Teams, and Microsoft 365 Groups data across different data center regions (multi-geo). This means that the organization has a home region (known as the "central geo") where most of its work runs and one or more satellite regions. Sites including team, communication, and hub sites, created by distributed users are in their assigned geo-location (otherwise known as the PDL, or "preferred data location", an attribute of their Microsoft Entra ID account). Microsoft says that they are exploring how to add multi-geo capabilities to other applications.

The normal use case for multi-geo is an international company that needs to satisfy data sovereignty requirements. For example, a U.S. company might have subsidiaries in France and the UK. Due to the sensitive nature of the work done in EMEA, the company does not want to store the data in the U.S., as would be normal. With multi-geo, they can choose to have user data for the supported workloads stored in local data centers.

Behind the scenes, once a tenant is enabled for multi-geo, Microsoft transfers the data belonging to the selected users to the satellite regions. During the transfer process, users continue to work as normal until the transfer is complete, at which point they switch over. Cross-region synchronization within the tenant's Microsoft Entra ID instance ensures that all the users within the tenant see a single worldwide picture and can continue to share work with colleagues without hindrance. The only thing that changes is the location of user data. OneDrive for Business is an exception because the transfer process does not move data belonging to an existing OneDrive account. Instead, administrators must run the *Start-SPOUserAndContentMove* cmdlet to [transfer user data to the new location](#).

Distributing user data across multiple regions causes some technical challenges, one of which is eDiscovery. Organizations need to consider if they wish to run eDiscovery locally or at a global level. See [this page](#) for more information.

Multi-geo deployments don't fix poor network performance. Some people assume that this is the case because "the data is closer to the users." This is a fallacy because, in most cases, poor network performance is due to issues such as lack of bandwidth or other problems in the link connecting users to Microsoft or poor routing inside the tenant's internal network. Once inside Microsoft's data center network, traffic flows from region to region very quickly and users do not see a difference when they move to a local region.

Multi-geo is available for most [general-purpose Microsoft 365 data center regions](#). It is not available for the sovereign clouds. To qualify, organizations must have an enterprise agreement with Microsoft and purchase multi-geo licenses for at least 5% of their accounts (previously, the organization had to license at least 250 accounts). Additional monthly fees of \$2 per user are payable for each user licensed for multi-geo capabilities. The fees cover the connection of the base workloads to different data center regions. Because of the extra cost, the most likely customers for multi-geo are multinational companies with complex data sovereignty needs and relatively large numbers of users. For more information, see the [multi-geo home page](#).

Relationship with Azure and Azure Services

Microsoft 365 has a strong relationship with Azure, the other major component in Microsoft's cloud strategy.

- The Office 365 data centers are co-located with Azure data centers.
- Microsoft 365 uses Microsoft Entra ID as its authentication and identity service.

- Microsoft 365 applications use many Azure services such as Azure Key Vault.

Office 365 applications use Azure Storage heavily. Because SharePoint Online provides document management services to applications like Teams, Planner, Stream, and Viva Engage. It is the largest single application consumer (Azure SQL). Teams uses Azure Cosmos DB for message and media stores. At this point, the only major Microsoft 365 storage system not running in Azure is Exchange Online, which continues to use physical mailbox servers.

Cloud Security

No organization will move to the cloud if they believe that their data will be less secure than it is on-premises. When you move to Microsoft 365, you're placing a large bet that Microsoft will do a better job securing your sensitive data than you can do yourself. In this case "securing" means maintaining all three aspects of the security triad: confidentiality, data integrity, and data availability. Add to that the requirement to ensure data privacy, and the additional need in many jurisdictions to maintain [data sovereignty](#), and you quickly find that the degree of security expertise and investment required to maintain a truly strong security posture is outside the budget and capability of the vast majority of on-premises customers.

Microsoft invests roughly US \$1 billion annually in security across its entire product line. This investment covers the typical "gates, guards, and guns" measures that most people think of for physical security, but the investment goes much deeper. All Microsoft 365 workloads are designed and implemented per the [Microsoft Security Development Lifecycle](#). This is described as "*a software development process that helps developers build more secure software and address security compliance requirements while reducing development cost.*" On a practical level, this means that data is secured by being encrypted at rest, that auditing information is available, and that the unified audit API is supported to allow customers and third parties programmatic access to information protection and compliance events. For instance, BitLocker is used to protect Exchange Online databases while files stored in [SharePoint Online and OneDrive for Business libraries are individually secured](#) with their own 256-bit Advanced Encryption Standard (AES) key. Strict adherence to this standard costs Microsoft money; for example, even the small 3-5% performance penalty imposed by BitLocker encryption adds up quickly when you're talking about millions of disk volumes across hundreds of thousands of servers. Microsoft believes that spending heavily on security is a wise investment, as it builds customer trust and credibility for the service. To further build credibility, they make extensive use of their products, including the various Azure and Defender security offerings.

Microsoft doesn't always provide specific details about the methods used to protect information because that could potentially undermine security by revealing too much to potential attackers. However, a reasonable amount of information, including several white papers that address the security topic in-depth, is available in the [Microsoft 365 Trust Center](#) and details of the data encryption technologies used by the different workloads [are available online](#). The completeness of the security features developed for Exchange Online and Microsoft 365 in general was enough to warrant the inclusion of Microsoft in the "leaders" section of Gartner's 2015 Magic Quadrant for Secure Email Gateways, a status Microsoft has held since.

Some of the methods used to protect data include:

- **Physical security:** Anyone who has ever visited a Microsoft data center can attest to the extremely high level of security processes and procedures that apply. Access is strictly controlled to the servers and other hardware and every action is verified and logged. Any faulty disk drives are removed and demagnetized before they are destroyed to ensure that customer data cannot be compromised.
- **Reducing the number of administrators:** Microsoft has steadily been reducing the number of employees that have persistent administrative access to applications or the servers running in the

data centers. They don't discuss the specifics often, but their goal was to make all administrative access "just in time" (JIT) so that it can be monitored and regulated. Restricting access in this manner ensures that any interaction with customer data is controlled (and audited). The so-called "Lockbox" process ensures that administrators hold zero standing permissions, which removes the problem of how to control the growth of those holding elevated permissions over time. Administrators receive just-in-time permission to perform tasks and have the permissions removed when the task is complete. All administrator access is conducted from specially secured single-purpose workstations known as [privileged access devices](#) that layer additional physical and data security capabilities on top of the existing Windows platform.

- **Extensive auditing:** Microsoft audits all access to tenant data to provide a traceable record of who accessed what data, when, and from where.
- **Data isolation:** Microsoft takes great care to ensure that data cannot leak from one tenant to another (see this document for more information about [how tenant data is isolated](#)).
- **Cloud isolation:** as described earlier, Microsoft maintains separate physical cloud instances for certain services used by government agencies. These separate instances have no infrastructure in common with the commercial instances and are protected by additional physical and personnel security measures.
- **Transport encryption:** Transport Layer Security (TLS) encryption protects information sent between Microsoft 365 data centers and clients and messages sent between Exchange Online tenants. Exchange Online also uses opportunistic TLS to negotiate secure connections with external servers. You can also create transport connectors that use TLS to protect messages sent to specific domains, such as those belonging to trusted partners. Any client, including browsers, which connect to Microsoft 365 services should use TLS 1.2. Microsoft [began to deprecate TLS 1.0 and 1.1 in 2020](#) and formally ended support for those versions in Exchange Online in October 2020, but the protocols still work, at least for now. It will take some time before Microsoft has completely removed earlier versions from all Exchange Online servers worldwide. When this happens, Exchange Online will no longer send or receive emails from servers that want to connect with the earlier versions. In the meantime, they have added a [new, opt-in endpoint](#) specifically for older clients and services that need the older versions. This page gives the technical details about the [current TLS cipher suites](#) used for encryption. Keep in mind that some devices, such as Teams Room Systems, may require additional updates from their vendors to fully support TLS 1.2.
- **Data at rest encryption:** servers and data in Microsoft 365 data centers are protected by [BitLocker](#). Protection covers both Exchange Online mailbox databases and SharePoint Online and OneDrive for Business document libraries. That means that rogue administrators cannot remove customer information and sell it to other parties or otherwise misuse the content. See [this page](#) for information about the encryption of SharePoint Online, OneDrive for Business, and Exchange Online data.
- **Customer-applied encryption:** Users can choose to protect or encrypt messages using sensitivity labels (Microsoft Information Protection) or S/MIME. To be complete, you might include features such as Data Loss Prevention, Microsoft Defender for Office 365, and information protection using sensitivity labels in the overall assessment of security capabilities. Microsoft also offers large enterprises the ability to provide their own security keys which can be used to encrypt data (known as "customer key" or "bring-your-own-key" encryption, discussed in the tenant management chapter).
- **Endpoint protection:** not only does Microsoft offer its Defender line of products as part of Microsoft 365, but they also run Defender on the servers hosting the workloads, as well as the workstations used by engineers, administrators, and support personnel. In addition, if you subscribe to Windows 365, those Microsoft desktop environments are protected automatically as well.

- **Entra ID security:** Application sign-in and authentication depend on Entra ID, which has its own set of protections. For more information, see [this whitepaper](#). In addition, features such as [Privileged Access Management](#) allow tenants to control administrative access to PowerShell cmdlets that create or edit data. Administrators must request access to specific functions and give a reason for the access. After review, the access might be approved, in which case the administrator can go ahead and execute the task.
- **Purview Customer Lockbox**, a premium feature included in Office 365 E5 that gives more customer control over access to user data like mailbox content, documents, and chats. Any time an engineer needs access to tenant data, a request appears in the Microsoft 365 admin center for a tenant administrator to review and authorize (or deny). [Customer Lockbox](#) works for Exchange Online, SharePoint Online, OneDrive for Business, [much of the Power Platform](#), Copilot, and Teams.
- **Automated configuration:** Microsoft uses the [Office 365 Desired State Configuration](#) (DSC) tool to ensure that cloud servers run known configurations and that newly added servers are correctly baselined from the start. The automated and ongoing updating of servers with new versions of the operating system and applications means that a high degree of confidence exists that known bugs are not met in production.

Against all this, it must be pointed out that Microsoft itself has suffered several major security incidents in the last few years, including the [Storm-0558 attacks](#) (a Chinese attack which targeted Microsoft customers including the US State Department) and a long-running series of attacks by the Russian federal intelligence service (codenamed [Midnight Blizzard](#)). These attacks are serious, and there may be others that haven't yet been detected or publicly disclosed. It is reasonable to ask whether Microsoft's investments in cloud security are sufficient. Despite the attacks, the answer still seems to be a qualified yes—overall, most customers will be better protected in Microsoft's cloud than they would be against equivalent threats to their own self-maintained systems. As one proof point, it's notable how many organizations were affected by the [July 2024 CrowdStrike](#) failure that bricked Windows machines running the CrowdStrike sensors. Microsoft's own operations were unaffected, which cannot be said for many of their enterprise customers. That's not an excuse for Microsoft to pause in their ongoing security efforts; if anything, they need to improve their overall security hardening and posture to mitigate the risk of future attacks.

It is critical to remember that Microsoft owns the security of the cloud resources and services that you use but *you* are still responsible for the security of your own servers, services, and users. As the world saw with the [Exchange Server "HAFNIUM"](#) and ProxyShell attacks throughout the last three years, it is *never* safe to assume that you're immune to attacks; in the case of HAFNIUM, even organizations with no on-premises mailboxes were still vulnerable as long as they maintained at least one Exchange server on-premises. Don't let the potential of a move to the cloud lead you to skimp on your security practices, procedures, or investments.

Understanding the Microsoft 365 Substrate

It is an undeniable fact of IT life that it is much easier to process data in a single repository than it is to process data drawn from several. The Microsoft 365 substrate is the single repository for user documents, emails, meetings, tasks, groups, chats, and other data held by the service. The Microsoft 365 substrate holds data generated by applications like Exchange Online, SharePoint Online, OneDrive for Business, and Teams, either by an application that uses the substrate as its primary repository or as a "digital twin" of data stored elsewhere, which is often a much smaller version holding just the information needed for search and compliance, together with a pointer to the original item.

Exchange Online mailbox databases are the physical implementation of the substrate. Exchange Online mailboxes have stored non-email application data for years. Now, the substrate creates the digital twin items

from applications like SharePoint Online, Teams, and Planner and stores the data in hidden mailbox folders. It might seem surprising that Exchange Online databases serve in this role, but the Exchange database engine (ESE) has always been good at managing many different types of data, scales very efficiently, and runs well on low-cost storage. In addition, the Exchange Online Native Data Protection model retains four copies of application data (including one lagged copy) to ensure robust data availability. ESE also supports "sharding," the ability to connect different chunks of data from different databases into a logical whole (for instance, 50 GB mailboxes are combined to form expandable archives), which makes it easy to present data on a per-user or per-tenant basis.

The existence of the substrate does not mean that applications will migrate to Exchange Online storage. Teams will continue to use Cosmos DB and SharePoint Online will continue to use Azure SQL. What the substrate does mean is that copying data from applications into digital twins stored in the substrate gives common services like Microsoft Search, [Azure AI services](#), and Microsoft 365 Copilot an integrated platform to work against.

The substrate is the essential foundation for what Microsoft 365 is today. Without the substrate, Microsoft 365 apps couldn't get to data as easily as they can, or integrate with other Microsoft 365 apps or with other services as easily as they now can. It would also be harder for apps to incorporate new technologies like Microsoft Loop components. The substrate also facilitates "graph traversal," the ability to follow information from one graph to another, such as the way that the people card can connect to the LinkedIn graph to retrieve details of a contact's career. And without the substrate, cloud applications would still be like the collection of loosely cloudified on-premises products which formed the original service.

Tenant Domains

Customers that use Microsoft 365 are tenants of the service. Each tenant occupies a subdomain within the overall Microsoft 365 infrastructure called its service domain. You can think of a tenant as the container for the company within Microsoft 365 and the domain is a sub-domain under the `onmicrosoft.com` root. For example, the Contoso company might run a tenant domain called `contoso.onmicrosoft.com`. Each user account has a separate user principal name to sign in (or connect) to applications. For instance, the user principal name `TRedmond@office365itpros.onmicrosoft.com` is an account belonging to the `office365itpros` tenant.

Tenants often have one or more domains registered in the Internet Domain Name Service (DNS) and want to continue using that domain with Microsoft 365. These domains, sometimes called vanity domains, might be part of the company branding, which is why they must remain in use. To enable this to happen, an organization can register their domains with Microsoft 365 and associate the domains with their tenant. When this happens, user accounts can have user principal names and email addresses belonging to the vanity domains, meaning that we can replace the somewhat clunky service domain addresses like `TRedmond@office365itpros.onmicrosoft.com` with the more elegant and brand-friendly `Tony.Redmond@office365itpros.com`.

Microsoft 365 does not care what name a company gives to its tenant, but you should because you can't change the name of a tenant after its creation. Any change required by corporate restructurings such as a merger, acquisition, or divestiture usually ends up in a tenant-to-tenant migration, an operation that is often expensive and long drawn out. Some flexibility in outward presence is possible by using a vanity domain for external-facing email addresses and configuring Exchange to use the domain. Other applications can surface the tenant name in different places (it's now possible to [rename the domain for SharePoint Online](#)), which means that some care and attention is necessary to ensure that the tenant name you use is the right one for your company.

Microsoft's Cloud Domains: Current Microsoft 365 services use domains like *teams.microsoft.com*, *tasks.microsoft.com*, and *outlook.office365.com*. Microsoft is moving services to a common set of sub-domains under the **cloud.microsoft** top-level domain. For example, *teams.cloud.microsoft* and *outlook.cloud.microsoft*. New services will adopt the new domain scheme while existing services will move at a still-to-be-determined time. Users won't have to make any changes as connections to the current domains will forward to the new domains.

Directories and Identities

Microsoft 365 supports both cloud-pure and hybrid (cloud/on-premises) environments. A key aspect of the support is the ability to reliably authenticate user accounts with Microsoft Entra ID and on-premises Active Directory. To enable this to happen, a variety of directories and other tools provision, store, maintain, and synchronize identities.

Microsoft Entra ID is the cornerstone of Microsoft's cloud identity story and acts as the source of authority for cloud user accounts. In hybrid deployments, where the on-premises Active Directory is always the master directory, Microsoft Entra ID synchronizes with Active Directory to form a seamless view of user accounts and configuration data drawn from both environments. The tools used for this purpose are Entra ID Connect (AAD Connect) and Cloud Sync.

Many of the applications running inside Microsoft 365 need to store information specific to their operation. For instance, Exchange Online uses EXODS, its directory store, to hold information about public folders that are not mail-enabled. These objects exist only inside Exchange Online and are irrelevant to the other workloads, so there is no reason to store information about them in Microsoft Entra ID. The same logic applies to workload-specific objects and configuration data used by SharePoint Online (SPODS) and Teams. The Identities chapter presents a comprehensive discussion about directory services within Microsoft 365 and the different forms of identities (on-premises, cloud, and hybrid).

Automation

The Microsoft 365 infrastructure uses a sophisticated workflow engine called "Central Admin" (CA) that is capable of handling more than a hundred million workflow tasks per month. The idea is to automate the common tasks needed to keep services running as much as possible to remove the possibility that human error will compromise systems. A smoothly functioning workflow engine also achieves a reliable and robust throughput of actions across the system. Developers create CA tasks as scripted workflows in either C# or PowerShell. CA is responsible for the execution of scheduled tasks to perform actions such as server deployment, database rebalancing within a DAG, and so on. More complex tasks such as the addition of new capacity to the service still require some human intelligence and planning, but the application of a structured model and great attention to detail has enabled Microsoft to reduce the time necessary to complete even very complex tasks down from weeks to days.

Microsoft standardizes server configurations whenever possible. This does not mean that each server uses the same components, as this would be impossible in an industry where components change often. Instead, it means that a server will have the same general characteristics (CPU, disk, memory) and that software is installed in the same way on all servers of a specific type. Low-cost components such as JBOD arrays allow Microsoft to increase the storage available to tenants while still being market competitive. It also means that servers are built from modules to eliminate cabling. Everything is optimized for mass production and servers are integrated into racks at the factory and shipped to the data center ready to be plugged in and brought online.

Exchange is a good example of an application where sustained engineering investment has delivered huge performance improvements and made cloud economics possible. Exchange Online uses JBOD SATA drives to deliver cost-effective storage. Using these disks implies a risk of a higher failure rate than the more expensive "enterprise-class" drives often found in corporate data centers and indeed, across Microsoft's data centers, hard disk failures are the most common event in the tens of thousands of hardware events that are handled monthly. The low cost of storage and Exchange's performance profile makes it possible for Microsoft to offer enterprise users a 100 GB mailbox quota and auto-expanding archives, and to hold a mass of non-user data (such as information about File usage) in mailboxes. Without low-cost storage, the monthly subscription to a Microsoft 365 enterprise plan would be much dearer.

Software components help to insulate users from the effect of hardware failures. For instance, Exchange's Active Manager will failover a database to a new server quickly if a disk problem is detected. It will also create a new copy of the failed database using the auto-reseed feature if replacement disks are available. Across the entire fabric, a CA workflow called "RepairBox" constantly checks for hardware failures and will open support tickets automatically if an issue is detected like a failed disk. A technician can then replace the failed disk (no attempt is made to fix the disk). The same workflow monitors servers for inconsistencies in their state to detect and fix problems with configurations.

Even with such a sophisticated and smooth-running automatic support infrastructure, some problems still occur. For instance, "stragglers" are servers that run out-of-date software versions that might deliver an inconsistent service to users. The server infrastructure is in a constant state of server refresh to introduce new software builds and new features. As such, with so many servers and so many updates, some server updates do not happen as well as they should, which is the usual reason why a straggler exists.

Networks

Given that Microsoft 365 is a set of cloud services, it should come as no surprise that the network is a precious resource. Without enough high-quality bandwidth, users will be unable to connect to services, migrations cannot transfer data from on-premises servers, and hybrid connectivity will not work. Microsoft does not control the backbone used by tenants to connect their internal networks to its services as the links making up the backbone are managed by a large set of Internet Service Providers (ISPs) around the world. Although the Internet was originally designed to survive a nuclear holocaust, local failures caused by cable problems, ISP data center issues, and hardware failure can all prevent access to services.

Microsoft cannot control the Internet, but it can control traffic flow within the network that connects its data centers. This is a dedicated and tightly controlled and monitored network. Dark fiber optical connections link the data centers to ensure maximum data flow across the network. Automatic redundancy is deployed so that a temporary outage is contained and automatically addressed. Everything that can be done to ensure that the service is maintained is done, but even so, like all cloud services, the SLA for Office 365 can only be guaranteed at the boundary of the cloud provider's data centers as defined by the edge servers that handle inbound and outbound traffic.

Monitoring, Telemetry, and Intelligence

The sheer size of Microsoft 365 and the telemetry gathered through user interaction make a colossal set of signals available to Microsoft. For example, in late 2020, Exchange Online processed more than 300 billion messages monthly. Increasingly, Microsoft applies artificial intelligence and machine learning techniques to analyze and make sense of the data. The output is used to guide choices in software engineering investment to create new functionality that surfaces in applications like Outlook (suggested replies), Viva Insights (messages that users might have forgotten to respond to), and products like Microsoft 365 Copilot and

Security Copilot. For an application like Exchange Online that's been around for a long time and is very mature, the telemetry offers insight into issues that might have lingered without ever being addressed simply because they are not a huge problem at the scale of on-premises servers but are when viewed through the lens of the cloud.

Microsoft uses a "Data Insights Engine" to process the billions of events generated hourly, aggregating and analyzing events to understand how the overall service is running and to detect problems with individual components. The general approach is that if a problem surfaces in many entities or through different signals, then it must be true. By depending on signals from multiple resources you can get close to 100% fidelity when it comes to the automatic detection of problems, or "Red Alerts" as they are known. In addition, by analyzing signals from diverse sources, engineers can focus on where the root cause of the problem is likely to be with a high degree of accuracy and this, in turn, allows the launching of automatic recovery actions with a high degree of confidence that they will fix the problem. Taking a data-driven and analytic approach to the detection and resolution of problems is key to being able to run at scale.

In addition to its signal processing engine, Microsoft uses some much simpler techniques to know when something might be going wrong. For instance, if a spike in page views occurs for the Service Health Dashboard, it might be due to customers checking the dashboard to know whether a problem exists with the service. Such a spike can often be correlated with an output from the signal processing engine but sometimes it leads to the discovery of a problem identified by human beings. Microsoft can record the characteristics of that problem as a recognizable scenario for future automatic identification and resolution. It is also important to say that signals used to identify issues are both active (those generated by specific events) and passive (those generated by servers and users during normal work). Microsoft uses a process of triangulation to spot abnormalities between the two sets that can point to a developing problem. As in all knowledge, learning how to measure the pulse of cloud operations and figure out what is normal and what's not is an evolving art that requires great dedication and ongoing observation by both automated systems and humans.

A Constant State of Change

The size and technical complexity of the Microsoft 365 ecosystem creates a unique challenge for anyone interacting with the technology. Even more challenging is the way that the ecosystem flexes and changes as different Microsoft engineering groups make software updates available to customers. At Microsoft's FY21 Q3 results briefing in April 2021, [CEO Satya Nadella said](#) that Teams added: "*over 300 features over the past year, including more than 100 new capabilities so far in 2021.*" Adding Exchange Online, SharePoint Online, OneDrive for Business, the Viva suite, Planner, Microsoft Entra ID, and Microsoft Purview solutions like Information Protection and Data Lifecycle Management to the mix means that a customer might have to cope with over 500 changes annually.

Inside Microsoft 365, applications introduce new features on an ongoing and constant basis. The changes range from tweaks to a client interface to the introduction of a completely new feature that changes the behavior of an application. This is a major difference between the traditional on-premises model where new software releases often appear on an annual release cycle that customers can then factor into carefully planned "change windows". Becoming accustomed to the pace of change in the cloud can be quite a challenge for those used to the older way of deploying software updates but it is the method employed by most major cloud services.

The best way for administrators to know what Microsoft is working on is to keep an eye on the online [Microsoft 365 Roadmap](#) (Figure 1-4), which documents planned features coming across Microsoft 365. Although the roadmap sometimes misses an update and you always must keep your eyes peeled on what

appears in the service to detect some new functionality, Microsoft refreshes the roadmap regularly and its contents are comprehensive enough to allow tenants to plan for new functionality.

Microsoft organizes the Microsoft 365 roadmap into the following sections:

- **Launched:** Features that Microsoft has deployed to all applicable customers.
- **Rolling Out:** Features that Microsoft is now deploying. As you can imagine with such a large and distributed service, it can take some weeks to deploy new software to every server running in every data center around the world. Microsoft usually posts to [the Microsoft 365 blog](#) or to [individual product blogs in the Microsoft Technical Community](#) to inform customers about new features when they begin the roll-out process. Publication is no guarantee that a new feature will show up in a specific tenant anytime soon as this depends on whether the new feature belongs to the set available in the plans the tenant uses, the length of time that the feature spends in Targeted Release (previously First Release) status, and the time taken for Microsoft to deploy the feature to all applicable tenants after the software reaches standard release status.
- **In Development:** Announced features that Microsoft is actively developing. Microsoft does not commit to delivering any of the features listed here as reasons might emerge to change or cancel a feature before any code reaches tenants.

Each roadmap item has a feature identifier (in the form *ID 561652*). You can match the feature identifier against change notifications announced in the Message Center, part of the Microsoft 365 admin center (see the tenant management chapter), where a notification includes text such as "*This message is associated with Microsoft 365 Roadmap ID 61652*". In addition, each item has a date to tell you when Microsoft added it to the roadmap, when the new functionality should be available in preview and begin to roll-out to tenants (a phase otherwise known as general availability), and when Microsoft last modified the item. The integration between Planner and the Message Center is another tool a tenant can use to track change as Microsoft introduces updates to workloads. See the Planner chapter for more information about the integration with Planner.

The screenshot shows the Microsoft 365 roadmap interface. At the top, there's a dark header with the title "Microsoft 365 roadmap". Below the header, a sub-header reads: "Get the latest updates on our best-in-class productivity apps and intelligent cloud services. Rethink productivity, streamline business processes, and protect your business with Microsoft 365." There are two buttons: "Using this roadmap" and "Roadmap improvements".

Below the sub-header, there are two search/filter sections: "Search for a specific item:" and "Filter the items below:". The "Search for a specific item:" section contains a text input with "planner" typed in and a magnifying glass icon. The "Filter the items below:" section contains dropdown menus for "Product" (set to "Planner"), "Release phase" (set to "In development"), "Platform" (set to "Windows"), "Cloud instance" (set to "Microsoft 365"), and "New or updated" (set to "New"). A "Clear all" button is also present.

Under these filters, it says "Showing 12 updates:" and provides three filter options: "4 In development" (with a grey bar icon), "1 Rolling out" (with a blue bar icon), and "7 Launched" (with a green bar icon). Each option has a brief description: "Updates that are currently in development and testing", "Updates that are beginning to roll out and are not yet available to all applicable customers", and "Fully released updates that are now generally available for applicable customers".

At the bottom, there are two dropdown menus: "Sort by Rollout date" (set to "Newest to oldest") and "Newest to oldest". Below these are three roadmap items:

- Microsoft Project: Assigned to Me view for Project tasks**: Preview Available: June 2023, Rollout Start: August 2023
- Planner : Task Email Notifications for GCC and DoD**: Rollout Start: April 2023
- Microsoft Planner: Rich text in Planner task notes**: Rollout Start: March 2023
- Microsoft 365 admin center: Send email notifications from your own domain**: Rollout Start: March

Figure 1-4: Browsing the Microsoft 365 roadmap

The Microsoft 365 roadmap gives general guidance about upcoming changes together with indicative dates. The Message Center in the Microsoft 365 admin center gives a more authoritative view of new developments applying to your tenant. Roadmap items give a glimpse into the future, but they might not be available for six months or more. Once Microsoft posts a notification about an update in the Message Center, it's more likely to appear in the following few weeks, meaning that it is time to prepare for change.

You can apply filters to the roadmap to show updates for specific products. Using filters to navigate the roadmap is useful as the sheer number of documented changes can be overwhelming at first glance. Filters also allow you to zero in on functionality that is most important to your company. This includes application-level features (for example, OneNote or Outlook), service-level features (for example, Exchange Online or SharePoint Online), and even sector capabilities (for example, features due for delivery in the Government Cloud).

The roadmap supports a download facility, meaning that you can apply filters to find the set of information you're interested in and then download details of those features to a CSV file, which you can process later with Excel or load into Power BI for further analysis.

Versions of Software: Microsoft uses a variety of methods to release software to tenants. If you configure a tenant for *standard release*, it means that tenant accounts use software that is generally available (GA). This is the most stable version of an application. *Targeted release* means that you can choose for the complete tenant or specific users to see new features sometime before Microsoft makes it generally available. The exact period depends on the app and the complexity of the feature, but it is usually between four and eight weeks. A further delay might then come into play to allow client updates to appear to support new features, especially in desktop clients. All in all, it might take 90 days between Microsoft announcing that a feature is generally available before every tenant can use the feature. Control over targeted release is through the Organization Profile tab of Org Settings in the Microsoft 365 admin center.

Some product groups run dedicated test programs (*technology adoption programs*, or TAP) to make beta software available for use in customer production environments. TAP software is a targeted release for use by selected customers. Microsoft often talks about *rings* of software releases to describe the progression from initial builds to a targeted release and finally become the standard release. Rings go from the development group (1) to Microsoft (2) to TAP (3) to release (4). Because development never ceases, the only guarantee you have is that the version of software you use today will change over time. The ever-changing nature of the service is why Microsoft calls Office 365 *evergreen software*.

Command and Control

Microsoft 365 is a massive machine that moves forward at its own pace. Thanks to the roadmap, we know a lot more about what Microsoft is working on for the future than we did in the first few years, but even so, you cannot get away from the fact that customers cede an enormous amount of control to Microsoft when they sign up for cloud services. You accept that Microsoft will deliver a wide range of functionality, but you don't get to vote on what functionality Microsoft will deliver, when users see a new feature, or when changes show up. It just happens. This is a very different experience from the careful control that most IT departments exercise over the computer systems used in-house.

Most of the time this is not a problem, and users like to find that new features continually appear. Google proved the attractiveness of an evolving interface to end users when it kept Gmail in what seemed to be a perpetual beta for many years. Even now, new features appear all the time in Gmail and Google Workspace, so Microsoft is simply keeping pace with its competition when it refreshes applications frequently.

Dealing with a rapid update cadence can be problematic in the following ways:

- **User support:** Originally, two broad categories of users existed – people who access services through desktop clients and seldom make use of browser-based applications such as Planner and those who use a browser (the third category is mobile users). In some cases, you don't have a choice because some applications only have a browser interface. Many Exchange users prefer the desktop version of Outlook because it allows them to continue working when offline. To some degree, Outlook insulates users from the ongoing changes that occur within the service. New features only appear after installing a new version of Outlook on a workstation, and even the "click-to-run" version of Outlook is slow to introduce the user interface necessary to support new functionality. On the other hand, those who use OWA to interact with Exchange Online might see new features show up on an ongoing basis. It's worth noting that Microsoft's "One Outlook" initiative intends to bring the different clients closer together, notably by allowing the Outlook desktop clients to share OWA components (this already happens with components like the calendar room finder). Every change in a user interface creates a potential flow of calls to local IT support as users seek information about why the change occurred and what it means to them. This is a very different mode of working from the normal carefully controlled and planned change management practiced by corporate IT departments. On the other hand, the Outlook desktop client is based on what is now an old architecture. More modern desktop clients, like Teams, have auto-update capabilities which means that they pick up new functionality as soon as Microsoft releases updated code.
- **Administration:** Those who manage a tenant work mostly through a set of web portals such as the Microsoft 365 admin center, SharePoint Online admin center, and Teams admin center. Microsoft updates and refreshes these portals over time to accommodate new applications and features, or for their purposes such as rebranding. In addition to the web portals, administrators can use PowerShell or Graph-based tools to manage applications. Keeping up to date with the release of these features and learning how to manage them with the available tools (also usually dependent on whatever Microsoft provides) can be a challenge for tenant administrators.
- **IT management:** The role of IT management in an on-premises environment is well understood. They accept needs and requirements from the business and work out how best to meet these requests in line with the available budget, the current IT infrastructure, and the knowledge and experience available to the company. The business will continue to generate needs and requirements and Microsoft 365 is now one of the ways that the requests can be satisfied. The big difference is that IT management must accept whatever functionality comes from cloud providers. The task of matching needs and capability is easy if a good match is available within Microsoft 365. Things become a little trickier when functionality changes because a decision to invest in an on-premises solution or to buy in software from another provider might be undermined if Microsoft decides to offer equivalent functionality inside Microsoft 365.

The issues listed above are less important to small companies than they are for large companies who tend to have well-entrenched methods to control the introduction of new technology. In the same way, new companies usually embrace new technology faster than older companies do. A further consideration comes from the employee mix, where younger employees more readily embrace rapid change than their older peers do.

Apart from preparing IT support staff with information about new changes so that they can respond to user queries, it's hard to manage how functionality flexes and changes within the service because of its rapid release cadence. One method that IT departments have used to manage the interaction between Microsoft 365 and end-users is to appoint a change coordinator. This role is to monitor changes, collect information about the changes, and make sure that the information about the changes gets to the right people in a form that makes sense to them and can be used (whenever possible) by the business to gain an advantage. The

[Microsoft 365 Roadmap](#) is a prime source of information for this person but they should not limit their scan for information to Microsoft sources. A wealth of tips and advice exists across blogs, social networks, and conferences that need to be mined to form a complete picture of what is going on within Microsoft's cloud ecosystem. And that picture has then to be placed into context with the business goals and needs of the company so that the information is best used.

Standards and Accreditations

None of the security or management practices used by Microsoft are necessarily secret, and most of them aren't rocket science. What they *are* is implemented at massive scale and with huge attention to detail—but the basic practices they use to protect and secure data in Microsoft 365 applications are well-known and can be implemented by any company (and indeed, Microsoft [documents how they handle security incidents](#)). Of course, some of the lessons Microsoft learns from their massive environment don't translate to on-premises environments, and it has to be said that Microsoft is belatedly recognizing that their cloud security has some shortcomings that they need to address.

One area where Microsoft does do something different from many of its customers is that, realizing that customers want to see independent audits proving that their cloud data is well-managed, Microsoft seeks audit-based attestations and certifications that Microsoft has earned. These certifications include:

- [ISO 27001/27002](#): Information Security Management System and Best Practice for Security Controls.
- [SSAE 16 SOC1 Type II](#): Reporting on Controls at a Services Organization.
- [NIST 800-53](#): Security and Privacy Controls for (U.S.) Federal Information Systems and Organizations., Microsoft's audit controls for Microsoft 365 are based on the NIST 800-53A (Rev. 4) special publication.
- [HIPAA](#): U.S. Health Insurance Portability and Accountability Act.
- The [HITRUST](#) Common Security Framework.

Documents describing how Microsoft meets regulatory requirements and security standards can be found in the [Service Trust Portal](#), including the latest audit reports covering Microsoft 365 and other Microsoft cloud properties. The Service Trust Portal also publishes information about how Microsoft 365 meets requirements that exist in specific geographies, such as the [European Union model clauses](#), which are "*standardized contractual clauses used in agreements between service providers and their customers to ensure that any personal data leaving the EEA will be transferred in compliance with EU data protection law and meet the requirements of the EU Data Protection Directive 95/46/EC.*"

The European Union's General Data Protection Regulation (GDPR), in use since May 2018, affects how companies active in the EU gather and handle data. More information on GDPR and how it relates to Microsoft 365 is available from [Microsoft in the service trust portal](#) and the compliance chapter. The [Microsoft Compliance Manager](#) gives customers a framework to help them organize the steps to achieve compliance with regulations like GDPR.

In addition, Microsoft sometimes seeks external proof that its applications meet the specific requirements of different industries. For instance, in the financial sector, they commissioned a [report](#) to give an independent opinion as to why the compliance features built into Microsoft 365 meet the electronic records storage, retrieval, and management requirements of rule 17a-4 of the U.S. Securities and Exchange Commission (SEC), Rule 4511 (c) of the Financial Industry Regulatory Authority (FINRA), and regulation 17 CFR of the Commodity Futures Trading Commission (CTFC).

Microsoft also requires that its suppliers meet certification standards. The [Microsoft Supplier Security and Privacy Assurance](#) program requires vendors who sell software to Microsoft to prove their adherence to

privacy and security practices. Within and outside Microsoft's ecosystem, it's important to remember that no software exists in a vacuum; many of the components that services like Exchange Online depend on should also receive external oversight and certification. For example, [Azure](#) is certified against the [ISO/IEC 27018](#) code of practice for the storage of personally identifiable information in public clouds.

Companies that need more security than the capabilities built into the Microsoft 365 applications have a wide range of options available to harden different components. [Microsoft Defender for Cloud Apps](#) is available to protect cloud applications at an extra monthly cost per user. Other companies that are active in the provision of additional security capabilities include [Mimecast](#), [ForcePoint](#), and [Proofpoint](#).

Microsoft 365 Products and Licenses

Every active user in a tenant needs licenses to access functionality, although there are a few cases where Microsoft 365 functionality is available to unlicensed users. Microsoft is closing off those holes, so it's best to adopt the attitude that licenses are necessary to use features. A tenant can buy a mixture of products and assign licenses for those products to users based on their individual needs. For example, some users might only need kiosk licenses to gain browser access to applications while others need products that include the Microsoft 365 enterprise apps and sophisticated Teams calling plans. Both sets of licenses exist quite happily within the tenant and administrators can move licenses between users based on the available license pool.

Users can access the applications available through the licenses assigned to their account when they open the [Office portal](#). The portal uses Microsoft Graph queries to display a set of recently used documents tailored for the individual user.

Three terms are important to understand when discussing Microsoft 365 products and licenses:

- **Product names** are how Microsoft refers to licenses. Office 365 E3 is a product, as is Teams Premium or Enterprise Mobility and Security E5.
- Stockkeeping units (**SKUs**) are the internal names used to manage licenses. For instance, the ENTERPRISEPACK SKU refers to Office 365 E3. SKUs also cover add-ons like Microsoft SharePoint Premium.
- **Service plans** control access to a licensed feature. You can think of a SKU as a list of service plans; you can't buy service plans individually. A complex enterprise product like Microsoft 365 E5 includes over 70 service plans. When viewing details of licenses assigned to a user account through the Microsoft 365 admin center, a service plan is called an app. In the Entra admin center, it's referred to as an enabled service.

Microsoft 365 spans many different products, each of which specifies a range of functionality available to users and administrators. Details of [the current Office 365 enterprise products](#) and [Microsoft 365 enterprise products](#) are available online. Other pages describe offerings targeted at individual professionals and small companies.

Service Families

Microsoft divides Office 365 into a set of service families, each divided into individual products sold to customers. Table 1-2 lists the service families and plans available in July 2023.

Office 365 Service Family	Available Products
Microsoft 365 Business <i>Available for up to a maximum of 300 users</i>	Microsoft 365 Business Basic Microsoft 365 Business Standard Microsoft 365 Business Premium
Enterprise	Microsoft 365 Enterprise F1 and F3 (front line workers)

<i>Available for an unlimited number of users</i>	Office 365 Enterprise E1 Office 365 Enterprise E3 Office 365 Enterprise E5
Education <i>Available for an unlimited number of users</i>	Office 365 Education (A1, A3, and A5).
Nonprofit	Office 365 Nonprofit
Government <i>Available for an unlimited number of users</i>	Office 365 Government E1 Office 365 Government E3 Office 365 Government E5 Office 365 Government F1 + F3
Sovereign Clouds	See this page for information about the plans available in China.

Table 1-2: Service Families and products

Products available in specific markets vary from country to country, as does the pricing. Sometimes differences in tax regimes drive the price charged by Microsoft in a certain country and sometimes the competitive landscape within the country is the primary influence. Customers buy products based on their appropriateness, status, and availability. For instance, you can only buy Education licenses if your organization is a recognized university or another educational establishment. Likewise, nonprofit licenses are only available to organizations that meet Microsoft's criteria to have nonprofit status. Microsoft makes education and nonprofit licenses available at a large discount compared to enterprise plans.

The Microsoft 365 Business products are for small businesses rather than large enterprises. Each includes the basic applications (Exchange Online, SharePoint Online, OneDrive for Business, Groups, and Planner). The difference between the business and enterprise plans is in the detail and depth of the functionality rather than the individual server applications. For example, if you need access to the widest range of compliance features, you need to buy Microsoft 365 enterprise because those products include that functionality. The assumption here is that individual professionals or small companies probably do not need quite the full range of compliance features.

Functionality Available in the Office 365 Enterprise Products

The effective use of the functionality included in the Office 365 enterprise products is the major subject of this book (remember, the [Microsoft 365 E3 and E5](#) products include Office 365 E3 and E5 respectively). Although E1 is the cheapest Office 365 offering, it still includes the fundamental collaboration capabilities offered by Exchange, SharePoint, and Teams. Office 365 E5 is the most expensive and includes features that every user might not need or want to use. Table 1-3 compares the services in Office 365 E1 plan against the higher-end E3 and E5 products to illustrate the difference in functionality that grows as the price increases. The obvious differences between E1 and E3 are the lack of access to the Microsoft 365 enterprise apps, and the compliance features (mailbox holds, data loss prevention, information protection, encryption, etc.). Office 365 E5 adds more automation and advanced functionality, like Office 365 Cloud App Security and Microsoft Purview eDiscovery Premium.

Feature	Enterprise E1 \$10/month	Enterprise E3 \$23/month	Enterprise E5 \$38/month
Office Online (web versions of Word, Excel, etc.)	Yes	Yes	Yes
Office for smartphones and tablets (up to 5 installs per user on PCs/Macs, tablets, and phones)	No	Yes	Yes
Microsoft 365 Apps for enterprise (the click to run Office desktop applications)	No	Yes	Yes

"Basic" Exchange email functionality (mail and calendars)	Yes	Yes	Yes
Advanced Exchange email functionality (100 GB mailbox and 1.5TB archive storage, legal hold, mailbox auditing, Data Loss Prevention)	No	Yes	Yes
Teams (conversations and audio/video meetings). See the note about the unbundling of Teams from Office 365 and Microsoft 365 subscriptions.	Yes	Yes	Yes
SharePoint Online (team sites)	Yes	Yes	Yes
OneDrive for Business File Storage and Sharing	Yes	Yes	Yes
Viva Engage Social Network	Yes	Yes	Yes
Microsoft Stream (Plan 2)	Yes	Yes	Yes
Basic management (including PowerShell)	Yes	Yes	Yes
Rolling updates	Yes	Yes	Yes
Microsoft Purview Information Protection (rights management)	No	Yes	Yes
Security and Compliance (auditing, search, eDiscovery)	Yes (*)	Yes	Yes
Viva Insights	Yes	Yes	Yes
eDiscovery Premium	No	No	Yes
Advanced data governance (auto-apply, trainable classifiers)	No	No	Yes
Data Loss Prevention (DLP)	No	Yes	Yes (including Teams)
Teams Phone system and audio conferencing	No	No	Yes
Microsoft Defender for Office 365	No (EOP)	No (EOP)	Plan 2
Office 365 Cloud App Security	No	No	Yes
FastTrack onboarding service	Yes	Yes	Yes
Workflow automation with Power Automate (Flow)	Yes	Yes	Yes
Visio web app	Yes	Yes	Yes

Table 1-3: Comparing functionality across Office 365 Enterprise

(*) = Not all functionality is available.

EOP = Exchange Online Protection is available to all tenants with Exchange Online mailboxes.

The Microsoft 365 E3 and E5 plans also include Windows 11 Enterprise and Enterprise Mobility and Security. Since the start of 2023, Microsoft has focused their attention on Microsoft 365 E3 and E5 as the base platform for new applications like the Loop app and Clipchamp Enterprise. Although Microsoft will say that they are simply adding value to Microsoft 365 E3 and E5, a cynical view of the situation is restricting new applications to these products is a none-too-subtle hint to customers that they should upgrade from cheaper Office 365 licenses. The growing functionality gap between Office 365 and Microsoft 365 means that customers need to pay attention to ensure that they have the right licenses for the functionality they need. [This page](#) gives a detailed description of the features available to different versions of Office 365 and Microsoft 365.

The unbundling of Teams: Following some complaints about uncompetitive behavior, in August 2023, Microsoft chose to unbundle Teams from Office 365 and Microsoft 365 subscriptions in the European Economic Area (EEA) and Switzerland. In April 2024, [Microsoft decided to unbundle Teams from all net new subscriptions worldwide](#). Existing subscriptions are unaffected. The decision means that new customers must purchase Teams licenses separately.

Cheaper frontline licenses are available to accommodate deskless workers or those who use a shared PC. These plans include email and web-based versions of the Office applications. Mailboxes for F3 users are smaller than other plans (2 GB) and cannot be archive-enabled. Even so, these mailboxes are large enough to meet the needs of many users. Office 365 F1 and F3 include Teams, 2 GB of OneDrive for Business storage, Planner, Viva Engage, Sway, and Stream. F3 users also get Power Automate, Power Apps, and Exchange Online.

Microsoft 365 is flexible when it comes to altering the number and type of licenses that a tenant owns. Each user has a separate license, so you can mix and match license types within a tenant. The flexibility in licensing means that you can increase or reduce capacity as the number of users grows or declines over time. It also allows you to create a customized mix of licenses in a pool for allocation to users based on their needs. For example, a company of 10,000 users might have some people who only need intermittent access to email and never join online meetings. Kiosk (front-line worker) plans might satisfy these users while the enterprise products serve other users better. Even within the enterprise, a division might exist between users who only need basic functionality and those who need the more extended variety. In some cases, the need for advanced compliance or data governance features drives the choice of Office 365 E5 or Microsoft 365 E5 while factors such as the need to replace an old PBX will convince tenants to buy add-on licenses.

Microsoft publishes [Service Descriptions](#) and [comparisons](#) to guide customers through the functionality available in its current products. As in all negotiations, before you can decide which products are right for your company, you need to understand what functionality you need now, what might be necessary for the future, and the features that you do not need. Once you know the functionality you need, you can discuss licensing requirements and pricing with Microsoft. An independent and more graphical way to view the applications available in the available plans is available in the [Periodic Table of Office 365](#).

Remember that product details change over time, even within specific features. For example, in 2019, Microsoft moved the MyAnalytics (now Viva Insights) and Stream Plan 2 features from Office 365 E5 to E3. Microsoft introduces new features and applications on an ongoing basis. The plan you settled on two years ago might not be the best now. It is sensible to use the annual subscription renewal cycle as a reminder to check the functionality offered in the various products and confirm which is best for your organization.

Adding Cost

Microsoft is not a charitable organization, and it is in its interest to sell as many licenses for its cloud services to customers as it can. The sources of added revenue for Microsoft are:

- Convincing customers to use higher-priced products. For example, getting organizations to upgrade from Office 365 E3 to Office 365 E5 benefits customers by enabling access to many compliance features. Microsoft gains by charging an extra \$15/month per user.
- Selling plan add-ons. If customers do not want to buy a higher-priced plan, they might be able to buy specific functionality through something like a license for a Purview solution like Insider Risk.
- Expanding to include other cloud services. Tenants have basic access to Microsoft Entra ID. You might like to buy premium licenses to increase the overall security of the tenant and add functionality through features such as conditional access policies, group access reviews, group expiration policies, and password write-back to an on-premises directory used in hybrid deployments. The same is true of mobile device management, which you can perform at a basic level through the ActiveSync management tools built into Exchange Online but is easier and more functional when you deploy Enterprise Mobility and Security. An alternative to buying separate plans is to upgrade to Microsoft 365 to take advantage of the bundled price for Office 365, Enterprise Mobility and Security, and Windows 11.

Buying options can increase a tenant's monthly bill by a large amount. On the other hand, if the organization needs the functionality and it enables you to decommission older systems (especially on-premises servers), then the cost might be justifiable. Office 365 products include lots of functionality but sometimes you need just a little bit more. For example, assume that Office 365 E3 is the default license for most users, but that some need Office 365 Cloud App Security (included in Office 365 E5). You could simply buy some E5 licenses and assign the licenses to those accounts, but it is sometimes possible to buy the specific feature through an add-on. If this is the case, it is usually cheaper to buy exactly what you need rather than to upgrade to the next level. To discover what add-ons are available to you, click **Purchase Services** in the **Billing** section of the Microsoft 365 admin center, which brings you to the [service catalog](#). You can then select whatever add-on you need and decide how many licenses to buy. Microsoft charges for add-ons on a per-user, per month basis. The monthly charge for an add-on varies from country to country.

Product Retirement

Microsoft does its best to create compelling solutions, but sometimes it misjudges customer demand and discovers that a product doesn't sell well. When this happens, Microsoft retires the product. This has happened many times since the advent of Office 365 with solutions like StaffHub, Outlook Boards, Kaizala, Scheduler by Cortana, and Viva Topics.

When Microsoft decides to retire a Microsoft 365 product or solution, it gives at least a year's notice to allow tenants to prepare for the deprecation. In some cases, a replacement can be found elsewhere in the Microsoft 365 ecosystem (for instance, Microsoft asserts that Copilot can replace Viva Topics). In others, no replacement exists, and users must adapt to what is available.

Enterprise Mobility and Security and Microsoft Entra ID Premium

Microsoft 365 tenants use the basic version of Microsoft Entra ID to store information about user accounts, groups, devices, and organizational settings. Although the functionality available in the version of Entra ID is enough to allow users to authenticate, participate in groups, register devices, and access apps, some organizations, especially large enterprises, pay extra to access the features exposed through Entra ID premium licenses. Entra ID P1 or P2 licenses are available separately or as part of [Microsoft Enterprise Mobility and Security](#) (EM+S). The Microsoft 365 Business Premium plan also includes Entra ID P1. Table 1-4 lists the functionality available through the EMS plans.

Enterprise Mobility and Security plans	Identity and access management	Managed mobile productivity	Information protection	Identity driven security
EMS Plan E5 (\$16.40/month)	Microsoft Entra ID P2	Microsoft Intune	Microsoft Information Protection Premium P2	Microsoft Defender for Cloud Apps
EMS Plan E3 (\$10.60/month)	Microsoft Entra ID P1	Microsoft Intune	Microsoft Information Protection P1	Microsoft Defender for Identity

Table 1-4: Functionality available in the Enterprise Mobility and Security plans

Table 1-5 lists some of the features supported by Microsoft Entra ID P1 that are usually of interest to tenants. The [full list of individual features covered by Entra ID premium licenses is available online](#). Entra ID P1 includes other features, such as [conditional access policies](#), which tenants can deploy to control inbound connections to Office 365 and other applications. The Entra ID P2 license adds identity protection and Privileged Identity Management (PIM).

Feature	Use
Enhanced multi-factor authentication	Protects other cloud workloads in addition to Office 365.
Password write-back	Enables the write-back of user passwords to an on-premises Active Directory.
Connect health	Delivers information about directory synchronization performed with Entra ID Connect (AAD Connect).
Dynamic groups	Allows groups to have dynamic membership calculated based on queries executed against Entra ID (including dynamic Microsoft 365 Groups).
Group expiration policy	Expires Groups after a predetermined period and allows group owners to renew their groups for a further period.
Advanced reports	Includes reports such as password reset activity and irregular sign-in or anomalous sign-in activity.
Assign licenses via Groups	You can achieve a basic level of automation by using Groups to assign licenses to members of those groups.
Conditional access policies	Control who can access your tenant and the conditions under which they are allowed access.
Custom security attributes	Tenants can define their own attributes to assign to Entra ID objects.

Table 1-5: Microsoft Entra ID premium features of interest to enterprise tenants

Deciding to invest in premium licenses is dependent on the value that a tenant can gain from the available functionality. Some tenants (or even some users within a tenant) will never need any of the features enabled by a specific license, some will need just one or two features, and some will use all the features. The decision to use premium licenses influences the overall cost of Microsoft 365 for an organization, so it is a factor to include in budget discussions.

Licensing Requirements for Microsoft Entra ID

As described above, some Microsoft Entra ID features need premium licenses. Microsoft says that “a [proper license is required](#) if a user benefits directly or indirectly from any feature covered by that license.” Sometimes Microsoft does not enforce a license requirement to block someone from using a feature and sometimes a partial block is in place. For example, if an administrator account has an Entra ID P1 license, they can use the Entra admin center to create dynamic Groups or define a group expiration policy. The Entra admin center enforces the license requirement by not revealing the necessary UI unless the user has the correct license. No license requirement exists in PowerShell, so administrators can use PowerShell to create dynamic groups or create a policy. It is also true that dynamic groups work even if the accounts that come within the scope of a query do not have a premium license. Microsoft could enforce the requirement at any time in the future, so it is both unwise and contrary to the licensing agreement to take advantage of any gaps you find.

Buying Through CSPs (Cloud Solution Providers)

Microsoft is not the only company that sells its licenses. You can also buy Microsoft 365 through [Microsoft cloud solution providers](#) to gain the benefit of the insight and knowledge that they have about how to deploy and use Office 365. In many countries, local resellers bundle Office 365 with other services to suit the local market. You still get the same Office 365 that Microsoft sells along with whatever added benefits the reseller can deliver. The reseller might charge an extra fee on top of the subscriptions levied by Microsoft. The question, therefore, is whether it ever makes sense to buy from a reseller.

The answer depends on exactly what added services you get for the extra fee. For instance, some resellers will take care of the entire migration process for you while others deliver a “white glove” service where they manage any support issues that occur. Dealing with cloud support can be a particularly frustrating area so

interacting with a local services company that understands how cloud support works and has direct knowledge of Microsoft 365 to help solve problems without the need for escalation can be very valuable.

Trial Tenants

Microsoft makes trial tenants available to potential customers with [Office 365 E3 or Office 365 E5 licenses](#) to try for up to 30 days without payment. This is a practical way to try out the functionality available with different products and decide which is the best fit for your company. It is also an excellent method to allow administrators to become accustomed to managing a tenant as they can make as many changes to settings as they like without running the risk of impacting users. You can transform a trial tenant into a production tenant if you want, but in most cases, it is best to start over and treat the trial as a sandbox that can be discarded when no longer needed. For this reason, never use a corporate domain name for a trial.

Developer Tenants

The Microsoft 365 Developer Program supports the work of developers who need access to Microsoft 365 to build solutions for internal use or to sell to customers. By [signing up for the developer program](#), an organization can create a fully-functional test tenant with 25 Microsoft 365 Developer E5 licenses. [Microsoft now limits development tenants](#) to organizations with an active Visual Studio Enterprise subscription. This restriction became necessary due to abuse of development tenants by attackers.

The developer tenant can be used as a general sandbox for development activity from testing code to validating performance. It's an excellent way to host application development, demos, proof of concepts, and deployment and testing of software builds. To facilitate testing, Microsoft has [sample data packs](#) to populate the tenant with test accounts and user data, but you can add your test data too.

The tenant comes with an initial 90-day subscription. If the tenant remains in use for development purposes (using tools like the SharePoint Foundation or Microsoft Graph), Microsoft automatically renews the license every 90 days to ensure that development activity can continue for as long as necessary.

Microsoft 365 Copilot

Microsoft Copilot is a framework for the development of digital assistants powered by artificial intelligence. Many Microsoft development groups use the framework to build assistants for products like Dynamics 365. Each product is trained on a set of data pertinent to the tasks that it's expected to perform. For instance, Copilot for Dynamics 365 knows how to resolve customer queries while Microsoft 365 Copilot knows how to interact with Office documents, PDFs, Teams messages, and email.

Unless otherwise stated, references to Copilot in this book are about [Microsoft 365 Copilot](#), the enterprise version designed for use with Microsoft 365 tenants that can reason over documents and emails in the Microsoft Graph. The user-facing features available in the enterprise version are also in [Copilot Pro](#), a \$20/month version designed for use in the Office apps by individuals. Copilot Pro does not include administrative features such as eDiscovery, auditing, and retention.

Generally available since November 2023, Microsoft 365 Copilot is a solution designed to help people perform everyday tasks within Microsoft 365. It combines the following:

- **Options in the Microsoft 365 applications** (Word, Excel, PowerPoint, Loop, and Outlook) for users to create prompts (requests) for assistance, like "Create a report about Project Alpha." [This page](#) illustrates some of the capabilities brought by Copilot to Microsoft 365 apps, including the Office apps, Loop, and OneDrive. It's important to realize that each Microsoft 365 application implements its own Copilot functionality with its own limitations. For instance, users need to be aware that Copilot

for Word works differently to Copilot for PowerPoint or Copilot for Excel. Copilot doesn't support all the Office 365 languages available for prompts or in apps, so language availability is [another point to check](#).

- **A semantic index** from the information stored in the tenant. A process runs in the service to collect data from the tenant and use it to create and maintain the semantic index. The semantic index is built from information stored in repositories like SharePoint Online, OneDrive for Business, Teams, and Exchange Online. Although it's not strictly required for Copilot to respond to user prompts, the semantic index helps Copilot find relevant information over and beyond the regular search for items of interest run by Microsoft Search. Organization in the semantic index is organized at both the user and tenant level. For instance, the information held about tenants lists sites and other important sources of information, while user-level information includes email, @mentions, shared file links, document extracts, and other contextual information. The combination of tenant and user information coupled with regular search results gives Copilot a rich set of grounded data to feed to the Large Language Model for processing.
- **Graph API requests** retrieve information to give Copilot additional context to respond to user prompts. Graph requests find information stored in SharePoint Online, OneDrive for Business, Exchange Online, and Teams. Microsoft 365 Copilot is only available to users with Exchange Online mailboxes.
- Tenants can develop (or buy) [Graph connectors](#) that plug into Copilot to enable access to information from other sources. The information imported through connectors is read-only and inserted into the semantic index. Tenants can also use **plug-ins** such as Teams message extensions or Power Platform connectors to enable real-time response to Copilot prompts that include external data sources.
- A **ChatGPT-4 (turbo)-based large language model (LLM)** hosted by Azure AI services tailored to resolve user prompts. Before sending information to the LLM, Copilot incorporates extra contextual information such as relevant documents retrieved from the Graph (a process called "grounding"), including data available through Graph extensions. Copilot only includes information available to the user in the prompts sent to the LLM. This can include information protected by sensitivity labels where the signed-in user has view and extract usage rights to access the content. The LLM runs on the closest data center in the tenant's region but can offload some processing to other regions when demand is high. Processing for European Union tenants stays within the European Union Data Boundary. Information transmitted in user prompts is not retained in the LLM. After processing, the LLM returns results to Copilot for further grounding before delivery to users through the requesting app.
- **An orchestration engine** to coordinate the interaction between Copilot and the LLM to refine and respond to user prompts through conversations that might require multiple interactions. The quality of the information generated by Copilot is dependent on what's available to it in Microsoft 365 repositories like SharePoint Online. As noted above, Copilot uses Graph requests to find relevant information, a process known as "grounding." Users can add context to their queries by adding up to three reference documents to a prompt. These documents must be stored in Microsoft 365. Their content is included in the grounding process before Copilot processes a prompt.
- **Microsoft 365 Copilot chat**, a web-based chat application to allow users to interact with Copilot without going through a Microsoft 365 app. Microsoft refers to this app as Biz Chat or Business Chat.

Microsoft says that Microsoft 365 Copilot works best when "*an abundance of user data*" is available for Copilot to interrogate. In practical terms, this means that to get value from Copilot, users must store their data in repositories that Microsoft Search can index. This includes information from external repositories made

available to Microsoft Search through a connector. If Microsoft Search is not allowed to include SharePoint sites and document libraries in its search results, Copilot cannot find and use that information.

Microsoft 365 Copilot is only available to accounts with an eligible product license. Currently, those licenses are:

- Enterprise: Microsoft 365 E3 and E5, Office 365 E3 and E5.
- Small to medium business: Microsoft 365 Business Standard and Premium.

In addition to an eligible base license, user accounts must have a Microsoft 365 Copilot license (\$360 annually) and user workstations must run the latest version of the Microsoft 365 enterprise apps. Some preparation work is necessary to decide [users whose activity can justify the extra cost of Copilot](#) and how the organization can measure the benefits delivered by Copilot (organizations can also [analyze workload usage data from the Graph](#) to find people who actively use the applications supported by Copilot).

Copilot Privacy and Security

Microsoft 365 Copilot retains data inside the Microsoft service boundary, meaning that it doesn't export data to any external services. It is built to meet Microsoft's existing compliance standards with EU GDPR and related data-privacy standards. All the training and grounding done with user data is guaranteed to be done in a way that continues to meet those obligations.

One common concern about Copilot is what data it can see. Copilot only shows users data they already have permission to see; a user who asks Copilot to summarize the CEO's draft remarks to the board of directors will only see that summary if the user can access the underlying documents that contain the data to be summarized. In addition, the implementations of Microsoft 365 Copilot in applications will only ingest data they have permission to see. You can control access via traditional permissions for sharing, as well as by [applying sensitivity labels](#) or using [restricted SharePoint search](#).

There are still many unknowns surrounding how Microsoft will integrate generative AI into the service. One example: before the November 2023 announcement of Copilot's general availability, it wasn't clear whether administrators would be able to allow or block access to individual applications' Copilot connections. The answer turns out to be "not exactly"; at launch, you could use the Office cloud policy service (described in the device management chapter) to turn off Copilot in Outlook, but not for other applications, and now that feature has also been removed.

Other questions remain: Will individual users be able to opt out of having their data used for training? Will there be a way to remove unwanted data from training? We'll have to wait and see.

Copilot Training

Those assigned Copilot licenses should receive training covering how to:

- Store their information in Microsoft 365 repositories to maximize its usefulness to Copilot. In practice, this means storing Office documents in SharePoint Online, OneDrive for Business, or as attachments to Exchange Online messages. Copilot can also access data drawn from third-party or tenant sources (outside Microsoft 365) through Graph connectors and add-ons.
- Avoid the possibility of "oversharing" of confidential or sensitive information. When the Delve app appeared in 2016, many tenants discovered that Delve made confidential information available to users. The fault was not in the software, which assumed that if a user had access to documents, it could highlight those documents. Instead, the fault lay in poor information management and security practices in SharePoint Online and OneDrive for Business. Lax permissions exposed information to Delve. The same could happen with Copilot, but the consequences could be more serious. While

Delve highlights documents to users, Copilot consumes documents and can include sensitive information in its output. Again, the problem is not with the software: if Copilot can access documents on behalf of a user, it can use the knowledge stored in those documents.

- Construct functional prompts to drive the interaction with Copilot and provide the AI with the context it needs to create the best possible results. Unlike the queries used to interrogate other computer systems, Copilot prompts are framed in natural language. Everyone asks questions differently, so Copilot can generate different results for what users think are the same questions. The best prompts are those that tell Copilot what the user wants to generate (for instance, "summarize the information from the Contoso proposal and their response using these documents") and the output format ("in a document of less than a page"). Microsoft has an online Copilot Lab to help users understand how to create functional and effective prompts.
- Conduct conversational interaction with the AI to refine the results into a form suitable for distribution.
- Decide whether to allow Copilot to include web content to improve its responses. Settings to control Copilot access to web content are available at tenant and user levels. When enabled, Copilot runs Bing searches to retrieve information which might end up in its responses. You can't swap Bing out and use a different search engine for Copilot searches.
- Verify and correct the output generated by Copilot to ensure that it is valid, does not contain sensitive information, and is well suited to the intended purpose.
- User education is a big part of success with Microsoft 365 Copilot. This is not just a matter of teaching people how to use Copilot in applications like Outlook, Word, and PowerPoint. It's also important to encourage a healthy suspicion of AI-generated content so that people are trained to take the time to review and correct text in Copilot responses. Skepticism is often a negative word, but it becomes a positive attribute when reviewing Copilot-generated content to make sure that hallucinations (basically, made up text that has no basis in fact or little relevance to the question asked) do not exist. Humans often accept the output of computer programs without question. They cannot afford to take a chance with AI-generated content.

Apart from trimming the information used in responses to whatever is available to the user prompting it for a response, Copilot does not apply filters to remove information that the user might consider inappropriate or unhelpful. Time is saved by the work done by Copilot to generate information. Users must dedicate part of the time saved to a careful review and possible editing of the AI output.

In addition to Microsoft 365 Copilot, tenants with the same eligible licenses can use Microsoft Copilot (previously Bing Chat Enterprise or BCE). This solution is like Microsoft 365 Chat with the big difference being that Copilot cannot access Microsoft 365 content. Instead, Copilot is limited to whatever information Bing Search can find. Despite this limitation, Copilot is a useful learning tool for people to become accustomed to interacting with AI search and the importance of well-formed prompts. Copilot can also be purchased as a \$5/user/month add-on. See the tenant management chapter for more information.

Preparing Yourself for the Cloud

Understanding Microsoft's Service Level Agreements for Online Services

Two formal documents govern the provision of Microsoft Online Services to customers. Microsoft updates both documents quarterly. [Microsoft licensing terms](#) lay out how which Microsoft delivers the service to

customers, and the [Service Level Agreement for Microsoft Online Services](#) (available in multiple languages) explains Microsoft's promises around service quality and availability.

Each of the individual workloads has its own SLA definition. For Exchange Online, Microsoft defines downtime to be "*Any period when end users are unable to send or receive emails with Outlook on the web.*" The actual calculation is a little more complex:

"The "Monthly Uptime Percentage" for a Service is calculated by the following formula:

$$\text{((User Minutes - Downtime)/User Minutes)} * 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident."

Incidents might only affect a few users, so the number of user minutes generated by an incident varies. Many incidents are transient, last just a few seconds, and are due to a temporary condition. Over a working day, micro-outages can happen five or six times without disrupting end users. These micro-outages can sometimes be detected as a failure of a page to load or a server to respond promptly. They usually resolve themselves without the need to intervene on the part of either Microsoft or the tenant administrator.

An incident that lasts several hours but only affects a small group of users (for example, in a single data center or region) will not have much effect on the overall SLA. To see any movement in the SLA, a global outage for a couple of hours needs to happen. Due to the distributed nature of the data center infrastructure, incidents usually stay constrained within a single region. Even high-profile outages that are limited to a small number of regions don't move the SLA needle very much. Indeed, a daily glance at the Service Health Dashboard will invariably show that at least one workload is currently experiencing some level of difficulty that might or might not affect your users. This is part of the joy and the pain of sharing in massive multi-tenant infrastructure.

Financially Backed SLA

If the reported Monthly Uptime Percentage falls under 99.9%, Microsoft guarantees that they will refund customers with a service credit for a set amount ranging from 25% to 100% (for less than 95% availability).

An SLA of 99.9% ("three nines" in high availability parlance) allows a service provider to have total downtime of up to 43.8 minutes per month or 8.76 hours annually. As explained above, lost minutes for Exchange Online accrue when users can't send or receive mail with OWA. For SharePoint Online, it is "*any period when users are unable to read or write any portion of a SharePoint site collection for which they have appropriate permissions.*" These conditions are in the Service Level Agreement for Microsoft Online Services.

Counting minutes for SLA calculation only happens when Microsoft records an incident and accepts responsibility for the problem. In most cases, this means that the problem must happen within a Microsoft data center due to a component that is under Microsoft's control. Anything that happens within the control of the customer, such as a misconfiguration of client software or a local network malfunction, does not count against the SLA. This is logical because Microsoft is responsible only for the parts of the service that it controls.

Microsoft is not the only cloud provider to limit SLA measurement at the boundary of its data centers. No one controls the Internet, and no one controls how data flows from your client to a data center. Many complex steps occur between a client connecting to a cloud service, perhaps using multi-factor authentication using a mobile device, to access and interact with data. It is therefore impossible for a provider to offer an SLA

guarantee as measured at the client. Well, perhaps possible because anyone can offer such an SLA, but certainly foolish in terms of their chances of ever meeting the SLA.

Microsoft excludes scheduled downtime from any SLA calculation. This is downtime that Microsoft needs to maintain its service. Customers should learn about the scheduled downtime at least five days before it happens. On the other hand, any sudden outage that comes without warning always counts against the SLA, if Microsoft accepts that their software or infrastructure caused the incident.

At any time, multiple incidents affecting Microsoft services are active across the world. Some incidents are very local and affect a single server. Some are more widespread and degrade the service delivered to large numbers of tenants or even stop an application working for those tenants. Some incidents are transient and go away on their own accord and some linger for days, albeit perhaps without affecting tenants. The point is that an infrastructure that is so large cannot run in a perfect state all the time. Because cloud software depends on hardware, software, and humans, you can be sure that something is always happening for the wrong reason. Of course, users will not care unless an incident stops them from sending emails, accessing documents, conducting a meeting, or some other operation.

In most cases, any issue that affects the SLA is soon obvious because users are unable to connect or do work. Microsoft has automated systems in place to interpret problems and map them against tenants so that the incidents highlighted in the Microsoft 365 admin center are those that might affect smooth operations for your tenant. Details of incidents appear in the Service Health Dashboard (SHD). We discuss how to use the SHD and file service incidents for your tenant in the tenant management chapter.

A summary of incidents for the last 30 days is also available in the Microsoft 365 admin center together with post-incident reports (PIRs) by going to **Service Health** and then selecting [History](#).

What is a PIR? A PIR is a Post-Incident Report with the formal analysis of an "*unplanned customer-impacting service incident*" or outage where there was a "*broad and noticeable impact across a large number of organizations*." Few incidents that you see in the Service Health Dashboard affect enough tenants for Microsoft to write and publish a PIR. When these incidents do happen, Microsoft makes PIRs available to customers through the Service Health Dashboard. The support team publishes a preliminary PIR within 48 hours of the incident closure followed up by a full and detailed PIR within five business days. A PIR includes the following sections:

- **Incident ID:** Every incident has a unique identifier. For example, EX29054 is an Exchange Online incident.
- **User Experience:** A brief description of the impact on end-users. It might be that the incident affected only administrators if the component involved is something like PowerShell.
- **Customer Impact:** What business impact (if any) the incident caused.
- **Incident Start Date and Time:** In UTC format.
- **Incident End Date and Time:** Logically, the difference between the start and end date is the incident period used to calculate the time lost against SLA.
- **Root Cause:** Microsoft's explanation of why the incident occurred.
- **Actions Taken:** A timeline of all the actions taken from the time when the incident occurred to its resolution. Sometimes several hours go by before engineers have correlated enough data from multiple tenants to be able to home in on the components that might lie at the root of the problem.
- **Next Steps:** What Microsoft proposes to do to ensure that the same problem will not recur.

As in all administrative documents, sometimes you must read between the lines to understand just what happened and why it happened. The PIR also exists in internal and "customer ready" forms, the former being much more detailed than the latter.

Social media is important to Microsoft when it comes to monitoring the service too. The sheer number of users connecting to Microsoft 365 means that any problem can quickly escalate to affect tens of millions of people. Microsoft monitors information flowing through social media to detect problems that users report (and complain about). This is just one of the ways that they try to figure out the quality of service delivered to end-users.

Seeing a tsunami of updates about a problem with an application like Teams or SharePoint Online is not a reason to panic because the problem might not affect you. Remember that Microsoft 365 uses data centers around the world. Many data centers offer local services to users in a single country. The way services run within a data center means that any problem which appears in a data center likely only affects people connected to that data center. Sometimes this isn't the case when a component running in a single location fails. For example, this happened when the [Entra ID multi-factor authentication service suffered a couple of outages in late 2018](#). As time goes by, the number of single points of failure declines within the Microsoft 365 infrastructure, but issues can still happen, as occurred with [another authentication outage in March 2021](#).

The average administrator has no real chance of understanding the data used in SLA calculations because much of it is invisible to anyone outside Microsoft. The SLA equation excludes factors such as Internet outages, local network delays, or client misconfiguration. This means that while one tenant believes they receive an excellent service measured against SLA, another tenant who experienced some problems, perhaps some of their own making, has quite a different perception of the service quality received. Beauty is in the eye of the beholder, and it is obvious that the sheer size of Microsoft 365 creates a blurring effect across its regions. Service is excellent overall (as seen in the reported SLA figures) but is awful when experienced by individual tenants affected by different bugs or operational issues.

To be fair to Microsoft, they have met their financial commitment to refund customers when the root cause for obvious outages turned out to be mistakes that were under their control. It is important to recognize that most outages are of short duration and only affect a small percentage of the overall user base.

Performance Against SLA

Microsoft reports Office 365 SLA performance [against its 99.9% target](#) every quarter. Microsoft aggregates the data for all regions to create a worldwide result and does not give SLA information for individual regions or applications. The latest published SLA figure (Q2 2024) was 99.99%. Table A-3 in the Appendix lists the quarterly SLA results for the Office 365 commercial cloud since Q1 2013. Microsoft doesn't publish SLA data for the GCC, GCC-High, or DoD clouds, nor does it publish SLA data for Office 365 China.

Microsoft usually makes SLA results available six weeks after the end of the quarter. Remember that the SLA data is a unified view generated for all the data center regions in the commercial cloud. Also, failures in some dependent services affecting Microsoft 365 do not impact the SLA. For example, several problems experienced by tenants over the years have been associated with failures in the Microsoft cloud infrastructure. Some of these failures affected the performance of Office 365 against its SLA for the relevant quarter; most did not.

Microsoft 365 and Your Network

In many respects, "the cloud" is shorthand for "the Internet." No cloud project can succeed without reliable high-speed, high-capacity connectivity to the Internet, so the most fundamental question that you must answer when considering a move to the cloud is this: can your network infrastructure cope? It is surprising just how many companies discover that they might have difficulty securing enough high-quality bandwidth given how much advertising for Internet providers floods the world, but it does happen. In these instances, all you can do is wait for the local network provider to upgrade their pipes.

Organizations that move to the cloud also often discover that their internal network infrastructure is not fit for purpose. This is quite normal. A network design created to serve the needs of an internal infrastructure where servers and clients are co-located on the same wide-area network (WAN) won't suddenly transform itself to handle completely different traffic patterns and user demand. Thus, a move to embrace Microsoft 365 is an opportunity to review your network from several perspectives.

- Is your existing internal network configured for maximum performance? For example, customers sometimes find that they have outdated or incorrect network routes that send traffic along suboptimal paths, or that their TCP or IP network settings for things like auto-negotiation aren't properly set. Before your migration starts it would be a good idea to review the underlying quality of your network. You'll want to ensure that you have the most efficient routing possible from where your clients are located to Microsoft's service "front door" locations.
- Do you need to upgrade your internal network to handle a higher volume of client traffic to Microsoft cloud services? We have already discussed the need for more bandwidth, but you also need to account for a possible increase in load caused by additional TCP/IP sessions consumed by users as they connect to Microsoft 365. A single user can consume up to 20 sessions to connect to Exchange Online, SharePoint Online, OneDrive for Business, Teams, Planner, and other services. To help, Microsoft publishes information about [network planning and performance tuning](#). Another page covers [network capacity and devices](#), including elements such as WAN accelerators. Another interesting source of information is the [Microsoft Cloud Networking for Enterprise Architects poster](#). This poster shows some of the changes in an on-premises network that tenants might need to make to support connectivity to Microsoft cloud services.
- What ports and IP ranges must be available through firewalls to allow users to connect to cloud services? To help in this task, Microsoft regularly publishes updates for the [URLs and IP address ranges](#). They offer a [web service](#) to inform customers about changes in their network, including updates to route traffic to Microsoft 365 and how to avoid latency and other network challenges.
- If you're upgrading applications as part of your move to the cloud, will those application changes themselves require additional network resources? For instance, both the cloud and desktop Microsoft 365 applications have an AutoSave feature to capture changes made to documents during editing sessions. Every AutoSave operation creates an update and syncs it to OneDrive or SharePoint Online. The save might then trigger OneDrive sync operations back to other devices.
- Do you need to make network security changes? For example, if you deploy MFA to protect Microsoft 365 applications, can you use Azure MFA to protect other applications? Is your cloud migration an appropriate time to deploy new services (such as deep packet inspection, WAN acceleration, or cloud application security improvements) or would you be better off doing those separately?

Understanding Changes in Client Traffic Patterns

Client traffic patterns change with the cloud because the target servers are no longer within the internal network. Instead, clients connect via HTTPS across the Internet to Microsoft 365 and Azure service endpoints. The outbound links that connect your company to the Internet must be able to support the new volume of traffic. The exact type of link needed varies depending on the number of clients that you expect to be active at any time, the type of clients, and the cloud services they will access. Although Microsoft has created a large network of local front-end points of connection (or "edge nodes") to speed traffic to its data centers, unless the link from your company locations to Microsoft's network can carry the amount of traffic your users generate, they will not be able to work as well as they should. Once traffic enters Microsoft's network, it is carried across fiber to its destination data center. Microsoft's cloud network, including other services like Azure, spans enough fiber to stretch to the moon and back three times. The combination of edge nodes and

fiber networks means that it is usually possible to make a fast connection to Microsoft's network, wherever you are in the world. That is, if your local or last-mile connection can carry the traffic.

Microsoft maintains [a flashy interactive model](#) of their network that shows data flows, renewable energy generators, Azure and Microsoft 365 data centers, and network points of presence, with each type of item clickable so that you can get more information on specific items.

If you run on-premises servers today, you probably have some data to show how much network bandwidth applications and users consume. One rule of thumb is to double (some say triple) this figure and use that amount as the basis for planning. Advice and guidance on this topic have evolved over time as cloud services change and knowledge increases, so it is best to ask Microsoft or an experienced consulting company for their recommendation as to the capacity you need – and to then add 30% or so to cater for growth in user demand and to accommodate new applications and features which affect usage patterns and consumption. It is therefore important to keep an eye on changing demand over time.

If this seems like an unnecessarily high increase in bandwidth, consider the experience of companies that deployed Teams for voice and video calling before the COVID-19 pandemic—Microsoft has worked very hard to optimize the codecs used in the service, but users have been so eager to adopt these communication methods that average bandwidth consumption at every customer I've worked with since Teams' debut in 2017 has gone up significantly year-over-year, over and above increases in employee count. Organizations that moved rapidly to telework because of COVID-19 often have legacy VPN systems, and people who are used to them; if your users VPN into the corporate network and then connect to Microsoft 365 services, both your network and your users will suffer poor performance—split tunneling (described in the client management chapter) will help with this. If you have a consolidated network where traffic is backhauled from remote offices to a central location, you should also investigate providing a separate link per location. This will deliver better performance and uptime.

Remember that moving to the cloud will not make a bad internal network any better. In fact, if users rapidly adopt new cloud applications (especially features that use more bandwidth, such as video conferencing), you may see a disproportionate impact on your overall network quality. If that network is barely able to cope with the demands of on-premises client-server connections, it will do no better and is likely to do worse when cloud services take over.

During the migration period, the volume of network traffic will be higher than normal because of the need to move information like mailbox data and documents to the cloud. After the migration period is over, network demand should settle into a more predictable load. There will be peaks and valleys in demand, but you should be soon well acquainted with the general shape of network demand for each of your company's locations and be able to make whatever changes are necessary.

What About ExpressRoute?

Azure ExpressRoute is a dedicated MPLS network connection between your internal network and Microsoft. Although this might sound like a great way to improve connection speed and performance, Microsoft [recommends against using ExpressRoute for Microsoft 365](#), and they won't let you configure it unless you're able to persuade them that you should be granted permission. If you think you might need it, read their [service guide](#) first for more details.

What about Informed Network Routing?

Software-defined network (SD-WAN) solutions have become increasingly common in large enterprises because of their flexibility and capability. Instead of using a fixed network configuration, SD-WAN solutions can be reconfigured, often automatically, to adjust to changes in loading, network damage or outages, or

changing requirements. If you deploy SD-WAN solutions, special devices known as SD-WAN [controllers](#) aggregate usage and quality data and use it to push configuration changes to the network.

Microsoft added limited support for SD-WAN integration through a feature they call [Informed Network Routing](#). If you have compatible equipment (currently limited to Cisco IOS XE), and are using the commercial version of the Microsoft 365 cloud, you can enable performance and network quality data from Office 365 to be funneled to your SD-WAN controllers so that your network will dynamically adapt to changes or problems with the network. This is a promising technology, but in practice, it's still too limited to be useful to most of us. It requires equipment from a specific vendor, and you won't get any real benefit from the feature unless your network has multiple redundant paths to the Internet—if you only have one route to the service in the first place, the adaptive nature of SD-WAN can't do much for you. However, as with many other high-end enterprise technologies, as SD-WAN becomes less expensive and more widely deployed, it may add value to your network.

Planning for Different Types of Network Traffic

When you plan for new network capacity, make sure that you accommodate four types of traffic that may be required *de novo* as part of your upgrade:

- **User connections to the new cloud environment plus existing work.** Remember that users often make use of company networks to access external social sites such as Facebook and Twitter during work hours. You can try to restrict this access but, in many cases, this is like pushing water uphill, so it is best to include a certain overhead for personal network activity. Different clients often have different network characteristics. For example, Outlook desktop clients consume more bandwidth than OWA. As explained in the Teams calling and devices chapter, Teams voice and video conversations are sensitive to network conditions and need certain basic capabilities to be able to function. Microsoft has [network calculators for Teams and Exchange](#) that help assess likely demand (further information is available [here](#)).
- **Migration of user data to the cloud.** You might be able to move 500 users in a single cutover operation during one weekend—but migrating 50,000 users will probably take a little longer. In either case, you'll be moving data from your internal network across the Internet to a Microsoft data center. Depending on how much data is involved and the available throughput from your network to Microsoft, that movement could take longer than you think. It's also worth considering the impact of where your Office 365 tenant is homed; it's entirely possible, based on its usage location, that you will be migrating data from a physical data center in one country or region to an Office 365 data center in a completely different part of the world. For example, consider a US company that creates a tenant (homed in the US) to consolidate its worldwide operations. As it migrates data from its regional data centers in the UK, EU, and Australia, much of that data will end up by default in US data centers, meaning it must transit from its original location across at least one ocean.
- **Client updates.** The way that Office desktop applications are updated in Office 365 may be different than the way you've upgraded them in the past. Because the default state is to let every device fetch updates whenever it wants to, you may find that your client OS and application updates consume more bandwidth (or at least consume it in different patterns) than they did when you used centralized updates.
- **Administration operations.** Intelligent applications like Outlook isolate users from the effect of network outages and allow them to work offline. All Microsoft 365 administrative operations occur online, and a reliable (and fast) network connection is necessary if you want to be sure that administration can be performed without difficulty.

You should also keep in mind that Microsoft has gone through a lot of effort to categorize its network endpoints according to the network priority they should receive; see Chapter 15 for more on how you can work with these categories to prioritize the most important client-facing network traffic to Microsoft's data centers.

The Commercial Success of the Microsoft Cloud

Only Microsoft knows the details of how successful its cloud services are and how many paid subscribers each service has. This is commercially sensitive data, and it should come as no surprise that they reveal as little real data about the numbers as they possibly can. Commercial Cloud is an artificial mixture of revenue derived from different Microsoft cloud services including Office 365, Azure, Dynamics 365, and LinkedIn. It is not one of the formal business segments Microsoft uses to report results like Intelligent Cloud or Productivity and Business Processes. Nevertheless, the number reported for commercial cloud revenues (now referred to as the Microsoft Cloud) is useful because Microsoft has reported comparable data for several years.

Microsoft Cloud Revenues

Much of the early growth for Office 365 (2011-2015) came from small to medium business companies that moved from on-premises to the cloud. Today, even the largest enterprises are comfortable with the security, privacy, and operational aspects of cloud services. The growth rate for Office 365 has slowed over the years, but still reflects a continuing movement of work from on-premises systems to the cloud. Today, annualized revenue for the Microsoft Cloud, a large percentage of which comes from Office 365, is a major contributor to Microsoft's overall income. Although Azure continues to grow faster than Office 365, the higher prices customers pay for Office 365 subscriptions (computed by Microsoft as the ARPU, average revenue per user) and the number of Office 365 users mean that Office 365 represents a large part of the Microsoft Cloud revenue mix. Some estimates put the revenue generated by Office 365 annually at around \$60 billion. Importantly, the revenue comes with a healthy gross margin (reported by CFO Amy Hood to be 69% for Microsoft Cloud in Microsoft's FY24 Q4 earnings call).

In its FY16 Q4 results, Microsoft reported that its annualized revenue run rate (ARR) for commercial cloud products [had reached \\$12.1 billion](#). Fifteen months later, when they announced their FY18 Q1 results (October 2017), Microsoft said that the run rate was \$20.4 billion, a remarkable jump of \$8.3 billion over five quarters which comfortably allowed CEO Satya Nadella to attain the goal of \$20 billion set in 2015. To calculate the annualized run rate, Microsoft takes the result achieved in the last month of a reporting period and multiples it by 12. In July 2023, Microsoft reported \$36.8 billion revenues for the Microsoft Cloud, which equates to an annualized run rate (ARR) of \$147.2 billion. The actual Microsoft Cloud revenue for their 2024 fiscal year was \$137.4 billion, but because Microsoft books varying numbers of customer projects over a year, a difference always exists between the actual revenue achieved in a year and the ARR. Nevertheless, the headline figure used for ongoing comparison is the ARR.

Microsoft attempts to increase ARPU by moving subscribers to higher-priced plans or by selling add-ons to license additional features. To encourage customers to upgrade, Microsoft restricts access to many new features, especially in the areas of compliance and security, to tenants with high-end licenses. The importance of driving an increase in ARPU is illustrated by the [revelation by Microsoft's CFO](#) that in FY20 the E5 SKUs contributed \$7.5 billion in revenue, even though only 5% of the Office 365 user base had these licenses, an increase from the \$4.2 billion recorded in FY19. In July 2022, Microsoft said that 12% of the Office 365 installed base held Office 365 E5 licenses but didn't give a new figure for how much this contributed to overall Microsoft Cloud revenues. See Table A-1 in the Appendix for a full list of quarterly revenue results from April 2015 to now.

At the time of writing, Office 365 is available in [249 markets and 44 languages](#). It is probably easier to list the places where Office 365 is *not* available: Cuba, Iran, Democratic People's Republic of Korea, Sudan, and Syria.

Price Increases: In March 2022, Microsoft increased [the cost for Office 365 and Microsoft 365 products](#).

For example, both Office 365 E3 and E5 increased by \$3/month. Microsoft justified the price increases because of the new Office 365 apps added since 2011, the volume of individual changes made in that period, the use of artificial intelligence and machine learning to automate processing for organizations and users, and the introduction of better security and compliance functionality. Some will be more convinced than others, with doubters pointing to Microsoft's need to continue growing cloud revenues to please Wall Street as a more likely driving force. The price increase did not affect Office 365/Microsoft 365 academic and personal products.

Growth in Usage

The increase in Office 365 users is in line with the growth in revenues. Microsoft uses a concept called *monthly active users* to report usage. This number is not the total number of licenses sold to customers. Instead, it reflects those who have licenses who log on and use the service at least once a month (which is not much for anyone using any of the applications). A definition of what monthly active users are for a workload is:

The maximum daily users performing an intentional action in the last 28-day period across the desktop client, mobile client, and web client.

Intentional action is something that a user does to perform some measurable activity, like creating and sending a message or scheduling a meeting. For SharePoint Online, countable operations are things like uploading or editing a document, while counted actions in Teams clients include attending an online meeting or starting a chat. The definition of an active user does not count actions like starting or exiting an app. Signals captured in the Microsoft Graph record user actions. The data is deduplicated based on user identifiers (the GUID for user accounts) to eliminate the possibility of counting users twice.

The number of active users reported by Microsoft understates the total usage because it does not include accounts that Microsoft has provisioned for tenants which are not yet in active use, free accounts (such as Microsoft's use of the Service), and trial domains. The numbers are even higher if we speak about mailboxes instead of accounts. The number of cloud mailboxes is considerably higher than the number of cloud user accounts because of shared mailboxes, inactive mailboxes, resource mailboxes, and group mailboxes.

The latest number reported by Microsoft for paid Office 365 paid seats is "over 400 million" (January 2024). Given that customers have paid for some seats that are not yet assigned to users, the number of active users today is possibly a little lower. You can add a few extra million free seats (used by Microsoft and their partners) to this number. Table A-2 in the Appendix details the growth in Office 365 users since November 2015.

Workload-Specific Usage

When it reports overall Office 365 numbers, Microsoft doesn't break the data down by workload and seldom gives precise numbers for individual workloads. What numbers are given appear sporadically. For instance, in November 2019, Microsoft said that SharePoint Online has 100 million monthly active users; they updated the number for [SharePoint Online to 200 million in December 2020](#), but haven't said much about SharePoint Online users since. Much of the increase in SharePoint usage comes from Teams. Every team has a SharePoint team site, and Teams stores shared files and recordings of Teams meetings in SharePoint Online and OneDrive for Business. In October 2023, Microsoft said that Teams has 320 million monthly active users but does not break out how many of these users are commercial, personal, or educational. Each of the Teams users is probably a SharePoint Online user too.

Given that a very high percentage of active Office 365 users have an Exchange Online mailbox, it's reasonable to assert that Exchange Online is the largest workload and that Exchange Online is hugely influential on the overall success of Office 365. In 2017, Microsoft said that Exchange Online alone handles about 60 billion requests per day from all connected clients (many people use more than one client, and each client handles multiple transactions). As documented in the Exchange Online chapter, the volume of work handled by Exchange Online continues to grow.

Other products benefit from the consistent growth in Office 365. In their FY24 Q1 results briefing, Microsoft revealed that Enterprise Mobility and Security has 259 million users (an increase of 32 million users in a year). Microsoft often sells EMS to enterprises along with Office 365 (standalone or as part of Microsoft 365), which points to high penetration of EMS in Office 365 enterprise tenants. In [July 2023](#), Microsoft said that Microsoft Entra ID had 610 million monthly active users (eighteen months prior, the reported number was 425 million monthly active users). Previously, Microsoft said that over 200,000 organizations pay to use Entra ID. It's worth remembering that among the 90 billion sign-in events handled daily by Azure, many come from non-Microsoft applications like WorkDay and ServiceNow which use Entra ID as their directory of record. An indication of the revenue flowing into Microsoft from products associated with Office 365 comes from the assertion that the Microsoft security business surpassed annual revenue of \$20 billion in January 2023. The security business includes products like Purview, Entra, Intune, Sentinel, and Defender, all commonly found in Microsoft 365 tenants.

Leveraging the Breadth of Office 365

When Microsoft CEO Satya Nadella told the audience at the October 2014 Gartner conference that "*Office 365 is the new Exchange and one will cannibalize the other. The key is to ensure that current Exchange customers can transition on their own terms,*" he reflected the reality that many customers selected email as the first workload to move into the cloud. The reason why he called Office 365 "the new Exchange" is that the movement of email into the cloud mimicked the movement of email from expensive mainframe and minicomputers to PC-based Windows NT servers from 1996 onward. Exchange Server was the first Windows server application capable of scaling to deliver the kind of email service needed by the world's largest corporations.

Email is a big reason why many companies decide to move their workloads to the cloud, but what of the other cloud applications? After all, you pay for these applications alongside Exchange, so it is wasteful if you do not seek to take advantage of them. Any plan to migrate should consider what advantages a company can derive from the full spectrum of Microsoft 365 rather than applying a narrow email-centric focus. Here are the services that round things out:

- **SharePoint Online:** While organizations were initially slow to move on-premises SharePoint deployments to SharePoint Online, that point is long past and SharePoint Online now boasts over 200 million daily active users. The mission of SharePoint Online is different from the way organizations often deploy the on-premises variant. SharePoint Online is the document management service for Microsoft 365 applications and is closely integrated with many apps including Teams and Planner.
- **OneDrive for Business:** OneDrive for Business is core to enabling people to work offline or across low-bandwidth environments. Its synchronization client uses differential synchronization to deal with files of up to 250 GB stored in SharePoint Online or personal OneDrive for Business accounts. Microsoft provides large quantities of OneDrive storage to Microsoft 365 users with enterprise accounts to allow them to move files traditionally kept on local PCs to the cloud.

- **Teams** offers a chat-based workspace for users to work together with audio and video calling, federated communications with Skype consumer users, an application platform, and a replacement for traditional phone systems.
- **Stream** provides video recording and consumption services to applications. See the Managing video chapter for information about managing video content.
- **Planner** focuses on task-based planning for team activities.
- **Viva**: Microsoft bought Yammer in July 2012 to acquire its enterprise social networking technology and renamed Yammer to be Viva Engage in February 2023. They have introduced a number of other employee engagement and management services under the Viva brand, including [Viva Goals](#) for goal and objective tracking and [Viva Amplify](#) for managing corporate communications.

Perhaps the most interesting thing that has happened since the introduction of Office 365 is how the barriers that existed between on-premises applications disappear when Microsoft has total control of deployment and operations. Relatively few on-premises environments successfully integrate SharePoint and Exchange, but the configuration and operational difficulties go away with the cloud versions. Microsoft takes advantage of this to build new applications that exploit Exchange Online for email and calendaring and SharePoint Online for document management, adding whatever extra software is necessary to complete the picture. Teams and Planner are examples of new applications that could not exist on-premises. Both are unique to the cloud.

If the right licenses are in place, all this functionality is available to tenants. Many companies plan to move to the cloud for a specific purpose and can benefit even more by exploiting the other technologies mentioned above. The best thing is that Microsoft takes care of all the work to deploy and manage the technology, meaning that the normal learning curve needed to master the details of capacity planning, server deployment, and application configuration and installation is not necessary. All efforts can focus on the question of how best to use the features available through SharePoint Online, Teams, Planner, and other applications to solve business problems.

Like any migration, the transition from on-premises servers to their cloud equivalents are projects that benefit greatly from experience. If you don't have the necessary expertise within the company, you should find some experienced consultants to help you plan for and execute the change.

Chapter 2: Managing Identities

Brian Desmond

Your online identity, and by extension the authentication process that establishes the identity, is the cornerstone of security in Microsoft 365. Once a user or workload identity is successfully authenticated by Microsoft Entra ID (rebranded from Azure Active Directory in July 2023), access to any authorized resource is granted. Throughout the book, we distinguish between two separate processes:

- *Authentication* is when a system verifies the identity of a user. For example, the familiar Windows logon process you go through is how Windows authenticates your domain or local user account.
- *Authorization* is when a system decides whether a specific user or workload identity should have access to an object or service.

In its simplest form, the Microsoft 365 authentication process needs an identity, represented by the combination of a User Principal Name (UPN) and something by which their identity can be confirmed. Often the authentication method is a password, but it can also be a specific device such as a FIDO2 token, a biometric mechanism such as Windows Hello for Business, a certificate, or a combination of several methods (also referred to as multi-factor authentication, or MFA). Once Entra ID has confirmed a user's identity, it returns an artifact that an application or service can accept as proof of identity.

Although the default identity and authentication options suit most customers, not all organizations have equal security requirements. Nonetheless, protecting your (digital) identity is an important task; both inside and outside Microsoft 365. After all, once someone can gain access to your account, they hold "the key to your kingdom", granting them access to all the data accessible within the boundaries of your identity. To meet the need for stricter security policies dealing with authentication, Entra ID supports a plethora of options to customize and further secure the authentication process, as discussed here.

Because identities and authentication touch on so many aspects of Microsoft 365, it is important to carefully consider the implications of the various identity models and authentication options. The importance of factors such as complexity and cost differ across organizations and can greatly influence the decision as to which solution is best for you.

In this chapter, we explore the various authentication options that are available to you, spanning both cloud-only and hybrid deployments. As you will see, a robust identity infrastructure is fundamental to a successful deployment. Before exploring the available options, we should first look at the Entra ID infrastructure which supports both identities and authentication for Microsoft online services.

The Role of Entra ID

All the Microsoft 365 workloads depend on Entra ID for identity and directory information. Entra ID provides authentication and authorization for Microsoft 365 workloads as well as third-party applications. Entra ID has few other similarities to traditional on-premises AD. Entra ID is one component of Microsoft's Entra family of products and services.

Entra is the umbrella Microsoft has organized its identity and access management solutions under and Entra ID is the flagship component. In addition to Entra ID, Entra includes a [cloud infrastructure entitlement](#)

[management \(CIEM\) offering](#) for managing permissions across cloud providers and [Entra Verified ID](#), a decentralized identity issuer. To support the Entra brand and provide a consistent experience for identity administrators, A dedicated Microsoft Entra admin center is accessible at <https://entra.microsoft.com>. The Entra admin center unifies administrative access to Entra ID, Entra External Identities, Entra Verified ID, and Entra Permissions Management.

Since Entra ID is a cloud service, there are significant differences between how on-premises workloads like Exchange Server or SharePoint Server use on-premises Active Directory (AD) when compared to how cloud apps interact with Entra ID. Some workloads, like Exchange Online, implement workload-specific directories behind the scenes to bridge this gap. Entra ID is, like most cloud implementations, designed to be a highly available multi-tier, multi-tenant service capable of handling load at an immense scale.

Every Microsoft 365 tenant has a corresponding instance within Entra ID, and each instance is isolated from others so that no tenant has access to data belonging to another tenant. When you create a new tenant, Entra ID creates a new instance for that tenant. The Entra ID instance is not licensed separately, and you do not pay anything extra for it. As you add users and groups, those objects go into this Entra ID instance.

Entra ID is deployed in multiple Microsoft data centers around the world and [operated with a service level agreement](#) (SLA) of 99.99%. In addition to Microsoft 365, Other Microsoft cloud services like Microsoft Dynamics 365 and Microsoft Intune consume Entra ID, as do numerous third-party applications. Microsoft has made significant investments in Entra ID to offer a 99.99% SLA. As with any cloud service, Office 365 has suffered from large-scale outages on occasion, and in some cases, an Entra ID issue was the root cause of the outage. You can even [see how your tenant performs](#) against the SLA in the Admin center.

To address the problems caused by transient outages, Entra ID includes a [Backup Authentication Service](#) (BAS) that automatically steps into action to process authentication requests from supported applications if the primary service is unavailable. To do this, the BAS caches successful authentication requests for three days. The BAS relies on features such as continuous access evaluation and conditional access (discussed later) to deliver resilience in a secure and configurable manner.

Like other cloud services, Microsoft updates Entra ID regularly to introduce new features and improve quality. See the [Entra ID release notes](#) for details.

Workload-Specific Directories

Because of the way that some workloads work, Entra ID cannot offer the necessary functionality to support all the features required by those services. For example, the mailbox-specific attributes used by Exchange Online are not all stored in Entra ID. The same is true for many of the user profile properties used by SharePoint Online. To support workload-specific needs, and to isolate the configuration and other data owned by a single tenant inside the multi-directory Entra ID architecture, some services add another layer on top of Entra ID. This layer is a workload-specific directory store and is named after the workload:

- Exchange Online Directory Services (EXODS).
- SharePoint Online Directory Services (SPODS).
- Viva Engage (Yammer) Directory.

This workload-specific directory is essentially a cache of information held in Entra ID combined with workload-specific information. Some of the objects stored in the workload directories are linked to objects in the tenant's Entra ID instance. The workload-specific directory is designed to deliver a certain level of redundancy against network or other disruptions. To further explain the concept of workload-specific directory stores, we can use Exchange Online as an example.

Exchange Online Directory Services

Exchange Online uses EXODS to hold its configuration data, including information about mail-enabled recipients and other Exchange objects, like public folders or the mail user objects for guest accounts. Exchange Online deploys its service across multiple forests with tenants divided between the forests. Each forest is unique to a data center region (multi-geo tenants spread mail-enabled objects across multiple forests) and uses an instance of EXODS together with a synchronization endpoint that is used to replicate information with the directories used by Microsoft 365 (for user accounts and licensing), other applications (like SharePoint for mailbox information used in eDiscovery), and Entra ID. The introduction of support for spreading a single tenant's data across multiple data center regions means that Microsoft has made additional changes to the way these forests are structured and synchronized so that all locations where a tenant's data may exist have complete and consistent data.

Synchronization occurs across the directories on an ongoing and continuous basis to ensure that the latest information is always available to all workloads. Occasionally, glitches can happen with the synchronization process, and you might have to wait for a new user account to be visible.

Exchange Online can create new user accounts during the mailbox creation process. In this case, Exchange Online pushes the information about the new account to the EXODS and Entra ID [in parallel](#). Exchange Online is unique in this capability. When on-premises identities synchronize with Entra ID via the directory synchronization process in hybrid deployments, Entra ID is the target, and the resulting objects will synchronize to EXODS afterward.

Entra ID Licensing

Every tenant includes a free version of Entra ID that provides all the core functionality necessary to use Microsoft 365 services. For many organizations, the core capabilities of Entra ID are not enough to meet security requirements in the context of today's cyber threats. Microsoft bundles many of the security features that today's organizations require into various licenses, including Entra ID P1 and P2 and Entra Suite. You can purchase Entra ID licenses on an a-la-carte basis, or use the licenses bundled in the Enterprise Mobility + Security (EMS) and Microsoft 365 enterprise and business premium SKUs. Microsoft also makes paid features for external identities, identity governance, workload identities, and network access available on an additive basis in addition to Entra ID P1 and P2 as part of the Entra Suite.

For many organizations, Entra ID P1 is enough, but Entra ID P2 brings a set of governance tools and risk-based controls that can dynamically enforce security policies based on Microsoft's determination of the risk factor of each user and their sign-in attempt. Entra Suite includes Entra ID P2 as well as additional security and assurance capabilities. These include Entra Internet Access, Entra Private Access, and Entra ID Governance. Entra Internet Access and Entra Private access are part of Microsoft's Secure Service Edge (SSE) offering. You can use Entra Internet Access to apply policy to every Internet connection a user makes. With Entra Private Access you can connect users to traditional on-premises applications (web based or otherwise) without a virtual private network (VPN). Entra ID Governance extends access governance capabilities in Entra ID P2 and brings lifecycle workflows that allow you to automate identity processes for joiner, mover, and leaver scenarios.

A comparison of the different types of Entra ID licenses is available [online](#). Throughout this chapter, we call out whether a capability requires a paid version of Entra ID. Unless otherwise noted, you can assume that Entra ID P1 is sufficient.

Administrators can track the consumption of Entra ID Premium licenses by accessing the License Utilization dashboard in **Monitoring & health > Usage & insights** in the Entra admin center. The data is also available via the [Graph API](#) for programmatic reporting.

Licensing Guest Accounts

Guest users (external users whose account and credentials exist outside your tenant) need rights to use Entra ID P1 functionality too. Microsoft's billing model for external identities (including guest accounts) uses telemetry to measure the number of unique identities that access paid Entra ID features monthly. Microsoft does not charge for the first 50,000 active external identities measured in a month and the charge thereafter is small. For instance, access to Entra ID P1 features incurs a charge of \$0.00325 per month for each active external identities past the 50,000 monthly threshold.

An Entra ID tenant must link to a valid Azure subscription through the External Identities section of the Entra admin center to support billing for external identities. Before doing this, you must create an Azure subscription or use an existing one linked to your Entra ID tenant and create a resource group to use for billing.

Microsoft charges for each SMS-based multi-factor authentication request processed for an external identity. The charge levied pays for the telephony fees and is \$0.03 per attempt (successful or not). The charge does not apply when external identities use the Microsoft Authenticator app for MFA.

Although Microsoft does not currently enforce licensing restrictions for guest users, it is important to make sure that your licensing plans take this point into account if you deploy applications that support guest accounts, like Microsoft 365 Groups, Teams, and Planner. See [this guide](#) for more information.

Identity Architectures

There are two options for how you create Entra ID user accounts (also referred to as "identities"):

- **Standalone identity:** In this model, user accounts exist only within the cloud environment and are not linked or related to an AD forest. This means that a user may (or may not) have an account in an on-premises AD, as well as an account in the Entra ID tenant that supports the organization's tenant. The accounts may happen to have the same username and password, as well as other attributes, but are separate and independent objects, and need to be managed independently as well. This duplicates administrative effort and introduces risks if attributes conflict or are not maintained correctly. Some organizations use standalone identities for users that do not require an account in their on-premises AD, such as third-party vendors. Using standalone identities to isolate privileged accounts in Entra ID from on-premises AD is also a good security practice.
- **Hybrid identity:** In this model, user accounts are created and managed in the on-premises AD environment and subsequently synchronized to Entra ID. Entra Connect or Entra Connect Cloud Sync performs the synchronization. In the hybrid identity model, the on-premises AD forest is the "source of authority" for most objects, with objects and attributes replicating from on-premises to the cloud. Because the on-premises AD is now the source of authority, an administrator can only change limited aspects of synchronized identities in Entra ID.

Each approach has its pros and cons. For example, standalone identities are convenient because they do not need an on-premises AD. Many small organizations do not have or want to operate an on-premises AD and larger organizations are planning for a future without on-premises AD. However, if an on-premises AD exists, standalone identities can be more time-consuming to manage because organizations must manage two separate accounts for each user. There is no arbitrary threshold for how many user objects you should have before synchronizing identities makes more sense. It typically comes down to how much time and effort an administrator must put into managing dual identities versus maintaining a synchronization infrastructure.

Hybrid identities simplify administration because all changes occur to the on-premises AD and are then synchronized to the cloud by Entra Connect. The hybrid identity model doesn't prevent you from creating and using standalone identities.

You can deploy a mixture of the two models. For example, you may need to provide customers or contractors with access to certain resources. Using standalone identities for these users and hybrid identities for employees allows you to isolate the on-premises environment from customers and contractors. Ultimately, the decision about which identity model to use is driven by the business and technical requirements of the organization.

You can optionally add identity federation to your hybrid identity design. Federation gives organizations much greater control over how to enforce security policies such as logon hours, third-party multi-factor authentication, and network locations from which users can access cloud resources. Most of the additional controls that federation offers are also available natively in Entra ID if you have Entra ID P1 or P2. It is critical to remember that the identity federation infrastructure must scale to meet performance and workload requirements. It must also be secure, highly available, and resilient to failure because Entra ID may not be able to authenticate user logins if the federation service is unavailable.

Hybrid Identity Authentication Infrastructure

Even after you have synchronized your identities to the cloud, your users will still need a way to authenticate. In a hybrid identity model, there are three ways to do this:

- **Password hash synchronization:** In this model, a cryptographic hash of the user's password, but not the password itself, is synchronized to the cloud. The hashing process is discussed in detail later. When a user requests access to a service component, the password they provide is hashed in Entra ID; if that hash matches the stored hash, the passwords are considered to match. This process relies on directory synchronization but does not require any other servers or components. Combined with Seamless Single Sign-On, hybrid Entra join, or Entra join (discussed later) you can achieve single sign-on (SSO) with password hash synchronization.
- **Pass-through authentication (PTA):** In this model, authentication requests from the service are sent to a queue, where they are retrieved by a small agent that is installed by Entra Connect. The agent validates passwords against the on-premises domain controller (DC) and returns a status (success, failure, password expired, or user locked out) to Entra ID. Like password hash synchronization, PTA can be combined with Seamless SSO, hybrid Entra join, or Entra join.
- **Federated authentication:** In this model, authentication requests from the service are passed to a federation server or service. This can be AD FS, or a third-party federation service such as Ping Identity or Okta. The federation server is responsible for authenticating the user by passing an authentication request to an on-premises DC or a third-party federation service and returning an authentication token for the user to access cloud services. This process provides the end-user with an SSO experience that can be used to access various Microsoft 365 services.

You can combine password hash synchronization with PTA or federation. This provides a manual fallback mechanism for authentication if the on-premises PTA or federation infrastructure is unavailable. As of November 2019, 91% of Entra ID tenants globally enabled password hash synchronization.

If you are thinking about switching authentication methods, a feature exists that can make this much easier. Rather than switching from federated authentication to password hash synchronization, PTA, certificate-based authentication, or seamless single sign-on for every user at once, you can control which authentication method is used on a per-group basis. To do this, access the **Hybrid management > Microsoft Entra Connect -> Connect sync** blade in the Entra admin center. Click **Enable staged rollout for managed user sign-in** and you will be taken to the configuration area. Using staged rollout is a great way to test the user experience and better plan what amounts to a major change to your authentication infrastructure.

Password Hash Synchronization

When directory synchronization is implemented with password hash synchronization, users can log on to services using the same password as their on-premises AD user account. This is referred to as "same sign-on", which is not to be confused with "single sign-on" even though they both can be abbreviated to SSO.

The concept of synchronizing passwords tends to raise immediate concerns within an organization, as people inevitably assume that real passwords are being transmitted over the Internet and stored on Microsoft servers. The reality is that password hash synchronization is a secure process, and the passwords themselves are not transmitted or stored. Instead, a password hash is used. Despite this, some organizations may still object to the use of password hash synchronization, so it is important to understand what is being synchronized.

On-premises AD stores passwords as hashed values that are said to be *irreversible*. In other words, a password hash cannot be used to determine a user's plain text password. Entra Connect extracts the password hash from AD, combines it with a user-specific salt value, and then hashes the combination 1,000 times before transmitting the hash over a secure HTTPS channel to Entra ID.

When password hash synchronization is enabled, the password complexity and expiration policies of on-premises AD override the policies set in Entra ID. When a password is changed on-premises the new password is synchronized to Entra ID. This process usually occurs in under two minutes. You can [selectively synchronize](#) password hashes using a custom synchronization rule. This adds complexity to your deployment and impacts password writeback so you should only use this capability if it is truly required.

If an on-premises password expires, the expired password will continue to work in Entra ID. This is because when password synchronization is enabled, Entra ID account passwords are set to not expire. For this reason, you should not rely on expiring or changing passwords to prevent a user from logging on. Instead, you should disable the on-premises user account and either force a directory synchronization, or block sign-in for their account in the Microsoft 365 admin center. If you want synchronized passwords to expire in Entra ID, you can configure Entra ID to apply the password policy in your tenant to synchronized users by following [these steps](#). You can use the `Update-MgDomain` cmdlet to configure the password policy for individual verified domains.

Another important benefit of password hash synchronization becomes available if you have Entra ID P1. With Entra ID P1, Microsoft provides leaked credential risk event information for users if they discover the user's UPN and password in a list of stolen/lost credentials. To perform the comparison, password hash synchronization must be enabled. Microsoft applies the same hashing process to the leaked password that is performed on-premises. They then attempt to match the hashed version of the leaked password to passwords in Entra ID. This works even if you use another sign-on methodology. It simply requires password hash synchronization to be enabled. In November 2019, Microsoft stated that they had processed over 5.5 billion leaked credentials and matched them to over 14.2 million Entra ID users. This feature is one of many reasons we strongly recommend that you enable password hash synchronization in your tenant.

Pass-Through Authentication

PTA, if enabled, allows you to offload authentication from Entra ID to your on-premises AD without the need to deploy AD FS or a third-party federation solution. As such, it can greatly simplify your deployment if you are seeking to keep control of the actual authentication process.

For this to work, you must install and configure one (or more) on-premises PTA connectors to validate user authentication requests. The connectors can be installed as part of Entra Connect and are very similar to Entra App Proxy connectors. They share the same architecture; the PTA connector is a customized version of the Entra App Proxy connector.

From a high-level perspective, here are the steps an authentication request goes through when PTA is enabled:

1. The client connects to a service endpoint and is redirected to Entra ID for authentication.
2. The client connects to the Entra ID authentication endpoint and is prompted for credentials.
3. After the user submits their credentials and assuming PTA is enabled, Entra ID encrypts the credential data and holds the authentication request in a queue for validation.
4. The PTA connector makes an outbound connection to Azure and retrieves the authentication request from the queue.
5. The connector decrypts the data from the request and validates the decrypted credentials against the on-premises AD. The result of this verification process is then communicated back to Entra ID.
6. If the credentials were verified successfully, a token is issued, or the MFA flow is started.

Seamless Single Sign-on

Seamless SSO enables Entra ID to accept a Kerberos ticket from the on-premises AD to authenticate the user if you are using password hash synchronization or PTA. The addition of Seamless SSO to either authentication model enables true SSO for users that are connecting from a domain-joined client computer. SSO is when users authenticate to both the on-premises organization and Entra ID using the same username and password without having to type their credentials again whenever they access a cloud resource. At a high level, this is what happens when Seamless SSO is enabled:

1. The client connects to a Microsoft 365 service and is redirected to Entra ID for authentication.
2. The client connects to the Entra ID authentication endpoint and is challenged for a Kerberos ticket.
3. The client turns to AD and requests a Kerberos ticket for the URL which is associated with Entra ID.
4. Active Directory locates this URL in the service principal name (SPN) of a computer account associated with Entra ID and encrypts a service ticket using that computer account's secret.
5. The client sends back the service ticket it received from AD.
6. Entra ID decrypts the Kerberos ticket using the computer account's secret which it received during the setup of the feature. If the ticket can successfully be decrypted, Entra ID will craft a token for the user.

For Seamless SSO to work, the following requirements must be met:

- Modern authentication must be enabled, and the client must support modern authentication.
- The client must be domain-joined and able to directly communicate with an AD domain controller. This is necessary for it to request a Kerberos ticket. Without direct access to a DC, SSO fails, and the process reverts to the regular authentication option (username/password). This prerequisite means that Seamless SSO cannot be used with Macs (unless joined to a domain), mobile devices, or any other device that isn't joined to an AD domain.
- The Entra ID authentication endpoints must be added to the computer's browser Local Intranet zone settings; by default, browsers do not send Kerberos tickets to public endpoints.

Microsoft describes the SSO-feature as "opportunistic." This means that SSO will be attempted if enabled. However, if anything goes wrong during the process, the authentication process will fall back to the default authentication option. For more information about configuring Seamless SSO, refer to [this document](#). Hybrid Entra join and Entra join do not have the same requirements for ongoing access to a DC to enable SSO. We will discuss both options later.

Federated Authentication

Identity federation offloads credential validation, and optionally MFA, to on-premises federation infrastructures such as AD FS or Ping Identity, or a third-party cloud identity solution. A by-product of configuring identity federation is that it can provide an SSO experience.

When you federate a domain, the responsibility for validating authentication requests is shifted towards the federation solution. The application that's asking the federation system to perform authentication is known as the *relying party* (because it's relying on the federation service). A federation standard named WS-Fed/WS-Trust is almost always used to federate with Entra ID. The standard specifies the format and content of data and metadata that the service and federation broker can use to negotiate and perform the authentication.

Federation depends on the concept of *claims*, which are statements made by one party about another. For example, the application might send a claim to the federation server that says "the user requesting authentication is coming from IP address 172.16.0.204" and the federation server might reply with a set of claims that includes "the email address associated with the account you are trying to authenticate is britta.simon@office365itpros.com." You can configure AD FS *claims rules* that allow or restrict authentication based on the contents of these claims.

Federation is enabled per domain and all users in Entra ID for whom the domain portion of the UPN (the UPN suffix) matches a federated domain are automatically considered to be federated identities (except if the user is included in a staged rollout group). Even with federated identities, the first authentication request is still received by Entra ID. The user's UPN is examined and, if the domain name is federated, Entra ID will redirect or proxy the authentication request to the customer's federation solution. This process is called *home realm discovery* and needs to be performed for each initial authentication (such as the first time that someone logs on). You can see this process at work when you have federation set up and you visit a logon page; at first, you see the standard Microsoft logon dialog, which contains code that looks at the UPN and determines if it's for a federated user, redirecting to the organization's federation solution if so.

The details of the organization's federation solutions and all the relevant details such as the federation endpoint and certificate information are stored in Entra ID during the federation setup process. The initial request (home realm discovery), and the subsequent redirects all happen within a matter of seconds, often transparent to the user.

When authenticating with Entra ID, you will notice that most of the time the user is asked to enter their email address. However, that is not entirely true. Although the web page or application might ask for the "*Email Address*" on the screen, the user should enter their UPN to complete the logon. Because of this, the general recommendation is to align the user's UPN and primary email address to remove any potential for confusion for the end-users. If your organization can't align the UPN and primary email address, you may be able to use Alternate Login ID, discussed later.

To Federate or Not?

Various elements influence the decision of whether identity federation is the right solution for you. Apart from the added infrastructure that is needed, complexity is often the reason why organizations avoid federation, especially when they must manage the federation solution themselves. Unsurprisingly, password hash synchronization is the most popular authentication method in Entra ID, as it is much easier to deploy and maintain, and it offers a similar login experience to end-users when combined with seamless single sign-on or a device that is Entra joined or Hybrid Entra joined. In addition, users will still be able to authenticate, even when the on-premises infrastructure is down; the only thing that would (temporarily) stop working in such a scenario, is the actual synchronization of passwords.

On the other hand, identity federation (for example, through AD FS) can solve very specific problems, like whether to block authentication from outside the corporate network, limit access to Microsoft 365 services to members of a specific group, or use a third-party MFA solution. These types of problems can also be solved without AD FS if you have Entra ID P1.

In general, we often recommend that you start with password hash synchronization and Seamless SSO for authentication with Microsoft 365 and Entra ID. If you have complex business or technical requirements that

cannot be met without implementing federation, only then should you do so. Be sure to consider the tradeoff of complexity with the requirements you are trying to meet.

Third-party Federation Solutions

AD FS is not the only federation solution to enable SSO. Several third-party solutions, such as those from Okta, Ping Identity, and OneLogin take a similar approach to federation. The decision to use a third-party solution depends on several factors such as integration with other cloud systems. Different solutions have different requirements and capabilities.

Entra ID also offers advanced SSO features like those supported by third-party vendors. In addition to these SSO features, Entra ID contains additional features such as enhanced MFA and self-service password management. Many of these features require users to have a license for [Entra ID P1](#). While these capabilities come at an additional cost, they are worth evaluating along with other third-party solutions.

The pitfall you will run into if you elect to purchase a third-party federation solution is whether you can avoid the cost of Entra ID P1. Many of the security controls that organizations require to secure their Office 365 implementations are native to Entra ID P1 and P2. Without Entra ID P1 or P2 it may be difficult or impossible to implement these controls. Where it is possible to implement substitute controls, the user experience is often lacking. For these reasons, we find that many organizations find Entra ID P1, or one of the bundles that includes it, is better value than third-party federation solutions.

Alternate Login ID

Like many other cloud services, Microsoft 365 requires the logon ID to be *Internet routable* because ownership of non-routable domains like internal domains ending in ".local" cannot be verified. Users for which the on-premises UPN suffix does not match any registered domain are given a UPN suffix based on the default domain. For instance: *britta.simon@office365itpros.onmicrosoft.com*. Note that the tenant's default domain cannot be federated.

By default, when you configure AD FS, the UPN is used as the primary logon ID for Entra ID. Generally, it is recommended to ensure the UPN matches the user's email address so that they only need to remember their email address to sign in to Microsoft 365. Unfortunately, sometimes you might not be able to change the UPN to match the email address. If you are unable to change the UPN for your users, for example, because a legacy application needs a specific value, you can use a feature called "Alternate Login ID". This feature allows you to specify which attribute – other than the UPN – should be used to sign on to Microsoft 365. For instance, you can configure the actual Email Address attribute to be the new identifier. Although Microsoft supports Alternate Login ID for Hybrid deployments, there are some severe drawbacks from an end-user perspective (like extra authentication prompts). Unless you absolutely cannot reconfigure the UPN, we do not recommend choosing Alternate Login ID.

In [this](#) article, Microsoft describes the end-user experience for various applications and protocols if Alternate Logon ID is configured. Connections from within the corporate network are most likely to work just fine. External access, regardless of the client, can be problematic and result in extra authentication prompts. No matter what approach you use, the end-user experience suffers as soon as Alternate Logon ID is enabled.

You can [configure alternate login ID in AD FS](#), or you can configure it in Entra ID if you use password hash synchronization or PTA. When you [enable alternate login ID](#) in Entra ID (currently in public preview), users will be able to sign in to Entra ID using any email address configured for their account. These email addresses must be in their proxyAddresses attribute and belong to a domain namespace validated in the tenant. You can also use [staged rollout](#) to enable alternate login ID for a subset of your users.

Understanding Authentication in Entra ID

Establishing a standalone or hybrid identity to use with Microsoft 365 is only half of the work. Once you have an identity, you must first authenticate before you can access resources online. Leveraging the power of Entra ID, Microsoft 365 offers a variety of authentication options, ranging from the default username/password combination to more advanced authentication solutions.

Before diving into the advanced scenarios, let's first look at how Entra ID performs authentication. The simplest credential is the combination of a username and a password. This option is also the default in Microsoft 365 for all non-federated identities.

When a user attempts to access resources, the service prompts them for credentials. Depending on what client is used, the authentication prompt comes in various forms. Microsoft has worked hard to standardize the appearance of the Entra ID-based logon interface across clients and platforms, so the logon experience is remarkably consistent across devices and applications. No matter the interface, once the user provides a credential, various things happen behind the scenes depending on what client is used and what authentication method has been configured.

Most authentication flows in Entra ID are based on the use of the OAuth 2.0 authorization protocol. Figure 2-1 depicts the authentication flow of a desktop client using modern OAuth 2.0 based authentication:

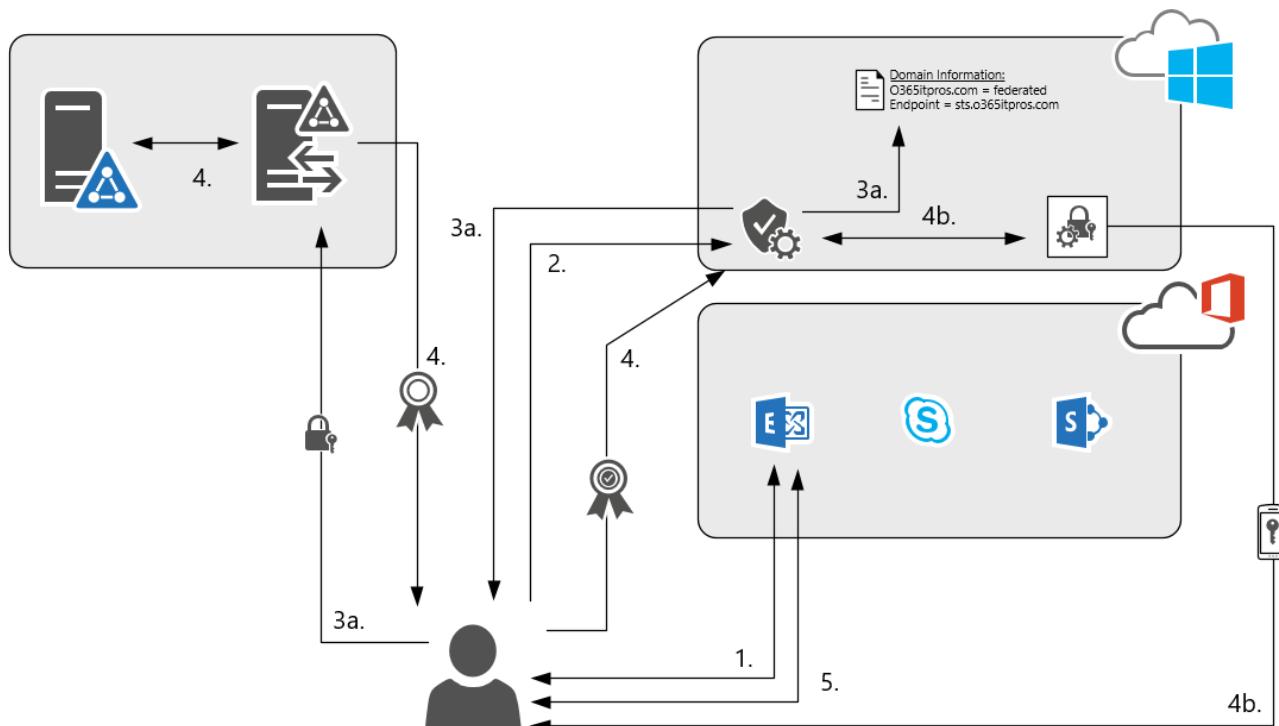


Figure 2-1: Authentication flow

1. The user connects to Exchange Online and is redirected to Entra ID for authentication.
2. The user connects to the Entra ID authentication endpoint and is prompted for credentials via a forms-based dialog.
3. After the user submits their credentials, Entra ID first verifies the identity type of the user. It does so by looking at the user's UPN and verifying what type of authentication the user is configured to use.
 - a. If the user is federated, the client is redirected to their identity provider. Depending on what client the user is connecting with and how the endpoint is configured, the user might need to enter additional credentials.
4. The client receives a token from Entra ID and uses it to access the Exchange Online service.
5. The user is granted access to the Exchange Online service.

- b. If Seamless SSO is enabled, the user's browser is challenged for a Kerberos service ticket to identify the account. If the browser returns a service ticket to Entra ID, the service ticket is validated, and the user is signed in.
 - c. If the device is hybrid Entra joined or Entra joined, the user's primary refresh token (PRT) is validated, and the user is signed in.
 - d. If PTA is enabled, the user's request is passed on to the on-premises AD via PTA agents.
 - e. If the user's password is managed in Entra ID (standalone identity or using password hash synchronization), the username/password combination is verified by Entra ID itself.
4. When the credentials are successfully validated, one of the following happens:
- a. In the case of federated authentication, the user receives a token (from the identity provider) and is then redirected to Entra ID where the user receives an artifact that identifies the user.
 - b. If MFA is required, and the user's federation service did not tell Entra ID that MFA was already performed, the user is first requested to enter additional verification after which (if successfully validated) the identifying artifact is created and returned.
5. The user is now redirected to the service it initially connected with (for example, Exchange Online). Using the artifact previously received from Entra ID, the client can now access the online resource.

Following successful authentication, Entra ID issues two tokens to the user: an access token and a refresh token. The access token is short-lived, meaning it has a limited lifespan (one hour by default). An app like OWA uses the access token to authenticate to Exchange Online. The refresh token, which can remain valid indefinitely, is used to request new access tokens from Entra ID when they expire. With a valid refresh token, the user does not have to re-authenticate. Instead, the refresh token is used to obtain a new access token from Entra ID. The flow described above assumes the client has no valid refresh token, which would be the case when the refresh token expired or when the client has not yet connected to Entra ID.

Several things control the validity of the refresh token, such as how often it is used or whether the user changes their credentials. When the refresh token expires, the user must sign in again. Depending on the client, and how authentication is implemented, this might require a user to provide their credentials again. If true SSO is used, re-authentication should happen automatically and is fully transparent for the end-user. If no SSO is configured, the user will be presented with an authentication form.

To comply with European Union regulatory requirements, end users connecting to Entra ID from a device with its region set to a country in the European Economic Area (EEA) will be prompted to confirm if they want to sign-in to Entra using the same credentials they use to sign into Windows. This prompt will be shown the first time the user tries to sign-in and cannot be controlled by administrators. Microsoft provides more information on this behavior in this [article](#).

Revoking Tokens

As mentioned earlier, Entra ID authentication uses two types of tokens: access and refresh tokens. The access token ultimately grants you access to the online service: with a valid access token, you can access the requested service and do something like opening a mailbox. You can continue to work with the service until the access token expires or you interrupt or close the active session (like closing the browser window). When an access token expires, the client can acquire a new access token using a valid previously-received refresh token. If a valid refresh token exists, the user does not have to re-authenticate.

Because of how these tokens are used, organizations sometimes face a new challenge: what if you need to revoke someone's access immediately? The same problem also exists in an on-premises organization to a certain extent: when you disable an account in AD, subsequent authentications are no longer allowed, but the user is not forced to close any open session/applications being used at that time.

Access tokens cannot be revoked. This means that once someone gets a valid access token, they can keep using that token for up to its maximum lifetime. You can, however, revoke the refresh tokens which prevents the user from acquiring a new access token when it expires, and thus force the user to re-authenticate (which will fail, if you disable the account). To revoke valid refresh tokens for a user, navigate to **Users** in the Entra admin center, find the user, click **Profile**, and then click **Revoke sessions** on the toolbar. You can also revoke all the refresh tokens for an account by running the following PowerShell commands:

```
$UserId = (Get-MgUser -UserId Andy.Ruth@Office365itpros.com).Id  
$RevokeStatus = Revoke-MgUserSignInSession -UserId $UserId
```

Although revoking the refresh token is not ideal, it will at least prevent the user from continuing to obtain valid access tokens. Some organizations need to customize the default sign-in frequency behaviors. If you have Entra ID P1, you [can use a feature](#) of conditional access to control how frequently users must sign in to access applications.

Modifying lifetimes for tokens used to be an acceptable approach to mitigating risk. A better approach is for tokens to automatically get revoked when a risk event occurs. A feature called [Continuous Access Evaluation](#) (CAE) addresses this need. With CAE, when a risk event occurs, the workload (Exchange Online, SharePoint Online, OneDrive for Business, Microsoft Teams, or the Microsoft 365 admin center) is notified so that it can take near real-time action to revoke access. When CAE is enabled, the one-hour lifetime for access tokens discussed earlier is increased to 28 hours for CAE-capable applications. Since the workload is continuously evaluating the validity of the access token, the increased lifetime does not present a new or additional security risk.

The events below currently trigger a notification to the subscribing workloads:

- The user account is disabled/blocked.
- The user account is deleted.
- The user's password is changed (or reset).
- MFA becomes mandatory for the user.
- Refresh tokens are administratively revoked for the user.
- Entra Identity Protection detects elevated risk for the user.

CAE is enabled by default in all tenants. If you want to disable CAE or modify the behavior of CAE, you can do this with a conditional access policy (discussed later). You can use conditional access to place CAE in strict enforcement mode for some or all users. In strict enforcement mode, CAE will revoke access if a user's IP address changes or when the client [lacks the capabilities to handle CAE processing](#).

Passwordless Authentication

Passwordless authentication offers significant security benefits over passwords. By removing passwords, you can remove a significant attack vector. You can also improve user experience by removing the need for users to remember passwords, periodically change passwords, etc. If you have frontline workers that do not frequently use a computer as part of their job, passwordless authentication can reduce the friction involved in deploying IT services to this population. While it is not yet possible to entirely remove passwords, we strongly recommend beginning the journey of exploring how passwordless authentication can be integrated into your organization's IT strategy.

Whether you are in a hybrid or standalone identity model, Microsoft supports multiple passwordless authentication methods:

- **Text message sign-in:** In this model, users can authenticate to Entra ID with a one-time passcode sent via SMS/text message to their previously registered mobile device.

- **Microsoft Authenticator App:** In this model, users enter their UPN, and Entra ID sends a push notification to the Authenticator app. The user sees a random two-digit number on the sign-in screen and must enter the two-digit number into the Authenticator app. If the user provides the correct number in the Authenticator app, enters a PIN, or provides a biometric (e.g., Apple TouchID), Entra ID accepts their sign-in. iOS devices can register to provide passwordless sign-in to multiple tenants.
- **Passkey (FIDO2) sign-in:** [FIDO2](#) is an industry standard for authenticating to devices and online services using a standards-based hardware token. FIDO2 tokens are supported on a variety of [operating systems and devices](#). The FIDO2 authentication method also includes support for device-bound passkeys using the Authenticator app.
- **Certificate-based authentication:** this model allows users to sign-in using a client certificate, typically stored on a smart card. Certificate-based authentication works with browser-based, certain mobile apps, and Entra-joined sign-in on [certain versions](#) of Windows 10 and Windows 11. You can configure Entra ID to use the certificate as the primary factor of authentication or as a second factor that satisfies MFA requirements.
- **Windows Hello for Business:** In this model, users use a PIN or biometric to unlock a private key that is specific to the device and typically stored in the trusted platform module (TPM). The key is used as part of an exchange with Entra ID to obtain a primary refresh token (PRT) that is valid for access to Entra ID protected resources.
- **Platform Credential for macOS:** this model is like Windows Hello for Business except for Mac devices. A hardware-protected key stored in the device's secure enclave is unlocked and used to obtain a PRT for access to Entra ID.

To use a passwordless authentication method, you must first enable the authentication method. Sign into the Entra admin center and navigate to **Protection** and then **Authentication methods**. From here, you can enable text message, Microsoft Authenticator, certificate-based authentication, or FIDO2 Security Key sign-in for a group of users, or you can enable it for all users. Once you enable a new authentication method or make configuration changes to an existing one, it might take a few minutes to start working.

Text message sign-in has several limitations. The most important limitation right now is that Teams is the only Office thick client application that text message sign-in works with. Otherwise, you can only use text message sign-in with web applications.

FIDO2 sign-in requires users to have a [supported](#) hardware token. Once the user has a hardware token, they can browse to <https://mysignins.microsoft.com>, click **Security Info**, click **Add method**, and choose **Security key**. The user will be walked through the process of pairing their security key with Entra ID. Once this is complete, the user can click **Sign in with a security key** on future Entra ID sign-in prompts. As mentioned above, the Authenticator app can host device-bound passkeys for Entra authentication. You can also use FIDO2 keys to sign in to devices with [Windows Hello for Business](#), [sign in to AD joined](#) devices, and on iOS devices.

Certificate-based smartcard authentication is a critical scenario for a relatively small number of organizations, including the United States government. We do not expect that many organizations will use this authentication method unless they already have a mature smartcard deployment. Instead, we recommend that organizations invest in passwordless architectures based on Microsoft Authenticator and/or FIDO2 devices. For information on configuring certificate-based authentication, refer to the [Microsoft documentation](#).

Temporary Access Pass

One of the challenges to deploying passwordless authentication is how to enroll a user with a FIDO2 token or another authentication method for the first time. If the user has a password, they can use their password (and MFA) to enroll. If they are a new employee, then you must give them a password for their initial sign-on,

which defeats the concept of passwordless authentication. To address this challenge, Entra ID has a feature called Temporary Access Pass (TAP).

TAP lets you provide users with a short-duration unique code that the user can use to set up their passwordless credentials. When a TAP is created for a user, they attempt to sign in to Entra ID in the same manner as a normal user. Instead of prompting the user for a password, they will be prompted for their TAP. After entering a valid TAP, the user can enroll their passwordless authentication method such as a FIDO2 token or the Authenticator app. You can also use TAPs to restore access for a user that needs their passwordless credential replaced.

To enable TAP in your tenant, navigate to **Protection** in the Entra admin center and then **Authentication methods**. Next, enable the Temporary Access Pass method. You can configure the lifetime of the TAP, whether it can be used more than once, and the length of the code. Once TAP is enabled, members of the global administrator, privileged authentication administrator, and authentication administrator Entra ID roles can create TAPs for users.

To create a TAP, navigate to **Users** and then find the user you want to create a TAP for. Click **Authentication methods** and then **Add authentication method**. On the screen that appears, you can create a TAP and optionally specify when it becomes valid. This capability may be useful if you want to create a TAP in advance for a new employee. You can make the TAP valid beginning on their first day of work, for example.

Note: If you do not see the Add authentication method button, you might need to click the **Switch to the new user authentication methods experience!** banner on the top of the screen first.

In addition to using the Entra admin center to configure TAPs, you can also use the [Graph API](#) to automate TAP management tasks.

Third-party Authentication Methods

Entra ID supports [the integration of third-party authentication solutions](#) as authentication methods, meaning that when the need exists for an inbound connection to verify itself using multifactor authentication, Entra ID can redirect the connection to a third-party solution and accept the response in the same way as any of the native authentication methods. The advantage of this approach is that organizations can exploit multifactor authentication solutions that they've deployed to serve other platforms and applications. The set of supported third-party solutions include Cisco Duo, Entrust Identity, HYPR Authenticate, Ping Identity, RSA, Silverfort advanced MFA, Symantec VIP, Thales STA, and TrustBuilder MFA.

Documentation explaining how a third-party solution integrates with Entra ID as an authentication method is [available online](#).

Customizing the Tenant Sign-In Page

Tenants can customize the sign-in page presented to users when they sign in via Entra ID. Customizing the sign-in page lets you apply your organization's look and feel by modifying background colors and images as well as replacing the Microsoft logo. Applying your organization's brand has the added security benefit of giving your users a recognizable place to enter credentials. Customization is not hard, but it usually takes some homework to identify the right images and colors. Partnering with your marketing or internal communications teams is usually the best way to be successful.

When a user accesses resources from another organization as a guest, the branding experience changes slightly to provide context about the user's organization and the organization they are accessing. In this scenario, the background image (element 1 in Figure 2-2) changes to the background of the organization that owns the resource. The remaining elements represent the user. For example, if a user from the Coho Vineyard

is accessing a resource in Contoso's tenant, they will see Contoso's background image and the Coho Vineyard's banner logo, username hint, and sign-in page text.

Custom branding elements apply to all users, with one exception. You can define different branding elements based on the user's language. The user's language is determined dynamically by information provided by their web browser about language settings on their computer. To configure branding, go to **User experiences > Company branding** in the Entra admin center. If you edit the default settings, they will apply to all users. To create different branding settings based on user language, click **New language** on the toolbar.

If your organization uses AD FS or another identity provider, the branding settings in Entra ID will not be visible in some scenarios. You should also customize the sign-in page for your identity provider. More information about branding AD FS' sign-in pages is located [here](#). If you're running AD FS on Windows Server 2019 or later, don't forget to [enable paginated sign-in](#). This makes the AD FS sign-in process much more like Entra ID.

Figure 2-2 shows the sign-in page with customized branding elements and the optional footer enabled. The numbers in Figure 2-2 correspond to the branding elements in Table 2-1. Pay attention to the notes in Table 2-1 too. For the best user experience, you will need to select images that work best with how Entra ID displays the branding elements.

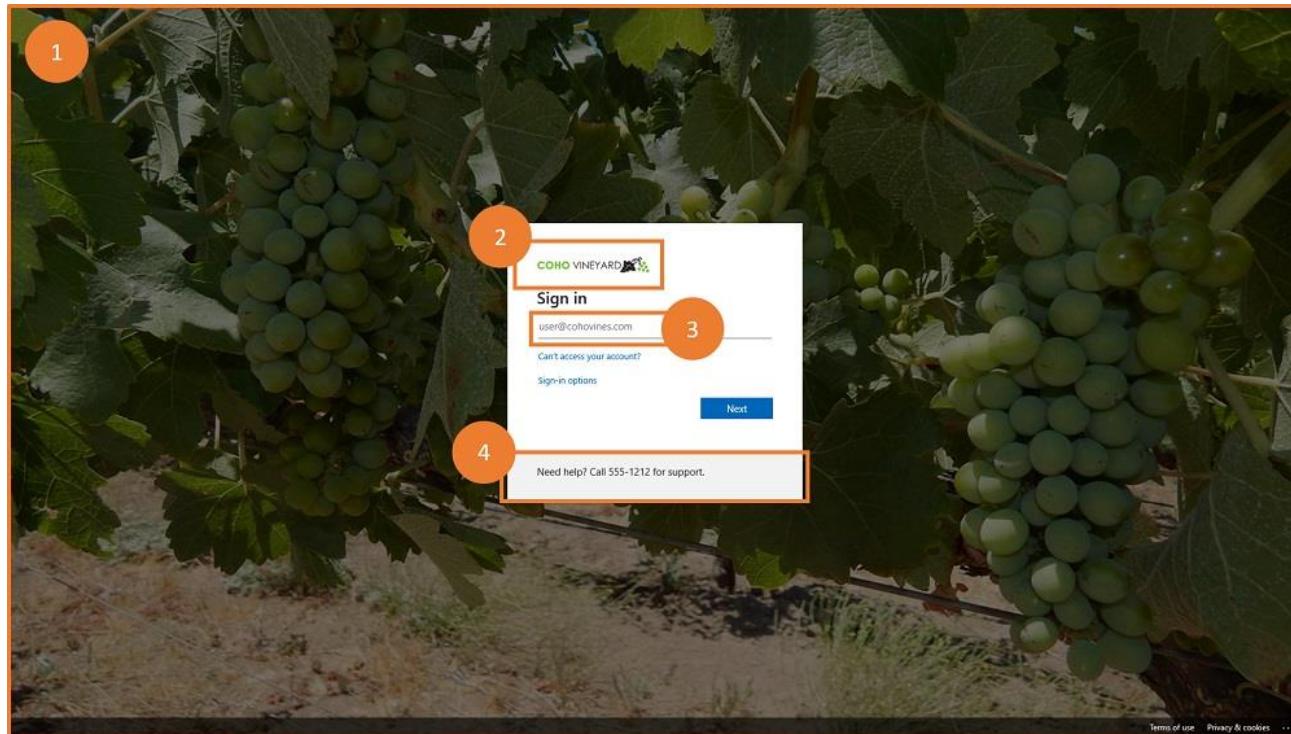


Figure 2-2: A Branded Entra ID sign-in page

#	Element	Requirements	Notes
1	Background image	Dimensions: 1920x1080px Format: PNG, JPG, or JPEG Size: 300KB or less	<ul style="list-style-type: none">This image is dynamically cropped based on screen size. Avoid using an image that includes text.Minimize the file size where possible to improve page load speeds.
2	Banner logo	Dimensions: 280x60px Format: Transparent PNG, JPG, or JPEG	<ul style="list-style-type: none">Use a transparent PNG fileThis image is shown in automatically generated email

#	Element	Requirements	Notes
		Size: 10KB or less	communications and other places like the MyApps portal.
3	Username hint		<ul style="list-style-type: none"> Text displayed as a reminder to the user about how to format their sign-in name.
4	Sign-in page text		<ul style="list-style-type: none"> Optional but useful for helpdesk contact info, legal disclaimers, etc. You can use a limited number of Markdown styles to boldface, italicize, or underline text and add hyperlinks.
Not Shown	Sign-in page background color	RGB color code (hex format)	<ul style="list-style-type: none"> Shown instead of the background image when the screen size is too small.
Not Shown	Square logo image	Dimensions: 240x240px Format: PNG, JPG, or JPEG Size: 50KB or less	<ul style="list-style-type: none"> Used on Windows devices during Entra join, Windows Autopilot, and other experiences. Provide two versions – one for light backgrounds, and another for dark backgrounds.
Not Shown	Favicon	Dimensions: 32x32px Format: PNG, JPG, or JPEG Size: 5KB or less	<ul style="list-style-type: none"> Shown in the web browser tab in lieu of the Microsoft logo icon

Table 2-1: Branding elements

You can also customize the layout of the sign-in page including showing optional header and footer areas, resizing the layout of the background image, and customizing the text on links shown on the page. You can use a limited number of custom cascading style sheet (CSS) selectors to further customize the sign-in screen beyond what the GUI allows. You can learn more about this option and download a CSS file template [here](#). Microsoft's [announcement](#) includes screenshots of sample changes you can make with the new functionality.

If you want to automate the configuration of branding settings, use the script [described in this article](#) as a starting point. Just keep in mind that frequent changes to your sign-in page branding may be detrimental. If users do not have a familiar sign-in page, they may not realize a malicious page they're redirected to through a phishing email (for example) is not legitimate.

Joining Computers to Entra ID

Windows 10 and newer versions support the concept of joining client computers to Entra ID. There are two different ways to join Entra ID: 1) Entra join and 2) hybrid Entra join. In the first scenario, the client computer only has a relationship with Entra ID. Rather than signing into the device with a local account, users sign in with their Entra ID credentials [or a client certificate](#). This can be a standalone identity or a hybrid identity. In the second scenario, the client computer remains joined to an AD domain (in the same manner it has for decades), but the device also maintains a parallel relationship with Entra ID. Users sign in with their AD credentials and the computer also acquires a primary refresh token (PRT) used to authenticate with Entra ID (and in turn dependent resources like Office 365 workloads).

Entra join can be useful for any organization, including smaller organizations that do not have an on-premises AD forest. If you have a workforce that primarily works remotely, you can achieve benefits of domain join like

single sign-on without the need to have network connectivity to reach a DC. Even if a client computer is solely joined to Entra ID, if there is an AD forest, that user can [seamlessly access](#) traditional resources and applications that use Kerberos authentication when they are on the network. Entra join requires no specific configuration to begin using the feature. You can control who can join a device to Entra ID in the Entra admin center. Go to **Devices > Overview > Device settings** and configure the **Users may join devices to Azure AD** setting. We also recommend that you require MFA to join a device. The best way to enforce this requirement is with a conditional access policy. We discuss conditional access and applying a policy to user actions later in this chapter.

Hybrid Entra join requires some initial configuration to use the feature. Windows 10 and newer devices locate the Entra ID tenant they should attempt to hybrid join by searching AD for a service connection point (SCP). The easiest way to create the SCP is to use Entra Connect. The configure device options task in Entra Connect will create the SCP record for you. If you use federated authentication, you will need to make sure that your identity provider supports Hybrid Entra join. AD FS supports hybrid Entra join, however, it must be configured to [issue certain claims](#) specific to computers. Entra Connect will also configure AD FS for you.

After configuring hybrid Entra join, you can begin using a client computer's identity as an input to conditional access, discussed later. You can also achieve SSO from Entra joined and hybrid Entra joined devices without configuring seamless SSO. Microsoft Edge and Mozilla Firefox (beginning with version 91) natively support this form of SSO, however, you can also deploy an [extension](#) for Chrome if your organization uses it. In both cases, the browser can submit your PRT to Entra ID at sign-in. The PRT identifies the user, whether they have performed MFA (or not), and the device. You can check on the PRT as well as the general health of a device's Entra ID relationship by running **dsregcmd /status** from a command prompt.

Linux devices enrolled in Intune are also registered in Entra ID. Once Linux devices are registered, they can participate in conditional access policies that rely on the device's identity if the Edge browser is used on the device. For more information on registering Linux devices in Entra ID, refer to [this document](#).

Guest Access with Entra ID Collaboration

Entra ID provides a rich and flexible fabric for bringing external people into your tenant in the form of guest accounts with Entra External Identities (formerly Business-to-Business B2B) collaboration. A guest is an external user whose account and credentials exist outside your tenant (often in another tenant). Entra External Identities is the component of Entra ID that enables guest accounts to work. One of its most valuable benefits is the ability for guest users to authenticate using their organization's credentials while accessing an application in another tenant. For example, a user from contoso.com needs access to a file stored in SharePoint Online in the Office365ITPros.com tenant. The user from contoso.com authenticates to Office365ITPros.com using their contoso.com credentials, rather than a separate username and password. This also means that when the user's contoso.com account is deactivated (such as when they leave the organization), their access to Office365ITPros.com is also deactivated.

Entra ID assigns [guest accounts a more restrictive set of permissions](#) than it does to member accounts. However, you can change the **Guest users' permissions are limited** setting to No in the Entra admin center if you want guest accounts to have the same default permissions to see information in the directory (like group memberships) as member accounts do. Guest accounts can have administrative roles and execute functions associated with those roles.

Because guest accounts are Entra ID objects that share many of the characteristics of user accounts, applications can use guest accounts to control access to content. Entra ID uses email addresses to create UPNs to identify guest accounts. The email address can point to another tenant domain within Microsoft 365, an email domain for a company that doesn't have a tenant, or a consumer email service, like Gmail.com or Yahoo.com. You can view a list of guest accounts in a tenant through the Users section of the Microsoft 365

admin center, the Users section of the Entra admin center, the Contacts section of the Recipients tab in EAC, or by running the command:

```
Get-MgUser -All -Filter "userType eq 'Guest'" | Format-Table DisplayName, UserPrincipalName
```

You can edit properties of guest users through the Microsoft 365 admin center or Entra admin center. You can't make changes to guest accounts through the Exchange Admin Center because the list of guests displayed there is for informational purposes only. It is common practice to update visible properties such as display names, telephone numbers, job titles, and addresses for guests. And as we'll see later, it is also possible to upload a photo for a guest account.

Creating Guest Users

You can create guest users through [the Entra admin center](#) by clicking **New user > Invite external user**. The account creation process allows you to add the new guest user to groups. You can also create guest users with [PowerShell](#), but the most common method used is when applications issue invitations to external users, which is what happens when you add a guest to an Microsoft 365 group or team, or share a document or folder with SharePoint Online or OneDrive for Business. If you have regular (member) user accounts created for external people in your tenant, these accounts can be [converted into guest accounts](#).

When Entra ID adds a new guest, it calls [the Invitation API to create and send an invitation](#) via email to the user's address to tell them that they have been invited to start using an application in the tenant. Applications can send invitations and can customize the form of those invitations. In addition, the API supports the inclusion of a link for the user to access the application, like the access information needed for someone to join a group or team.

The value of the *ExternalUserState* property for a guest user account created after generating an invitation is *PendingAcceptance*. This state is enough to add the guest user to a group. At this stage, the guest user is a placeholder. When the guest redeems the invitation, the *ExternalUserState* property changes to *Accepted* and Entra ID puts the account into a state where it can access tenant resources. Guest accounts don't need to redeem invitations to be functional. For example, guest members of Outlook groups can participate in group conversations through email without redeeming their invitations. Guest members must redeem invitations to access SharePoint Online and OneDrive for Business content and to participate in Teams.

You can discover what accounts are in a specific state with the *Get-MgUser* cmdlet. In this example, we list the guest accounts in a pending acceptance state. The *ExternalUserStateChangeDateTime* property is the timestamp for the last account update.

```
Get-MgUser -All -Filter "userType eq 'Guest' and ExternalUserState eq 'PendingAcceptance'" -  
Properties DisplayName, UserPrincipalName, ExternalUserState, ExternalUserStateChangeDateTime |  
Format-List -Property DisplayName, UserPrincipalName, ExternalUserState, @{e={Get-  
Date($_.ExternalUserStateChangeDateTime)} -format g};n="Invitation Issued"
```

The norm is that user accounts have the same UPN and primary email address. Guest accounts often use their email address to sign in. If you need to change a guest's email address, you can do that by resetting their redemption status. To do this, you can use the [New-MgInvitation](#) cmdlet's *ResetRedemption* parameter, or you can use the [Entra admin center](#). Apart from the updated email address all the other properties of the guest user remain unchanged. After the user redeems the invitation sent to the new email address, the guest user switches to that address. This mechanism preserves access to all resources available to the guest user.

If you need to collaborate with another tenant in your organization or you are merging with another company that also uses Entra ID, you can use cross-tenant synchronization to automatically provision guests in your tenant by connecting to their home tenant. By using cross-tenant synchronization, you remove the need to

manually invite guests to your tenant. For more information on configuring cross-tenant synchronization, refer to the [Microsoft documentation](#). Note that cross-tenant synchronization requires Entra ID P1.

Cross-tenant synchronization does not independently solve some of the challenges of collaborating in a multi-tenant organization. For example, interacting with users from another tenant in Microsoft Teams is not as fully featured as for internal tenant users. To address these challenges, Microsoft 365 [multi-tenant organizations](#) (MTO) automate the creation of the cross-tenant synchronization relationship and smooth collaboration in Microsoft 365 apps. Member accounts created through multi-tenant synchronization require Entra ID P1 licenses.

Guest Identity Sources

The identity source for the guest is a property of the user object that tells Entra ID where the guest comes from and how it will authenticate. You can see the source by looking at the profile of guest accounts in the Entra admin center, where accounts have a variety of [sources](#):

- Users from **other tenants** have "External Azure Active Directory" as their source. These guests sign into Entra ID using the credentials from their home tenant.
- Users of **Microsoft consumer services** such as Outlook.com have a "Microsoft account" as their source. These guests sign in o their Microsoft account (MSA).
- Users of Google's Gmail service can login with their Gmail credentials if the tenant configures federation with Google.
- Facebook users can sign-up and login with their Facebook credentials if the tenant uses [self-service sign-up](#).
- Users of **other services** such as Yahoo.com have "mail" as the source. In this case, guests sign in using a one-time passcode that is sent to their email address.
- Federation with a **SAML or WS-Federation identity provider** for guest users can be configured if the domain name in the guest's UPN is not verified in an Entra ID tenant. This capability is often used with organizations that have on-premises directories or federation systems that authenticate large quantities of external users.

The source for the guest account for anyone who has not redeemed an invitation is "Invited User." When the redemption process is complete, the source changes to one of the sources listed above.

The host tenant extending invitations to guests can require MFA to force guests to use a mixture of credentials: their password and another authentication method (like a one-time code sent to the guest's mobile device).

All applications that use the Entra External Identities collaboration framework generate and redeem invitations in the same manner. The difference is the link contained in the invitation – it can point to an individual team, group, or other application and the application referenced must be ready to allow access to that guest.

SharePoint is an exception in that it creates a guest user account in your tenant when an external user from another tenant redeems a sharing invitation to a document or folder with the usual one-time code mechanism.

Entra ID stores information about the identity source for guests in their accounts. Sometimes it's interesting to fetch this information for analysis. Here's how to find guest accounts that use Microsoft accounts for their identity:

```
Connect-MgGraph -NoWelcome
[array]$Guests = Get-MgUser -All -Filter "userType eq 'Guest'" -Property id, DisplayName,
userPrincipalName, Identities
ForEach ($Guest in $Guests) {
    If ($Guest.Identities.Issuer -Like "*MicrosoftAccount*") {
        [array]$Issuer = $Guest | Select-Object -ExpandProperty Identities
        [string]$Issuers = $Issuer.Issuer -join ", "
```

```
Write-Host ("Guest account {0} has issuer {1}" -f $Guest.DisplayName, $Issuers)
}}
```

Audit Records for Guest Additions

Entra ID captures details of the addition of a new guest account in an “Add User” audit record. Other audit records are captured for “Add member to group” events when a new member joins a group. Together, these audit records give enough information to allow administrators to track and report when new guests join groups in the tenant. To extract the information, use the Audit log search feature in the Microsoft Purview Compliance portal, or use the PowerShell `Search-UnifiedAuditLog` cmdlet. Several examples of how to use the cmdlet to extract, refine, and analyze audit log data are included in the reporting and auditing chapter.

Federated Identity Providers

Entra External Identities supports federated identity providers. Federation means that guest users can sign in to access tenant resources without needing to create a Microsoft account or account in the local tenant. The first [federated identity provider is Google](#), where support is available for sign-ins for guest accounts using the Gmail.com domain. [Federation with Facebook](#) is also supported. See [this article](#) for information about how to configure federation between Microsoft and Google. Teams also supports federated authentication for Gmail accounts.

One-time Passcodes

One-time passcodes (OTP) for guest accounts allow users with any email address to authenticate using codes sent to their mailbox. The codes last for 24 hours. During this period, the user can access any resource they have been granted access to in the tenant. [OTP is enabled by default](#). Any guest account whose email address is not part of an Entra ID tenant, a Microsoft account, or belongs to a federated identity provider, will receive a one-time code that they can use to redeem their invitation. The initial token lasts 24 hours and once it expires, the user must receive another code to reauthenticate.

Creating Invitations

You can reproduce what an application does when it generates an invitation to a guest with a series of PowerShell commands. It is critical to understand that this code is an example not intended for production use. Instead, it illustrates some of the processing that occurs when a group owner invites a new guest to join a group.

First, we run the `New-MgInvitation` cmdlet to generate and send an invitation to the email address of the guest we want to add, in this case, `John.Doe@outlook.com`. If the user accepts the invitation, the redirect URL brings them to the specified URL.

```
New-MgInvitation -InvitedUserDisplayName "John Doe" -InvitedUserEmailAddress John.Doe@outlook.com -  
SendInvitationMessage:$True -InviteRedirectUrl  
https://office365itpros.sharepoint.com/sites/GroupName
```

When you generate an invitation to a guest, Entra ID checks whether a guest user already exists in the host tenant. If one exists, it is used. If not, Entra ID creates a new guest user. You can check this by running the `Get-MgUser` cmdlet after sending the invitation. The account has a `UserType` of “Guest” and the UPN is based on the email address used in the invitation. In our example, the UPN is

`John.Doe_outlook.com#EXT#@office365itpros.onmicrosoft.com`. If you don’t want Entra ID to send a standard invitation email, set the `SendInvitationMessage` switch to `$False`. You can later send your own customized message to the guest to invite them to join the tenant.

After they receive the message containing the invitation, the guest clicks the link to accept the invitation. If their account is already validated, they can go ahead and access the resource pointed to by the URL. If the guest account has never been used before, accessing a resource causes a redemption process to begin during which the account is validated. Following successful validation, the guest can go ahead and access the

resources to which they have been given access. Entra ID updates the guest account to set its *ExternalUserState* property to Accepted and the *ExternalUserStateChangeDateTime* property with the current timestamp. We can therefore check for outstanding guest acceptances with some code to retrieve all guest accounts whose state is not accepted.

```
[array]$Guests = Get-MgUser -All | Where-Object {$_ . UserType -eq 'Guest'} | Sort-Object DisplayName  
ForEach ($Guest in $Guests) {  
    if (([String]::IsNullOrEmpty($Guest.ExternalUserState) -eq $false -and $Guest.ExternalUserState -  
ne "Accepted") {  
        Write-Host $Guest.DisplayName, $Guest.ExternalUserState, $Guest.Mail, $($Get-  
Date($Guest.ExternalUserStateChangeDateTime) -Format g) }}
```

It all sounds simple, but the dependency on directory replication makes this approach to creating guests difficult to use in practice. For that reason, it is best to use the applications that you want to use guests with to invite those guests so that Entra ID creates their accounts through the redemption process.

Converting External Accounts to Become Internal Accounts

A preview feature is available to convert external accounts to internal accounts using an option in the Entra admin center or PowerShell. The criteria to determine the internal or external status for an account is how it authenticates. If the account authenticates with the tenant, it is an internal account. If it authenticates elsewhere, such as with another Microsoft 365 tenant, it is deemed to be external. The most common form of external account found in Microsoft 365 tenants are guest accounts and the accounts synchronized through membership of a multi-tenant organization also come into this category.

The process preserves group memberships for the external account and most of the account properties except for the user principal name and password, which must change to allow the converted account to sign into the tenant. See [this article](#) for more information about the process and a script to convert an account using PowerShell.

Restricting Guest Access

The [Azure AD Guest user access restrictions policy](#) in the [External Collaboration page](#) of the Entra admin center allows tenants to control the level of access guests have to Entra ID information. Three options are available:

- Guests have the same access as members (most inclusive) setting means guests have the same access to directory data as regular users in your directory.
- Guests have limited access to properties and membership of directory object settings. Guests don't have permissions for certain directory tasks, such as enumerating users, groups, or other directory resources. This is the default setting.
- Guests are restricted to properties and memberships of their directory objects (most restrictive).

Most Microsoft 365 apps currently are unaffected if the most restrictive level is selected. This might change in the future as product groups work out how to exploit the feature. For instance, Teams might not allow guests to see details of team membership.

Cleaning Up Old Guest Accounts

Many reasons exist to justify the creation of a guest account in a Microsoft 365 tenant. For example:

- An external expert is asked to review a document stored in SharePoint Online and receives a sharing link for this purpose.
- Someone is asked to join a Microsoft 365 group or team. If their account is outside the tenant, a guest account is created for them when the invitation is issued. Access to shared channels in Teams doesn't use guest accounts.

Over time, the reason why an external person has a guest account in a tenant might wane. For example:

- A guest account is used to review a shared document and is not needed thereafter.
- External people leave a team (or teams) and their guest account remains in Entra ID.
- People leave their employer and move on to new challenges. Their guest account is invalid because they can no longer authenticate using the Entra ID instance for the tenant of their old employer.
- Projects come to a natural end and the associated teams and/or private channels and their guest members are no longer needed.

Although it's possible to add expiration dates to guest accounts, processing accounts to remove them when they expire must be done manually or [with PowerShell](#). You can, of course, leave guest accounts in place on the basis that they might be needed in the future, but usually, it is a better idea to clean things up and remove these accounts when they are no longer used, especially because these accounts have access to tenant resources. Several ways exist to control the longevity of guest accounts in a tenant. You can:

- Use the script described in the PowerShell book (see the section "Finding Inactive Guest Accounts") to find groups with external members and then check the individual members of each group.
- Check guest accounts based on their activity level. The "Finding Inactive Guest Accounts Based on Activity" section in the PowerShell book describes how to use data from the audit log and email tracking logs to calculate the last activity for guest users. If a guest hasn't been active for months, perhaps it is time to remove their account.
- Deploy [Entra Access Reviews](#) to force group owners to check the memberships of the groups they manage and attest that group members should keep or lose their status. You can also periodically ask guests to attest if they still need access to your tenant. Finally, you can scope access reviews to groups that Entra ID determines to be inactive. This can be very helpful in situations where you have countless guest users in your tenant and no record of who invited their account. Access Reviews requires Entra ID P2. A Graph API is available for programmatic access to access reviews (see this [example script](#)).

Another approach uses a feature that [tracks sponsors](#) for guest accounts. When the time comes to review guest accounts, administrators can contact a guest's sponsor(s) to see if their account is still necessary.

After identifying guest accounts for removal, you can ask group owners to remove them or do so programmatically or through an administrative portal. Here's an example of using the *Remove-UnifiedGroupLinks* cmdlet to remove a member. If an account is a group owner, remember to remove it from the owner list first.

```
Remove-UnifiedGroupLinks -Identity "GDPR Planning Mark II" -LinkType Member -Links  
JackSmith_hotmail.com#EXT#
```

To remove a guest account completely, run the *Remove-MgUser* cmdlet:

```
Remove-MgUser -UserId JackSmith_hotmail.com#EXT#@office365itpros.onmicrosoft.com
```

Alternatively, you can leave it to individual guests to decide when it is time to remove their account from your tenant. A user can belong to up to 500 Entra ID tenants. By default, guests can also choose to leave a tenant and remove their guest account at any time. To leave a tenant, the user goes to the Entra ID [My Account](#) page and selects **Organizations** (they can also navigate to the page via Microsoft Teams). Entra ID lists the tenants where the user has a guest account. To leave a tenant, select **Leave**, and then confirm the decision by clicking **Leave** again (the user might have to sign into the tenant first). Entra ID then removes the guest account from the chosen tenant directory, signs the user out of the tenant, and sends an email to confirm that they have left the organization and can no longer access applications in that tenant. Leaving an organization only removes the guest account; it does nothing to remove any data which the user created in that tenant.

Following its removal, a guest account stays in a soft-deleted state for 30 days. During this period, the tenant administrator can restore the guest account, or complete the process by removing the account permanently. Removal of a guest account means that it loses all access to SharePoint and OneDrive documents, libraries, and lists that it has access to on an individual basis or through a group. The guest account also loses access to its membership of any Teams.

If you don't want to allow guests to leave your tenant, you can configure a setting to block this action. To configure this setting, go to **External Identities** in the Entra admin center. Go to **External collaboration settings** and then configure **External user leave settings**. If you configure the External user leave settings to No, you must have a privacy policy configured for your tenant. To configure a privacy policy, navigate to **Overview > Properties** in the Entra admin center and then configure the **Privacy statement URL** setting.

Entitlement management: [Entra entitlement management](#) is functionality to enable tenants to manage access to groups, applications, and sites at scale. You define access packages to describe the resources users can access and then assign the packages to users, making it easy to remove access to multiple resources at one time by removing an account's access to a package. Entitlement management requires Entra ID P2.

Cross-Tenant Settings

One of the challenges of Entra External Identities is the potential to allow guests from competitors access to tenant resources or to allow users from your organization to join teams and groups in a competitor's tenant. Collaborating across clouds (e.g., Azure China operated by 21Vianet or Azure Government) also requires special considerations. To mitigate this, Entra ID provides controls to limit guest collaboration. These controls come through external collaboration settings as well as cross-tenant access settings.

Cross-tenant access settings are the primary control that you should plan to use where possible. The primary limitation of cross-tenant access settings is that they cannot control the invitation of consumer identities (e.g., Gmail) or other domain names that are not verified in an Entra ID tenant. For these scenarios, you should use external collaboration settings.

Both groups of settings are available in the Entra admin center under **External Identities > External collaboration settings**. External collaboration settings allow you to determine what email domain names can be invited to collaborate with your tenant as guests. You can use the following settings under **Collaboration restrictions**:

- **Allow invitations to be sent to any domain (most inclusive)** – this allows collaboration in your tenant with any guest user
- **Deny invitations to the specified domains** – this allows collaboration in your tenant with any guest user, except guests from the domain names listed (e.g., a competitor)
- **Allow invitations only to the specified domains (most restrictive)** - in this scenario, you must whitelist individual domain names that you will allow guests into your tenant from

An important distinction between external collaboration settings and cross-tenant access settings, which we'll discuss next, is that external collaboration settings only control guests coming *into* your tenant. You must use cross-tenant access settings to control what tenants your users can be guests in. With cross-tenant access settings, you can apply much finer-grained control of guest behavior in your tenant ("inbound" access) and where your users can be guests ("outbound" access).

Rather than a domain name-based approach, cross-tenant access settings work on a tenant basis. You can control from which domains guest users can access your tenant, as well as what applications they can access in your tenant. You might choose to allow all users in another tenant to become guests in your tenant, or you might choose to only allow specific users to access specific applications as a guest. The granularity of control

that you choose will be a balance of managing risk and the operational overhead. You can apply similar controls in the opposite (outbound) direction to control what tenants your users can become guests in and what applications they can access in those tenants.

In Figure 2-3, the default settings for the tenant are configured to block all inbound access while permitting outbound access to any tenant. Direct Connect, used with shared channels in Microsoft Teams is blocked by default. You can configure specific settings for tenants that you want to override the defaults for – either allowing inbound access to your tenant or blocking outbound access from your tenant.

The screenshot shows the 'Cross-tenant access settings' page in the Azure portal. The left sidebar includes links for Overview, Cross-tenant access settings (selected), All identity providers, External collaboration settings, Diagnose and solve problems, Self-service sign up, Custom user attributes, All API connectors, Custom authentication extensions (Preview), User flows, Subscriptions, Linked subscriptions, Lifecycle management, Terms of use, Access reviews, Troubleshooting + Support, and New support request. The main content area has tabs for Organizational settings, Default settings (selected), and Microsoft cloud settings. A note states: 'Modifying default settings impact all collaboration with other Azure AD organizations. Click here to learn how to identify your existing inbound and outbound collaborations.' Below this, the 'Inbound access settings' section shows a table:

Type	Applies to	Status
B2B collaboration	External users and groups	All blocked
B2B collaboration	Applications	All blocked
B2B direct connect	External users and groups	All blocked
B2B direct connect	Applications	All blocked
Trust settings	N/A	Disabled

The 'Outbound access settings' section shows a table:

Type	Applies to	Status
B2B collaboration	Users and groups	All allowed
B2B collaboration	External applications	All allowed
B2B direct connect	Users and groups	All blocked
B2B direct connect	External applications	All blocked

Figure 2-3: Default cross-tenant access settings

To configure settings for a specific tenant, go to **Cross-tenant access settings**, and click **Add organization** on the toolbar. Enter a domain name valid for the tenant you want to configure and then click **Add**. Note that these settings will apply to the entire tenant, not just that domain name. You will see that the *Inbound access* and *Outbound access* columns say *Inherited from default*. The defaults are inherited from the settings on the **Default settings** tab, shown in Figure 2-3. Click **Inherited from default** and then choose **Customize settings** on the **B2B collaboration** tab to configure tenant-specific settings:

- **External users and groups** – You can choose to **Allow access** or **Block access** from this tenant (inbound) or to this tenant (outbound). For inbound access, if you choose to **Select <external tenant> users and groups**, you must provide the object identifiers for the individual users and groups that you want to allow access for. You can obtain the identifiers from an administrator in the external tenant. For outbound access, you can select the users and groups from your tenant allowed to become guests in the tenant.
- **Applications** – If you **Select applications**, you can choose the applications in your tenant that guests have inbound access to. For outbound access, if you **Select applications**, you must provide the

application ID from the external tenant that users in your tenant can access. You can obtain the application ID from an administrator of the external tenant.

In Figure 2-4, we have configured settings for the Redmond & Associates tenant to permit inbound access. In other words, users in the Redmond & Associates tenant can access applications in the pictured tenant as a guest user. This overrides the default settings shown in Figure 2-3 that block inbound guest access.

The screenshot shows the 'Organizational settings' tab selected in the top navigation bar. Below it, there are buttons for 'Add organization', 'Refresh', and 'Columns'. A search bar at the top right says 'Search by domain name or tenant ID'. A message bar at the top states: 'Use cross-tenant access settings to manage collaboration with external Azure AD organizations. For non-Azure AD organizations, use collaboration settings. [Edit](#) or view collaboration restrictions'. Another message below it says: 'Organizational settings are cross-tenant access settings you've configured for specific Azure AD organizations. Any Azure AD organizations not listed here will use the default settings.' There is a 'Learn more' link with a help icon. The main table has one row, showing the Redmond & Associates tenant with 'Inbound access' set to 'Configured', 'Outbound access' set to 'Inherited from default', and 'Tenant restrictions' also set to 'Inherited from default'. The table header includes columns for Name, Inbound access, Outbound access, and Tenant restrictions.

Name	Inbound access	Outbound access	Tenant restrictions
Redmond & Associates	Configured	Inherited from default	Inherited from default

Figure 2-4: Inbound access settings for a tenant

Ordinarily, when a guest user accesses your tenant for the first time, they must provide consent to sharing certain information about them. If you are collaborating with another tenant under your organization's umbrella, or with a close business partner where you do not need to collect consent, you can hide the consent prompt. To achieve this, both your tenant and the guest's tenant must configure consent suppression. This setting is found on the **Trust Settings** tab when you configure Inbound access or Outbound access settings.

For inbound access settings, you can also configure trust settings for the external tenant. We discuss how these settings work in the discussion about Conditional Access. You might find that cross-tenant access settings do not work quite how you would expect, especially if you have used external collaboration settings before. External collaboration settings control what domain names can receive an invitation to become a guest. Applications like SharePoint Online, OneDrive for Business, and Teams generate invitations when a user tries to share content in SharePoint, OneDrive for Business, or Microsoft Teams. When a user attempts to share with a blocked domain, the user receives an error message when they try to send an invitation. With cross-tenant access settings, users can send invitations to users in tenants that are on the collaboration blocklist. When the guest tries to accept the invitation to collaborate, they will receive an error message that they cannot access your tenant. We expect that this inconsistent experience will evolve as cross-tenant access settings mature.

You can also use cross-tenant access settings to control a feature called Entra External Identities Direct Connect. Teams is the first application to use Direct Connect in its shared channels feature. Shared channels allow users to join a Teams channel without having a guest account in the channel's home tenant. Users can also see the channel in their Teams client without changing tenants. The default cross-tenant access settings block Direct Connect for all users in your tenant and inbound connections from external tenants.

There are two sets of settings for Direct Connect. Inbound access settings allow you to control which external tenants can access your tenant. Outbound access settings control the users from your tenant can access resources in external tenants. You can enable Inbound or Outbound access globally, or you can enable it only for select users (or groups). If you have a tenant in Azure Government (GCC-High or DoD) and you want to allow guests from Azure Commercial tenants to access your tenant, or vice-versa, you must enable cross-cloud collaboration. These settings are found by browsing to **Cross-tenant access settings** and then opening the **Microsoft cloud settings** tab. In an Azure Government tenant, you must check the **Microsoft Azure**

Commercial checkbox. In an Azure Commercial tenant, you must check the **Microsoft Azure Government** checkbox. Once you have checked the appropriate box on each side of the relationship, you must add the tenants on the **Organizational settings** tab as discussed above. You should be careful when you enable cross-cloud collaboration to ensure that you do not negatively impact your organization's security and compliance obligations, particularly in Azure Government.

You can also collaborate between Azure Commercial and Azure China using the same steps. All the Entra External Identities collaboration features work as expected between clouds, however Direct Connect is not supported across clouds.

Protecting Identities

Microsoft has made significant investments in delivering features in Entra ID (and even on-premises) to combat the threats to identities. In today's world, every organization should have MFA deployed across the enterprise and enforced for all users. Even with MFA, passwords are still a problem. Traditional password policies that require frequent password changes and complexity rules that are difficult to comply with lead to people picking even worse passwords. Entra Password Protection is an important tool to mitigate some of the risks of passwords.

End users are ultimately the most familiar with their behaviors. Entra ID makes sign-in logs available for users to review directly by visiting <https://mysignins.microsoft.com>. Information about each of the user's sign-in attempts including whether they succeeded and the location (city) where the attempt originated are all presented in a searchable list. This same sign-in data is available tenant-wide to administrators in the **Monitoring & health** section in the Entra admin center.

Password Protection

Users often choose poor passwords. Sometimes they reuse passwords between services; other times they choose easily guessed passwords. Microsoft has long tried to educate both users and administrators about the rules of good password hygiene, and the on-premises Windows Server operating system has a long-standing [password filter feature](#) that allows you to install custom code to check proposed passwords when users try to change them on-premises. Two similar sets of Entra ID features are available to do this: [one for standalone identities](#) and the other for hybrid identities that are synchronized to the cloud.

First, for user accounts homed in the cloud, Entra ID applies a global banned password list when a password change is requested. All the old standards, such as "passw0rd" and "password123," are here, as are many others; the list is gleaned from password breach data that the Microsoft Security Intelligence center gathers, as well as from other factors. The suggested new password is first put through a set of normalization rules, then checked against the global banned password list, then checked against the organization's custom banned password list if you've defined one. The global banned password list is available to all tenants, but defining a custom banned password list requires an Entra ID P1 license for each user.

The on-premises equivalent of this feature is more complex. To use it, you install an agent on your DCs that checks password change requests against the Entra ID banned password list. There is also a proxy agent, which downloads the password policy from the service and makes it available to the DCs. When a user tries to change her password, the local DC agent (which is implemented using the password-filter mechanism in on-premises AD) checks it against the most recent list and either allows or blocks the change. The good news: this approach means that your cloud and on-premises identities receive the same protection and use the same banned-password lists. The bad news is that the on-premises capability requires you to purchase Entra ID P1 licenses for each user.

Hardening User Passwords: Entra ID allows accounts to have passwords of up to 256 characters.

Increasing the password length by just a single character dramatically increases the time to brute-force guess the password. However, as computers become increasingly more powerful, the processing needed to brute-force guess a password also decreases, and continually increasing the password length is not a long-term solution. If you want to use a long 200-character password, feel free, but there is a better solution now. After years of telling users that they needed long, complex passwords, the US National Institute of Standards and Technology (NIST) introduced a [new set of recommendations](#):

1. Use pass phrases instead of passwords. Phrases are easier for humans to remember.
2. Choose phrases with unique associations that only you will know.
3. Eliminate character-composition requirements.
4. Do not require passwords to expire.
5. Ban common passwords, to keep the most vulnerable passwords out of your system.
6. Educate users not to re-use their passwords for non-work-related purposes.
7. Enforce the use of multi-factor authentication wherever possible.
8. Enable risk-based multi-factor authentication challenges.

The [full NIST recommendation](#) makes for interesting reading, but if you implement the suggestions above, you'll greatly increase your security and, not incidentally, make your users happy. In addition to hardening user passwords, you should also monitor authentication attempts to track and report suspicious activities. Both options are discussed later.

Password Protection helps protect you from password spray attacks. Password spray attacks are a common technique used by adversaries to test common passwords and evade detection. In a password spray attack, an adversary will try the same password (for example, Winter2021) on hundreds or even thousands of accounts at a time. Because only one failed authentication occurs per-user account, typical detections for brute force attacks are bypassed. You can use Attack Simulation Training in Defender for Office 365, discussed in the Mail flow chapter, to simulate a password spray attack against your tenant.

Password Writeback

Password writeback allows users and administrators to change or reset Entra ID passwords and have that password propagate to the on-premises user account in real-time. The ability to write back passwords is integrated with Entra ID's [self-service password reset \(SSPR\)](#) capability and licensed through Entra ID P1.

This is how password writeback works:

1. The user clicks a link to request a password change.
2. The user enters their old and new passwords (or completes one or more challenge gates in the case of a forgotten password).
3. The selected password is encrypted with a special key that was created during the setup of the password writeback feature for that specific tenant.
4. The encrypted password is sent over HTTPS to a tenant-specific service bus endpoint which is used to communicate with the on-premises password writeback service. Communications on this bus are protected by a shared credential that was created during the setup of the password writeback feature and is only known to your organization and Entra ID.
5. The writeback feature looks for the user account in the on-premises AD. To find a match, the `sourceAnchor` is used to look up the user in the Entra Connect connector space. From there, the object is traced back through the metaverse to AD.
6. If the user account is found, the password is reset. If the reset is successful, the user is notified.
7. If the password reset operation fails, an error is returned to the user. One of the reasons the password reset might fail is when it does not satisfy the on-premises password policy. If the password writeback service running inside of Entra Connect is unavailable, the operation will also fail.

The password writeback features can also be deployed without using password hash synchronization; you can also deploy password writeback alongside AD FS. You can also enable users to unlock their on-premises AD account using SSPR and password writeback.

Configuring Password Writeback

Password writeback can be enabled as part of the Express and Custom installation modes for Entra Connect, or through PowerShell. The easiest way to enable password writeback is to select the password writeback option in the Optional Features section of the Entra Connect setup wizard. If you let the setup wizard configure the service account for Entra Connect, you do not need to make any further changes in AD.

Configuring Self-Service Password Reset

The password writeback feature also works when an administrator changes the password for a user from the Entra admin center, but it is most useful when combined with the SSPR capability in Entra ID so that users can update their password without having to worry about the passwords getting out of sync.

SSPR is managed in the **Protection > Password reset** blade of the Entra admin center. Once SSPR is enabled, you can modify the policy to control various aspects of the password management features in Microsoft 365/Entra ID, such as whether users are required to provide multiple verification methods (to verify their identity), and if so, what verification options they should use.

We recommend that you enable only a few of the available verification methods for SSPR. Specifically, we suggest that you use the mobile app notification, mobile app code, and mobile phone options if they work for your organization. Security questions are useful in situations where your users might need to reset their password for a location without access to their phone, or where you cannot require your users to provide a mobile phone to enroll. Be very careful when you pick your security questions. Security questions should capture details that only a user will know, and that cannot be easily researched by an adversary on social media.

You can use the **Protection > Password reset > Authentication Methods** settings in Entra ID to control which methods are available to users for password reset. Microsoft is deprecating the authentication methods configuration in the Password reset blade and is replacing them with the unified settings under **Protection > Authentication methods > Policy**. You should begin to migrate to the new unified settings before the planned deprecation in September 2025 by following [these steps](#).

You can also require your users to periodically confirm their SSPR registration details are still correct. We recommend that you configure this setting to be once or twice a year. After all, if the details are no longer correct, the user must call for support, which defeats the point of SSPR.

Reporting Accounts Not Capable for SSPR

After configuring the tenant to support SSPR, you might like to check what user accounts are unable to use SSPR for some reason. This PowerShell code looks for Entra ID accounts with assigned licenses and cross-checks the accounts against those noted as not being able to use SSPR.

```
Connect-MgGraph -Scope Directory.Read.All, UserAuthenticationMethod.Read.All

Write-Host "Finding licensed Entra ID accounts"
[array]$Users = Get-MgUser -Filter "assignedLicenses/`$count ne 0 and userType eq 'Member'" -ConsistencyLevel eventual -CountVariable Records -All
# Populate a hash table with the details
$userTable = @{}
$Users.ForEach( { $userTable.Add([String]$_.Id, $_.displayName) } )
Write-Host "Finding user accounts not capable of Self-Service Password Reset (SSPR)"
[array]$SSPRUsers = Get-MgReportAuthenticationMethodUserRegistrationDetail | Where-Object {$_ .userType -eq 'member' -and $_ .IsSSPRCapable -eq $False}
Write-Host "Cross-checking against licensed users..."
```

```
[array]$NonSSPR = $Null
ForEach ($S in $SSPRUsers) {
    $DisplayName = $UserTable.Item($S.Id)
    If ($DisplayName) {
        $NonSSPR += $DisplayName
    }
}
$PNonSSPR = ($NonSSPR.Count/$Users.Count).ToString("P")
Write-Host ("{0} out of {1} licensed accounts ({2}) are not enabled for Self-Service Password Reset"
-f $NonSSPR.Count, $Users.Count, $PNonSSPR )
```

A more developed version of the script is [explained in this article](#).

User Risk and Self-Service Password Writeback

Entra ID P2 includes Microsoft's Entra Identity Protection capabilities. One of the capabilities of Identity Protection is the ability to measure and report on risk scores for individual users. For example, if Microsoft finds a valid password for a user in a list of leaked credentials on the Internet, the user's risk score will be rated high. Entra Identity Protection evaluates numerous other factors to compute a risk score. Microsoft maintains a list [here](#).

You can configure the user risk policy in Entra ID to act when Microsoft assigns a high-risk score to a user. Two actions are available in the user risk policy. The first is to block the user from further sign-in until an administrator unblocks the account. The other option enables self-remediation. The next time the user signs in, after completing MFA, they must change their password. Entra ID writes the updated password to the on-premises AD using password writeback. If the user changes their password in on-premises AD, their risk will also be reset. Configure the user risk policy inside the Entra admin center by navigating to **Protection > Identity Protection**. You can leverage user risk and sign-in risk more granularly through conditional access policies, discussed later in this chapter.

Multi-Factor Authentication

Because of how people use them, passwords are inherently insecure. Some years ago, it would take a computer a very long time to crack or guess a password. As such, even the simplest passwords were secure enough to protect against most forms of attacks. However, as hardware became more powerful, the time needed for a computer to crack a password decreased exponentially. Today, with the right hardware, a simple six-character password can be cracked in a matter of minutes! To make it harder for passwords to be brute-force guessed, or at least to increase the time it takes, the advice is to use longer and more complex passwords. Unfortunately, research has shown that requiring longer, more complex passwords that periodically expire can lead to the selection of passwords that are sometimes easier to guess. Even with a complex password, the password is subject to phishing attacks.

When you think about it, authentications are based on a combination of three things: something you know (such as a pass phrase), something you have (like a physical token), or something you are (a biometric marker of some kind). Traditional password-based authentication combines your username with something you know, but anyone else who knows the same thing can pretend to be you.

An attacker who manages to steal a password, either by brute force guessing or through social engineering, might be able to leverage the stolen password to access multiple sites. Users who pick weak passwords, write passwords down, store them insecurely, or give them up to social engineering attempts aren't necessarily to blame; although many credential thefts are the result of user carelessness, it's difficult to blame non-technical users for making these mistakes when an average user must keep track of multiple credentials for different sites and applications, each with its length and strength requirements. Although password management tools can help with remembering passwords, those tools are often protected by a single password themselves.

Since knowing a user's password allows an attacker to perfectly impersonate the user, poor password management means that users are vulnerable to impersonation. To help fix this, we have several options. One

is to make it harder to guess or crack passwords; another is to harden systems, and train users, to reduce the chances that an attacker can steal the password. A third option is to require the user to provide more than one type of authentication factor, which is where the “multi-factor” part of MFA comes in. Passwordless authentication is a fourth option.

The principle behind MFA is that you add a second (or even third) factor from the “something you have” or “something you are” categories. Typically, MFA is implemented as a combination of a password with a smartcard or hardware token, one-time generated code, mobile app notification, or biometric information such as a fingerprint, facial recognition, or an iris scan. To gain access to a system, an attacker would have to have access to both the additional token and the user’s password. Although adding an additional factor to the authentication is a huge leap forward in terms of security, it does not take away all risks that entail the use of passwords.

Real-world: MFA is a valuable security measure, but it is not a replacement for good password and account management, and it has vulnerabilities of its own. For example, there have been several high-profile targeted attacks on MFA. In some cases, attackers took control of the target’s mobile phone number by convincing the mobile carrier to issue a new SIM so that the attacker received the MFA authentication code required to execute a password change. Even with MFA deployed and enforced, you should still be monitoring your users’ logon activity for anomalies, and where possible, you should discourage the use of MFA methods that are not phish resistant including SMS, phone calls, verification codes, and OATH tokens. NIST [guidance](#) also recommends against using SMS MFA.

Entra MFA and Office 365 MFA

The Entra MFA feature allows people to use multi-factor authentication to secure their accounts. A subset of Entra MFA features is available in Office 365 MFA. Although Office 365 MFA and Entra MFA are very similar in terms of functionality, the latter requires Entra ID P1. Two notable differences between Entra MFA and Office 365 MFA are:

- Office 365 MFA can only be used to secure access to first-party Office 365 workloads (e.g., Exchange Online, SharePoint Online, etc.). Entra MFA extends beyond these workloads and can protect other cloud and on-premises resources.
- Office 365 MFA supports per-user configuration. Entra MFA uses conditional access policies to enforce a requirement that connections use multifactor authentication.

Entra MFA supports the following additional authentication options:

- Mobile app ([Microsoft Authenticator](#) or third-party authenticators) for Android and iOS:
 - Notification: the user receives a notification in the mobile app to ask them to confirm their identity by entering a two-digit number and clicking the **Approve** button. Once the user confirms, they log in automatically.
 - Verification Code: the mobile app generates a new code every 30 seconds. After the user enters the current code (on-screen), the sign-in process continues.
 - Authenticator app sign-in: Also known as “passwordless sign-in”, in this mode the standard Microsoft sign-in dialog will display a two-digit number and generate a request to the Authenticator app asking you to enter the matching number on-screen. This method lets users log in using their phone with no password entry. See the [documentation](#) for more details on how to set this up.
- Phone call. The user receives a phone call, asking them to confirm that they are signing in by pressing the # key. After confirming, the user logs in automatically; no code is necessary.
- Text Message (SMS). A one-time passcode (6 digits) is sent to the user’s mobile device. This code must be entered before the sign-in process can continue. Users in India, Indonesia, and New Zealand can also receive SMS-based OTPs via WhatsApp.

- OATH Hardware Token. The user uses a physical token that generates a random one-time passcode every thirty or sixty seconds. These tokens are often useful in scenarios where the user cannot access their mobile phone when they need to complete MFA.
- Passkey or FIDO2 Token. The user uses a physical device that is associated with their account and compliant with the [FIDO2 standard](#). Many vendors make FIDO2 tokens in a variety of different form factors. FIDO2 tokens are highly phish-resistant so they provide a higher level of assurance when authenticating a user.
- Additional [third-party authentication methods](#), including those from RSA Data Security and Duo Security. If you want to use a third-party authenticator, you need Entra ID P1 licenses.

All administrative accounts should be protected with MFA. In a [November 2023 blog post](#), Microsoft VP for Identity Security Alex Weinert noted that 37% of Entra ID accounts have MFA protection enabled. Although these percentages mark an improvement (in 2018, only 1.8% of Entra ID accounts used MFA; in 2019 the figure was 9%), they're still disappointing. Implementation of modern authentication throughout Microsoft 365 means that old excuses like not using MFA to protect accounts used to run PowerShell are invalid. Microsoft has made it easier to do so by enabling security defaults in all tenants that don't already use MFA or conditional access policies. To further secure existing tenants, Microsoft added managed conditional access policies to require MFA in more situations. We discuss these policies later in the Conditional Access section.

Prioritizing the Authenticator App

In any organization that has deployed MFA for some time, the chances are your users may be using a mixture of voice calls, SMS messages, and the Authenticator app to perform MFA. The Authenticator app provides the most secure verification, and it offers additional valuable capabilities such as one-time pass codes, passwordless sign-in, and authentication broker support on iOS devices. It can be difficult to convert users from voice calls or SMS to the Authenticator app, though.

Entra ID can encourage this conversion through an in-line prompt to set up Authenticator. This prompt comes after the user completes their sign-in and MFA and only if they have not yet enrolled in the Authenticator app. To enable this prompt, navigate to **Protection > Authentication Methods > Registration campaign** in the Entra admin center. From here you can enable the prompt, configure how many days an end-user can ignore (snooze) the prompt, and optionally, target the prompt to a subset of users. If your registration campaign settings are set to Microsoft Managed, Microsoft will prompt users to set up the Authenticator app if they SMS or phone-based authentication.

In addition to this feature that prompts users to set up Authenticator, you can also enroll directly in the Authenticator app without scanning a QR code. Simply add a **Work or school account** in the Authenticator app and then click **Sign in** when prompted.

When configured correctly, the Authenticator app is the ideal mass-market MFA method. As MFA has become more prevalent, attackers have found ways to defeat it through phishing. Typically, the attacker sends MFA requests to the user (after compromising their password), and the user eventually becomes fatigued, and proceeds to tap 'approve' on their phone without further thought, letting the attacker in. To combat MFA challenge fatigue, Microsoft added number matching. The Authenticator app also filters push notifications for authentication requests that Microsoft determines to be suspicious. To respond to these requests, the user must open the Authenticator app and manually check for new notifications.

Number matching requires the end-user to input a random two-digit code into the Authenticator app when they are prompted for MFA. This virtually eliminates the chances of success through fatigue since there is a one in one-hundred chance of guessing the right number. It is still possible to phish this if the attacker contacts the user through an alternate channel and provides them with the two-digit code.

Entra ID also allows your organization to opt-in to dynamic security controls that prompt users who are enrolled for multiple MFA methods with the method that Microsoft deems to be the most secure. Microsoft documents this capability [here](#).

Although these features will not prevent a user from being convinced to approve a malicious MFA attempt in the Authenticator app, they provide significant barriers as well as context to help make a smart decision. Your security awareness training should cover good MFA decisions, in addition to traditional topics like clicking links in emails from external senders.

To reduce friction with adoption of MFA, Microsoft is also making a small subset of features from the Authenticator app available as "Authenticator Lite". The only app to include Authenticator Lite is Outlook Mobile. Authenticator Lite only supports push notifications with number matching and TOTP codes. It also cannot act as an authentication broker for other Microsoft apps on a mobile device. By default, Authenticator Lite is enabled. If you would like to disable Authenticator Lite for your organization, navigate to **Protection > Authentication Methods > Policies** and click on **Microsoft Authenticator**. On the Configure tab, set **Microsoft Authenticator on companion applications** to **Disabled**.

Configuring Accounts for MFA

If you have Entra ID P1, you can use conditional access policies to determine when a user must complete an MFA challenge. We discuss conditional access later and include samples of how to configure the policies. If you do not have Entra ID P1, you can use Security Defaults, also discussed later, to enforce MFA in your tenant. If you use the legacy Office 365 MFA settings accessible through the Entra admin center under **Users > All Users > Per-user MFA** and do not have Entra ID P1 licenses, you should consider migrating to Security Defaults. Microsoft plans to retire per-user MFA in the future.

To prepare for the eventual retirement of per-user MFA, you should begin migrating to Entra MFA and use conditional access policies to enforce MFA. The conditional access policies can apply to all users (preferably) or just those who use per-user MFA today. Settings you previously configured on the Service Settings page are now accessible in the Entra admin center under **Protection > Authentication methods > Policies**. Prior to the deprecation date, you can use both the Entra MFA and Office 365 configuration settings in parallel. Once you configure conditional access policies to meet your requirements, you should use the [migration feature](#) to disable the legacy Office 365 MFA settings.

You must enroll your users in MFA before they can begin to use MFA. If a user is not enrolled in MFA, they will be prompted to do so the next time they authenticate to a resource that requires it. You should consider how and where your users enroll for MFA. If you rely solely on prompting a user to enroll for MFA the first time they need to use it, it is very possible that an adversary might enroll on the user's behalf if they have compromised their password.

At a minimum, you can use conditional access to determine when a user can enroll for MFA. We discuss conditional access policies and applying policies to user actions such as MFA enrollment later. If the organization has Entra ID P2, you can configure an MFA registration policy to ensure that all users register for MFA. You can configure the MFA registration policy for your tenant by navigating to **Protection > Identity Protection > Multifactor authentication registration policy** in the Entra admin center.

To configure the MFA methods for a user account, find the user account in the Entra admin center, select **Authentication methods**, and then add the desired method. To reset the MFA enrollment for a user account, click **Require re-register multi-factor authentication** on the toolbar.

Scripting MFA Enablement

An administrator can also use PowerShell to configure MFA, [provision FIDO2 tokens](#), or to enable/disable MFA for users. In the following example, we enable an account for Phone-based MFA. You must connect to the

Microsoft Graph API with the *UserAuthenticationMethod.ReadWrite.All* permission. This script shows how to use Microsoft Graph PowerShell SDK cmdlets to work with SMS-based MFA challenges. The script:

- Declares the value of the identifier used for mobile phone number authentication method (the value is always the same).
- Gets the identifier for the target user account.
- Populates a hash table with the phone number to use and its type. The phone number must have a space between the international code and the local number. It should be unique within a tenant but doesn't have to be.
- Runs the *Get-MgUserAuthenticationPhoneMethod* cmdlet to check if a mobile phone number is already present in the account.
- If a phone number does not exist, the script runs the *New-MgUserAuthenticationPhoneMethod* to add it as an authentication method to the account.
- Alternatively, if a phone number exists, the script runs the *Remove-MgUserAuthenticationPhoneMethod* cmdlet to remove the old number and then adds the new number.

```
$MobilePhoneId = "3179e48a-750b-4051-897c-87b9720928f7"
$UserId = (Get-MgUser -UserId Lotte.Smith@Office365itpros.com).Id
$Params = @{
    PhoneNumber = "+353 862267785"
    PhoneType = "mobile"
}
$AuthPhone = Get-MgUserAuthenticationPhoneMethod -UserId $UserId -ErrorAction SilentlyContinue
If (!$AuthPhone) { # No authentication methods are there, so proceed
    New-MgUserAuthenticationPhoneMethod -UserId $UserId -BodyParameter $Params }
Else {
    Remove-MgUserAuthenticationPhoneMethod -UserId $UserId -PhoneAuthenticationMethodId
$MobilePhoneId -Erroraction Stop
    New-MgUserAuthenticationPhoneMethod -UserId $UserId -BodyParameter $Params }
```

The next time the account signs in, they will get an SMS MFA challenge (Figure 2-5).

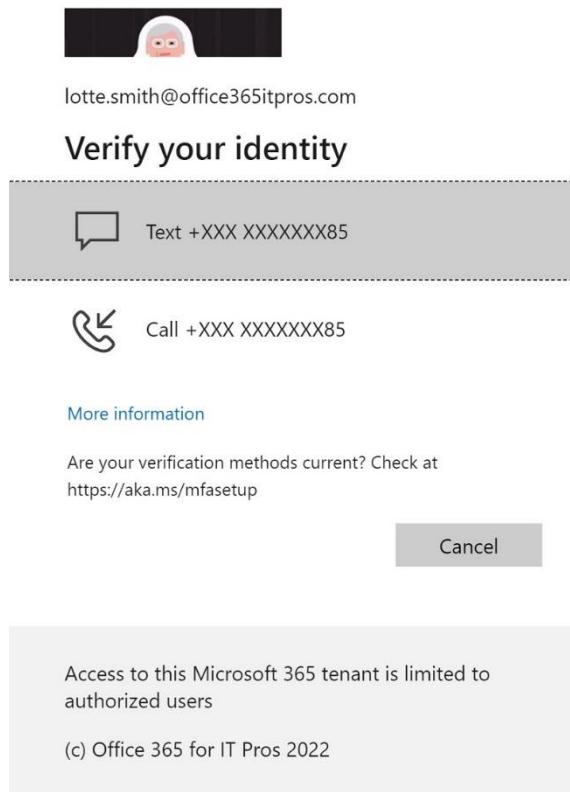


Figure 2-5: MFA sign-in using SMS

Removing Authentication Methods with a Script

If you run the `Get-MgUserAuthenticationMethod` cmdlet to return the full set of authentication methods for a user, you'll see that an account can have many authentication methods configured, including passwords. Each method has its own identifier:

```
$Methods = Get-MgUserAuthenticationMethod -UserId Jim.Smith@Office365itpros.com
$Methods.Id

Id
--
3179e48a-750b-4051-897c-87b9720928f7
3ddfcfc8-9383-446f-83cc-3ab9be4be18f
28c10230-6103-485e-b985-444c60001490
```

To remove a method, you must use the appropriate cmdlet. For example, to remove a FIDO key method, you use the `Remove-MgUserAuthenticationFido2Method` cmdlet. To find the method type, examine the `@odata.type` value in the `AdditionalProperties` property for a method. For example, this entry reveals that it is the phone authentication method, so the `Remove-MgUserAuthenticationPhoneMethod` cmdlet is the right choice to remove the method. You can't remove the default authentication method for an account unless it is the last (only) method. Unfortunately, the Graph doesn't return any indication about the default method. If a cmdlet returns an error when removing an authentication method, it might be that the chosen method is the default!

\$Methods[1].AdditionalProperties	
Key	Value
---	----
<code>@odata.type</code>	<code>#microsoft.graph.phoneAuthenticationMethod</code>
<code>phoneNumber</code>	<code>+1 617 881 4663</code>
<code>phoneType</code>	<code>mobile</code>
<code>smsSignInState</code>	<code>notConfigured</code>

Listing MFA-Enabled Accounts

When managing MFA for multiple users, it is useful to know which users are enabled for MFA, whether users have completed the onboarding process, or the verification options configured. You can access this information in the Entra admin center by accessing the **Monitoring & health > Usage & insights** blade and then selecting **Authentication methods activity**. From here you will be able to see (and export) information about MFA and SSPR enrollment. Note that you need an Entra ID P1 license to access the Usage & insights blade.

It's also possible to retrieve the information about the authentication methods used by Entra ID accounts using cmdlets in the Microsoft Graph PowerShell SDK. See [this article](#) and script for an example of how to report accounts that have registered MFA methods and use MFA for connections.

Tracking MFA Sign-ins

Like any other Entra ID sign-ins, MFA-enabled sign-ins appear in the [Entra ID sign-in logs](#). You can view the log interactively or download events to a CSV file and examine them afterward in Excel or Power BI. The Authentication Requirement column in the CSV file tracks whether the sign-in required MFA or not, while the status code captures the outcome of a sign-in attempt. Important codes include:

- **0**: Success.
- **50058**: An application tried to perform a silent sign-in (using an access token) to an MFA-enabled account but could not complete.
- **50076**: The user did not pass the MFA challenge because they did not respond in the allowed time.
- **50074**: The user did not pass the MFA challenge. For instance, they input an incorrect code. You can see the authentication method used in the MFA Auth Method column.

To look up the meaning of an Entra ID error code, use [this tool](#).

Using MFA

Users sometimes need some time to become accustomed to dealing with MFA challenges, but since so many other cloud services and applications support it (including Google's applications, Facebook, Apple iCloud, and almost every online banking system), MFA quickly becomes routine, needing minimal effort or thought. We recommend receiving notifications to the mobile app for authentication requests as the default MFA method. Because the mobile app needs a connection to the Internet to receive notifications, you might not always be able to use the app, for instance, when roaming in a foreign country or while you are on an airplane. In these cases, you can revert to another method, such as generating a verification code in the mobile app.

By default, the user's preferred additional verification option is used. If the user registered for multiple verification options, they can select a different method when their preferred verification method is (temporarily) unavailable or when the user doesn't respond to a challenge within a period. For instance, when the mobile app is unavailable because of a lack of Internet connectivity, a phone call or text message can be requested instead. To register for added verification options, the users must access their **My Sign-Ins** page. On the My Sign-Ins page, click **Security info**. From the Security info page (Figure 2-6), users can add extra phone numbers, configure the authenticator app, manage their SSPR registration (e.g., security questions and alternate email addresses), create passwords for use with registered apps, or change the preferred authentication method.

The screenshot shows the 'Security info' section of the Microsoft Entra admin center. On the left, there's a navigation menu with 'Overview', 'Security info' (which is selected and highlighted in blue), 'Organizations', 'Devices', and 'Privacy'. The main content area is titled 'Security info' and contains a sub-section 'These are the methods you use to sign into your account or reset your password.' Below this, it says 'Default sign-in method: Microsoft Authenticator - notification Change'. There's a button '+ Add sign-in method'. A table lists four sign-in methods:

Method	Device	Actions
Phone		Change Delete
Microsoft Authenticator Passwordless sign-in	iPhone	Delete
Security key	Feitian USB	Delete
Email		Change Delete

At the bottom, there's a link 'Lost device? Sign out everywhere'.

Figure 2-6: Changing MFA Verification Options for an account

Sometimes users complain about receiving too many authentication or MFA prompts from Entra ID. This can be because of the settings in the tenant policies; other times it is a result of devices or browsers missing important plugins or software updates. Microsoft has created an Azure Log Analytics Workbook to help diagnose authentication prompt frequency. This workbook is called [Authentication Prompts Analysis](#).

Managing Suspicious MFA Prompts

If a user's password is compromised and they are required to complete an MFA challenge as part of a sign-in, they will receive an MFA prompt when the attacker tries to sign-in with their compromised password. Number matching in MFA helps dramatically with the risk of users approving an MFA request that they did not complete. There is still a security issue you should investigate, however. You can now allow users to report suspicious MFA requests via the Authenticator App or a voice call.

When a user reports a suspicious MFA request, Entra ID marks their account as high risk. If you have Entra ID P2, you can use a conditional access policy to act based on the user's risk level. If you don't have Entra ID P2, you can still use the risky users report to identify users that are at an elevated risk level.

To enable reporting of suspicious MFA requests, go to **Protection > Authentication methods > Settings** in the Microsoft Entra admin center. Configure the **State** setting of *Report suspicious activity* to **Enabled**. You can optionally target a pilot group before enabling this feature for all users. If you support voice calls for MFA, the **Reporting code** setting controls what digit on the phone (0 by default) reports a suspicious request.

Controlling Access

For most organizations, the thought of allowing access to all their data from anywhere, at any time, on any device is not palatable. Microsoft has recognized this concern and made the conditional access features a core capability of Entra ID P1. With conditional access, you can exercise substantial granularity in controlling the who, what, when, and where of all connections.

Conditional Access Policies

By default, all users with a valid license can access resources available to their account if they can reach the service endpoint and log in. Sometimes, an organization might want to limit who can access resources, or perhaps control from which locations users can access those resources. Most Microsoft 365 applications do not provide such functionality. Instead, they leverage the advanced capabilities of Entra ID P1 and Microsoft Intune.

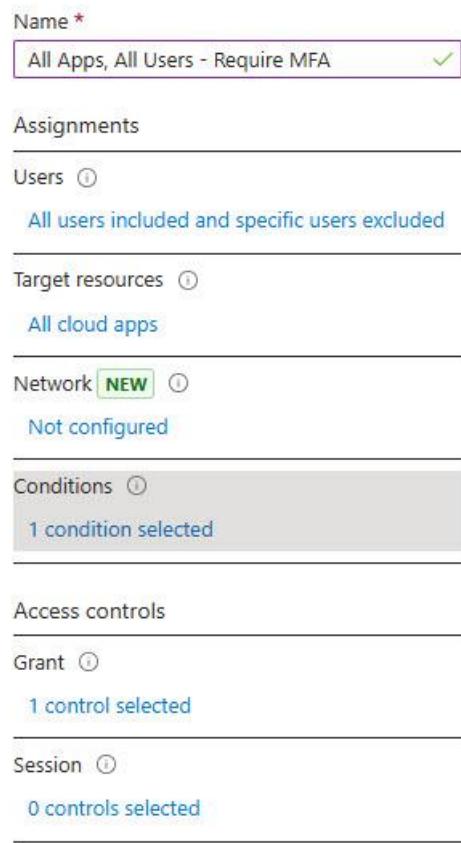


Figure 2-7: Settings available when creating a conditional access policy

Conditional access policies define rules that determine when and how a user or workload identity can access an application. Entra ID evaluates characteristics of the session such as the IP address, location, device, and sign-in risk score. If the device is enrolled with Microsoft Intune, the device's compliance with organizational policy as well as security risk determined by Microsoft Defender for Endpoint (MDE) can also factor into the conditional access policy. Collectively, these factors allow you to create policies to apply granular decisions about what sessions can access applications. These factors can also apply to certain activities such as whether a user can view documents in SharePoint Online, or view and download documents.

Numerous ways exist to restrict access to resources using conditional access policies. You can restrict who is allowed access to a resource, define which devices can be used to access resources or control from what locations an app or service can be used. You can also add restrictions based on the characteristics of the user logon; for example, if a user logs on from an unknown location, you can require them to authenticate with MFA even if the device itself would normally be trusted.

Before diving into an example of a conditional access policy, it is useful to know that each policy consists of one or more *conditions*, each of which can have a set of linked controls as illustrated in Figure 2-7. Conditions may have exceptions.

Conditions you can apply to the policy include:

- **Users** sets which users, guests, groups, directory roles, or service principals the policy should apply to. You can choose to include or exclude individual users or groups for the policy, or you can include or exclude all guest users or holders of specific Entra ID directory roles such as Global Administrators. Guests can be included or excluded individually or by group, or you can apply the policy to guests based on the [type of guest](#) they are. Finally, you can apply the policy to service principals via the

workload identities capability. This lets you restrict the use of service principals (also known as app registrations). Service principals often have highly privileged access to data in your tenant.

- **Target resources** define which applications the policy applies to or what user behaviors the policy applies to. You can choose to enable the policy for all applications or select the applications for which it should be valid. Applications include the various Office 365 workloads or a third-party application you configure to rely on Entra ID for authentication, like Salesforce, Workday, Facebook for Work, etc. Applying conditional access policies to individual Microsoft 365 workloads presents challenges to maintaining a consistent security posture. Microsoft has addressed this challenge by introducing a virtual application that represents all the workloads. This app can be selected in the **Cloud apps** section of a conditional access policy and is aptly named **Office 365**. Note that currently [some workloads](#), such as Microsoft Planner are not included in the Office 365 virtual application. Where possible, we recommend that you attempt to target your conditional access policies to the Office 365 virtual application rather than to individual workloads. Targeting individual workloads provides more flexibility but it also introduces [hidden complexities](#) due to the interdependencies of various workloads. A similar virtual application called **Microsoft Azure Management** is also available to target policy to Azure management tools like the Azure Portal, PowerShell, etc. The **Microsoft Admin Portals** virtual application allows you to target policy to the Azure portal, Exchange Admin center, Microsoft 365 admin center, [and more](#).

It's easy to target a conditional access policy to Office 365 since there is one virtual application. When you use conditional access to protect all your applications, this can become much harder. Many enterprises have thousands of applications, and they need to ensure that policies are applied consistently to different sets of applications. Entra ID lets you do this by applying custom security attributes to applications. You can include applications by query rather than using scripts or other methods to manually add them to the correct conditional access policies.

In addition to applications, you can also control when a user can register for MFA and SSPR or change their password (**Register security information**) and/or register or join a hybrid device (**Register or join devices**). This control is useful if your organization has a security policy that requires users to register for MFA/SSPR from a trusted device or location. To control what happens when the user registers or joins a hybrid device, you must also disable the corresponding MFA settings under **Devices > All devices > Device settings** in the Entra admin center.

Finally, you can create conditional access policies that are triggered when users perform specific tasks in supported applications by using Authentication contexts. An authentication context is a form of tag that administrators can assign to an object like a SharePoint Online site or an [Entra ID protected action](#). Conditional access policies can use authentication context to decide if it should allow an attempt to access the object. For instance, a conditional access policy could block access to specific SharePoint Online sites unless the session satisfies other conditions such as using multi-factor authentication and originating from a known location. Administrators create authentication contexts in the Entra admin center and assign the tags to SharePoint Online sites through container management (sensitivity) labels or PowerShell.

- **Network** identifies the physical location or source network the user is connecting from:
 - **Locations** are determined based on the IP of the client making the request, the user's Global Positioning System (GPS) location reported by the Authenticator app, or the country Microsoft infers the user is coming from.
 - **Networks** are based on Named locations defined in the tenant that define IP address ranges.
- **Conditions** define characteristics of the authentication attempt which lead to a policy to be applied or not. Examples of conditions include:

- **User risk** evaluates the risk of an individual user attempting to access the application. For example, a user whose password is in a list of leaked credentials is considered high risk. To use this condition, the target user must have Entra ID P2.
- **Sign-in risk** evaluates the risk that the sign-in attempt is coming from someone other than the authorized user. Microsoft evaluates sign-in risk using a complex supervised [machine learning model](#). To use this condition, the target account must have Entra ID P2. Sign-in risk can also be applied to workload identities. To use the sign-in risk condition for workload identities, you must select one or more workload identities in your tenant in the users or workload identities condition and the "*all cloud apps*" condition. This condition requires Entra Workload Identities which is a paid feature.
- **Insider Risk** allows you to make access decisions based on the user's risk score in Insider Risk Management. [Insider Risk Management](#) is a component of Microsoft Purview that correlates signals from Office 365 and external sources such as your human resources system to predict potential malicious or high-risk behaviors.
- **Device platforms** determine from which OS platform the authentication must be made before an action is considered. Options include Windows, iOS, Android, macOS, and Linux (in conjunction with Microsoft Edge).
- To define a location based on IP address, country, or GPS location, go to **Protection > Conditional Access > Named locations** in the Entra admin center and click **Countries location** (country or GPS location) or **IP ranges location** on the toolbar.
- **Client apps** determine what application type (browser, ActiveSync, mobile client, legacy authentication, etc.) should trigger the policy. Policies created before July 2020 only apply to the selected types of client apps (or "Other clients" for legacy authentication). All new policies apply to all client apps, including legacy authentication, by default.
- **Filters for devices** let you target the policy based on attributes of the device object in Entra ID. For example, you might want to have one conditional access policy apply to personal mobile devices, while another policy might apply to mobile devices that the organization owns. In combination with Intune, you can do this by creating a device filter rule. A filter rule of `device.deviceOwnership -eq "Personal"` will apply your policy only to devices marked as personally-owned in Microsoft Intune. A filter rule of `device.trustType -eq "ServerAD"` will apply your policy only to devices that are hybrid Entra joined.
- **Authentication flows** allow you to control whether users can engage in specific kinds of authentication. Microsoft recommends that you block the [device code flow](#) for all users unless it is necessary. You may find that certain situations require this flow. In this scenario, you should plan an exclusion group for your policy.

On the controls side (which you access through the link labeled **Grant**) you can choose from the following controls. There is also a radio button to control requiring any one of the actions selected (an *OR* condition) or all of them (an *AND* condition):

- **Block Access:** this is self-explanatory.
- **Grant (Allow) access**, with or without the following optional requirements:
 - **Require multi-factor authentication.** As the name implies, MFA must be used to complete a connection.
 - **Require authentication strength.** Requiring MFA is a very important security control, but, with the number of MFA methods available and the variability in their strength, you may want to require stronger forms of MFA or control how your users perform primary authentication. The authentication strength control lets you do exactly this. We show an example of how to use this control later in this section.

- **Require device to be marked as compliant.** For this option to work, the device must be enrolled in Microsoft Intune and targeted with a compliance policy. The rules in the compliance policy determine if the device will be marked compliant (or not).
 - **Require Microsoft Entra hybrid joined device** verifies whether the computer is simultaneously joined to the on-premises AD and Entra ID tenant.
 - **Require approved client app** lets you restrict whether applications must be accessed through a [supported](#) client application instead of through a third-party application or a bare API. Note that this control will be retired in March 2026. You should use the Require app protection policy control instead.
 - **Require app protection policy** allows you to restrict connections to apps that are subject to a Microsoft Intune app protection policy applied in your tenant.
 - **Terms of use** allows you to require users to view and accept text stored in a PDF document before they access an application. You must first create a terms of use document in Entra ID before you can use this control. To create a terms of use document, go to **Protection > Conditional Access > Terms of use** in the Entra admin center and click **New terms** on the toolbar.
 - **Require password change** allows you to force a user to change their password through SSPR. This grant is usually combined with the user risk condition to lower the user's risk score.
- **Session:** this control lets you restrict what authenticated users can do within the context of a specific application session:
 - **Use app enforced restriction** lets you enforce what users can do in Exchange Online or SharePoint Online such as printing and downloading attachments/files.
 - **Use Conditional Access App Control** integrates with Microsoft Defender for Cloud Apps (MDCA) to apply deep controls to actions users take within an application. This control proxies all the user's access to the application through MDCA.
 - **Sign-in frequency** lets you control how often the user must re-authenticate. You can also force a sign-in to occur every time an application is accessed.
 - **Persistent browser session** controls how long the user can remain signed-in to browser-based applications.
 - **Customize continuous access evaluation** allows you to disable CAE (discussed earlier) or enable strict enforcement of location policies. Strict enforcement of location policies requires additional planning and network configuration to avoid unexpected results. Review [this document](#) for details on planning for strict enforcement.
 - **Disable resilience defaults** provides the option to disable the safeguards of the BAS during an Entra ID outage. The BAS still evaluates tokens using CAE to ensure they are valid (e.g., due to the deletion or disabling of a user account) but assumes that conditions in a conditional access policy that were previously satisfied when a cached token was issued (such as group membership) are still valid. If you are uncomfortable with these assumptions, you can enable this session control, but, in the event of an Entra ID outage, any users included in the conditional access policy cannot take advantage of the BAS.
 - **Require token protection for sign-in sessions (Preview)** adds additional checks to ensure that the token presented by the user is cryptographically bound to the device that it is being used from. This control currently only works with Exchange Online and SharePoint Online via Office applications. There are additional restrictions and caveats that Microsoft [documents here](#).

As you begin building conditional access policies, you must be careful not to inadvertently impact user access to workloads and other applications. To help with this, Entra ID allows you to enable conditional access policies in report-only mode. When a conditional access policy is enabled in report-only mode, you will be

able to see the expected effect of the policy when you review the Entra sign-in logs. Users will not be affected since the policy is not fully enabled.

One important caveat to this is the device compliance requirement discussed earlier. Even if a policy is enabled in report-only mode, if you require device compliance in that policy, users of iOS, Android, and macOS devices may be prompted to select a certificate if their device is not compliant. You can avoid this behavior by excluding iOS, Android, and macOS devices from your policy while it is in report-only mode.

Whether your CA policy is enforced or in report-only mode, you can troubleshoot CA behavior from the sign-ins log in the Entra admin center. You can access the sign-ins log in the context of the entire tenant, a specific application (e.g., Exchange Online), or a specific user. If you click on a sign-in and then click on a specific CA policy in the Conditional Access tab of the details pane, you can see what policies were applied to the sign-in. The Policies blade supports search, sort, and filtering, which makes it easier to manage many CA policies. You can also use the What if tool to simulate the results of a sign-in and determine which CA policies will apply.

Microsoft-Managed Conditional Access Policies

Microsoft distributes a [small set](#) of CA policies that require MFA in various situations to tenants that have Entra ID P1 or P2 licenses. The policies require MFA for administrative access to Azure and Microsoft 365 and risky sign-ins. If you have CA policies that accomplish the same goals, the chances are you will want to disable these policies. If you do not, consider the new policies a wake-up call for strong authentication in your tenant. You can choose to use the managed policies or create new ones that are tailored to your needs. You can identify policies Microsoft has created on your behalf by browsing to **Protection > Conditional Access > Policies** in the Microsoft Entra admin center and looking for the "Microsoft-Managed" tag.

Require MFA for External Connections

To illustrate the capabilities of the platform, consider the following scenario: a company employs sales representatives who travel often as part of their job. Sales representatives are permitted to use personal devices, so there is a mix of iOS, Android, and Windows devices in use. The company's security policy requires that all external connections to Microsoft 365 from sales reps must use an additional authentication factor for access from outside the corporate network.

We can break down the scenario into the following elements to create a new conditional access policy that meets the software company's requirements:

1. The policy should apply to all users who are part of the sales department. Because all sales representatives are part of a group called "Sales", the policy can easily be applied to the latter.
2. Even though a conditional access policy can apply to many cloud applications (including non-Microsoft applications), it must only be applied to Office 365. Be careful applying conditional access policies to only a subset of applications. You can inadvertently forget to require MFA in some scenarios which would present a security risk.
3. Only logon attempts from outside the corporate network should require an additional authentication factor.
4. Given that all sales representatives can choose personal devices, the policy should apply, regardless of the device used to access resources.

To create a conditional access policy that meets these requirements, open the Entra admin center and navigate to **Protection > Conditional Access**.

1. Select **New policy** and name the policy "*Require additional authentication for external sales users*".

Under **Assignments**:

- a. Click **Users**, choose **Select users and groups**, and select the *Sales* group. Do not forget to click **Done** to save your progress before moving onto the **Cloud apps** blade.

- b. Under the **Target resources** blade, select Office 365.
 - c. Under **Network**, click **Yes** to enable this section and then click **Exclude**. There, select **All trusted networks and locations**.
 - d. Under **Access Controls**, click **Grant**, and then select **Require multi-factor authentication** and **Require one of the selected controls**.
2. Under **Enable policy**, click **On**.

Note: Before you can create a new policy, you should configure your known locations. This can be done by going to **Protection > Conditional Access > Named locations** and defining the IPv4 and Ipv6 address ranges that are used for Internet egress in your organization. For most organizations, these ranges will be network address translation (NAT) addresses defined on your firewalls. If your organization uses public IP space on your network, this might also be the IP addresses of client computers and/or member servers. You should not include private IP addresses (e.g., 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16). Entra ID also supports IPv6 ingress. In preparation for this, if your organization has IPv6 Internet egress, you should add your IPv6 address space to your named locations to ensure Entra ID correctly identifies where clients are connecting from.

Without the information on known locations, the conditional access engine cannot determine if an authentication request stems from inside or outside of the corporate network, and the machine-learning systems that help rate sign-in risk miss an important signal. Named locations are also in the sign-in logs, making the logs much easier to interpret with context for an IP address.

When you configure named locations, you can optionally mark those locations as "trusted". If you mark a location as trusted, Entra ID allows you to target a conditional access policy to "all trusted locations" without individually listing them. Trusted location information is also used as a signal to Entra's security reporting functionality.

Now, if someone from the sales department tries to authenticate to Exchange Online, no matter whether they access it through the Outlook mobile app, desktop Outlook, OWA, or an Exchange ActiveSync client using modern authentication, they will be prompted for additional authentication factors if the authentication is attempted from outside the known corporate locations.

The above example illustrates one of many possible scenarios in which conditional access can be very useful. For more information on conditional access, have a look [here](#).

Require MFA for All Privileged Roles

Privileged access to Microsoft 365 and Entra ID should always require MFA, with no exceptions. You might even consider requiring a hybrid Entra joined device or a device that is compliant with Intune as additional protection. Entra ID makes this easy to do by applying your conditional access policy to built-in directory roles. You should exclude "break glass" or "emergency access" accounts from this policy in case there is ever a situation where the MFA service is unavailable, or you do not have access to a device that will pass tests (if you require this)! Ideally, break-glass accounts should have as [few dependencies for authentication](#) as possible.

To achieve this, you will need to create a new conditional access policy. Configure the conditional access policy with the following settings:

- **Assignments > Users** – Include **Directory roles** and select the built-in directory roles you want to include. We recommend that you select all the roles unless you have a valid business or technical reason not to. Exclude **Users and groups** and select your break glass accounts.
- **Target resources** – Include **All cloud apps**.
- **Access Controls > Grant** – Check the **Require multi-factor authentication** checkbox.

If you want to also require hybrid joined or Intune compliance devices, select the corresponding checkboxes on the Access Controls > Grant screen. Once you are ready, configure the **Enable policy** setting to **On**. Your changes will take effect immediately.

In the past, it was accepted wisdom that break glass accounts should use a complicated password and be excluded from conditional access evaluation. With the change to [mandate MFA for access to Azure administrative sites](#) (including Azure PowerShell, Azure CLI, and the Intune admin center) enforced from mid-October 2024, the revised guidance is to use a strong authentication method like FIDO2 keys or certificates with break glass accounts. Whatever method you choose, be sure to test to validate that everything works as expected if an emergency happens.

Control MFA Strength for Certain Applications

You may have sensitive applications where you want to require a stronger form of MFA, or you may be piloting passwordless authentication. In both cases, you can configure conditional access and authentication strengths to require users to authenticate and/or step-up to MFA how you want. In this example, we will require the Authenticator app with a push notification for MFA. You can follow the same steps to require other MFA methods or control the initial sign-in method.

First, create a new authentication strength:

1. Navigate to **Protection > Authentication methods > Authentication strengths** in the Entra admin center.
2. Click New authentication strength on the toolbar and configure the following settings:
 - a. Name – Password and Microsoft Authenticator with Push Notification
 - b. Check **Password + Microsoft Authenticator (Push Notification)** under **Multifactor authentication**.
3. Click **Next** and then **Create**.

Next, create a conditional access policy with the following settings:

- **Assignments > Users** – Select the users or groups you want to apply this policy to. We recommend starting with a set of test users and excluding your break-glass/emergency access accounts.
- **Access Controls > Grant** – Check the **Require authentication strength** checkbox and then select the **Password and Microsoft Authenticator with Push Notification** authentication strength you created in the previous step.

Restricting Legacy Authentication Protocols with Conditional Access

Microsoft recommends the use of conditional access policies to block legacy clients. This seems like a straightforward thing to do, but there are some nuances. For example, it is a bad idea to block these clients without first looking at your sign-in logs to see which applications your users are using with legacy authentication, and how many of them there are. Turning off every scan-to-email device in a large organization at once, for example, would not be good.

To block legacy clients, you will need to create a new conditional access policy. Configure the conditional access policy with the following settings:

- **Assignments > Users** – Include **All users**.
- **Target resources** – Select **All cloud apps**.
- **Conditions > Client apps** – Check the **Exchange ActiveSync clients** and **Other clients** checkboxes.
- **Access Controls** – Select **Grant** and then **Block access**.

Unlike other conditional access policies, this change may take up to 24 hours to become fully effective. You should test with a small set of pilot users before you target the policy to all the users in your tenant. Except for

SMTP, legacy authentication is blocked in Exchange Online for all users. You cannot unblock it with a conditional access policy.

Restricting Access to the Outlook Mobile Application

While blocking access from legacy clients that do not support MFA is an important first step to securing email access, you may want to go a step further and require the use of Outlook Mobile to access Exchange Online.

To do this, you will need to configure a new conditional access policy with the following settings:

- Cloud apps or actions – Select **Office 365 Exchange Online**.
- Conditions > Client Apps – Select **Mobile apps and desktop clients**.
- Conditions > Device platforms – Select **Android, iOS, and macOS**.
- Grant – Select **Require app protection policy**.

The require app protection policy grant control depends on an app protection policy being assigned to Outlook Mobile in Microsoft Intune. For more information on App Protection policies, refer to the Intune chapter.

We recommend that you start by assigning this policy to a small number of users or groups to test functionality. Once you are satisfied with the results of the CA policy, you can target the CA policy to all users in your tenant.

Note: If you have an on-premises Exchange organization that is configured for Hybrid Modern Authentication (HMA), this CA policy will also affect client access to on-premises mailboxes.

Controlling SharePoint Downloads

A common requirement is to restrict downloading content from SharePoint Online to corporate devices. At the same time, users should be allowed to view content through browsers on unmanaged devices. This can be accomplished with a combination of conditional access policies and configuration in SharePoint.

First, you will need to configure SharePoint Online. To do this, complete the following steps:

1. Access the SharePoint admin center.
2. Browse to **Policies > Access Control**.
3. Select **Unmanaged devices**.
4. Select **Allow limited, web-only access**.

Next, open the Entra admin center and navigate to **Protection > Conditional Access**.

Note: You will find two new policies prefixed with [SharePoint admin center]. **Disable these policies immediately! They are automatically enabled by SharePoint Online and are very restrictive.**
SharePoint will also disable legacy authentication access (e.g., from Office 2010 and outdated Office 2013 clients) to SharePoint Online when you make this change.

Configure a new conditional access policy with the following settings:

- Target resources– Select **Office 365 SharePoint Online**.
- Conditions > Device platforms – Choose **Select device platforms** and then select **Windows**.
- Conditions > Filter for devices – Select **Exclude filtered devices from policy** and then configure a filter rule with the following properties: *'isCompliant' Equals 'True' OR 'trustType' Equals 'Azure AD Joined' OR 'trustType' Equals 'Hybrid Azure AD joined'*.
- Session – Select **Use app enforced restrictions**.

This policy will enforce restrictions on all Windows devices. If the Windows device is hybrid Entra joined or Intune compliant, users will have complete access to SharePoint documents. If the user is not using a hybrid Entra joined (or Microsoft Intune compliant) Windows device, they will only be able to view documents in the

web browser. Downloads and printing will be disabled, and the user will see a notification across the top of the browser.

Mobile devices and Macs are unaffected by the policy. To apply restrictions on mobile devices and Macs, you need to add Microsoft Intune to the solution and adjust your policy to target all device platforms. We discuss Microsoft Intune device compliance and app protection policies in more detail in the Intune chapter.

While the example in this section targets all SharePoint Online sites, you can also enforce policies on a site-by-site basis (see how in [this document](#)). Regardless of the path you choose, your changes might take ten-to-fifteen minutes to become effective. You can also use the SharePoint Online block download policy to block downloads. These features require the [Syntex-SharePoint Advanced Management license](#), which has an added cost. We show you how to use the SharePoint block download policy in the SharePoint Online chapter. If you have Entra ID P1, the chances are you will find the conditional access approach to be more flexible.

Require MFA and a Hybrid Joined Device When Accessing Labeled SharePoint Sites

While the previous example applies to SharePoint as a whole, chances are you have certain SharePoint sites that contain much more sensitive information. To protect this information, you may need to require more assurance that the data is being accessed in a manner that meets your security policies. In this example, we will combine multiple Microsoft 365 features with conditional access. Specifically, we will require users who access data in a Microsoft 365 group labeled with a Microsoft Information Protection (MIP) sensitivity label called *Highly Confidential* to connect with a hybrid Entra joined device and perform MFA every time they access the data. We will accomplish this using a feature of conditional access called authentication context.

With authentication context, applications can request that Entra ID re-evaluate authentication and authorization when a user takes certain actions. You can define up to 25 authentication contexts in your tenant that applications can use in their request. These contexts are simply a name that you can choose from a list in the application and your conditional access policy. For example, you might create a context called *Require MFA*, and another called *Require Trusted Location*. Today, Microsoft lets you use authentication context in SharePoint Online as well as via Microsoft Defender for Cloud Apps (MDCA). The interface is [publicly available](#) and third-party applications and in-house developers are free to use authentication context as well. Applications retrieve the contexts you have configured via the Graph API.

To begin, we first create an authentication context to use. Start by navigating to **Protection > Conditional Access > Authentication context** in the Entra admin center. Click **New authentication context** on the toolbar and create a context with the following values:

- Name – Require MFA and Hybrid Joined Device.
- Description – This authentication context requires the user to complete MFA and have a hybrid Entra joined device.
- Public to apps – Checked.

Next, we will create a conditional access policy to enforce our requirements. Configure a new conditional access policy with the following settings:

- Users – Select **All users**.
- Target resources– Select **Authentication context** and then check the **Require MFA and Hybrid Joined Device** context.
- Grant – Select **Require multi-factor authentication** and **Require Hybrid Azure AD joined device**. Select **Require all the selected controls**.
- Enable Policy – **On**.

We now have an authentication context and a conditional access policy that will enforce it, but, we have not yet created a trigger for the authentication context to be requested. To do this, we will configure our MIP

label. For this step, we assume that a sensitivity label called *Highly Confidential* already exists in the tenant. If you have not worked with MIP labels before, refer to the Information protection chapter for more information.

Browse to the [Microsoft Purview Compliance portal](#) and go to **Information protection > Labels**. Select the Highly Confidential label and click **Edit label** to begin editing it. Configure the following settings:

- Scope – Check **Groups & sites**.
- Groups & sites – Check **External sharing and Conditional Access settings**.
- External sharing & device access
 - Check **Use Microsoft Entra Conditional Access to protect labeled SharePoint sites**.
 - Select **Choose an existing authentication context**.
 - Select **Require MFA and Hybrid Joined Device** from the dropdown list.

Configuring the sign-in frequency session control to one hour requires users to complete MFA again if their session is longer than one hour. This achieves a variation of the requirement to ensure that users re-complete MFA any time they access content labeled *Highly Confidential*.

Once you save your changes, SharePoint sites labeled *Highly Confidential* will begin triggering the conditional access policy we created earlier. There are many ways to label a site. One method is to assign the label to the group in Teams. To do this, find the Team, right-click, and click **Edit Team**. Set the **Sensitivity** to **Highly Confidential**.

Several limitations exist about the extent of client and application support for authentication context that are documented [here](#). We recommend that you review this list before deploying authentication contexts.

Policy Templates

The conditional access policy examples we have illustrated so far are very commonly deployed. While creating policies by hand provides the most flexibility for customization, and enables you to learn the platform, it also introduces opportunities for inadvertent errors and gaps in coverage. To help mitigate this possibility, Microsoft also provides a set of templates for commonly used policies that you can start with. To access the templates, go to **Protection > Conditional Access** in the Entra admin center and select **New policy > Create new policy from templates** on the toolbar. Microsoft documents the set of approximately sixteen templates [here](#).

Reporting Conditional Access Policy Settings

As the number of conditional access policies in a tenant grows, the need to have some method of reporting policy settings becomes more apparent. There are a variety of third-party tools available on GitHub that can help you create a report or store your conditional access policies in a source control system like Git. Two examples of reporting tools that might be helpful are available at the [idPowerToys](#) project and the [DCToolbox project](#).

Security Defaults

While we recommend licensing Entra ID P1 (at a minimum) for all the users in your tenant, this may not be possible. You can achieve some of the most critical conditional access controls discussed earlier by enabling security defaults in your tenant. When you enable security defaults, you will get the following protections for your entire tenant, free of charge:

- Mandatory MFA for every privileged sign-in. This applies to members of [various privileged](#) Entra ID roles as well as access to Azure management APIs including the Azure portal, CLI, and PowerShell modules.
- Mandatory MFA registration for all users using the Microsoft Authenticator app.

- MFA on an as-necessary basis for regular users once they're registered for MFA.
- Block legacy authentication protocols for all users, except for Exchange ActiveSync.

To enable security defaults, access the **Overview > Properties** blade in the Entra admin center and then click **Manage security defaults**. Once you enable security defaults, the protections listed above will take effect immediately for your entire tenant. If you have Entra ID P1, you can only enable security defaults if there are no conditional access policies enabled in your tenant. Since security defaults cannot be scoped to specific users for testing, we recommend using conditional access policies instead if you have Entra ID P1.

Cross-Tenant Trust

When guest users from another organization access resources in your tenant via Entra External Identities, conditional access policies also apply to the guest users. This can create end-user experience issues because the user may be required to enroll for MFA in both their home tenant and your tenant. You can configure Entra ID to trust the MFA that was performed in a user's home tenant to satisfy MFA requirements in conditional access policies. You can also require a user's device to be trusted by their home tenant to satisfy device compliance and/or hybrid Entra join requirements in your conditional access policies. These capabilities are part of cross-tenant access settings.

To configure cross-tenant access settings, navigate to **External Identities > Cross-tenant access settings** in the Entra admin center. You can configure your tenant to trust MFA and device identity from a guest's tenant globally by selecting **Default settings** and clicking **Edit inbound defaults**. On the **Trust settings** tab, you can check the following boxes:

- **Trust multi-factor authentication from Microsoft Entra tenants** – if the user completes MFA in their home tenant, that MFA will also satisfy the require multi-factor authentication grant control in your conditional access policies.
- **Trust compliant devices** – if the user's device is marked as compliant by Intune or a partner solution in their home tenant, the device will also satisfy the device state filters in your conditional access policies.
- **Trust Microsoft Entra hybrid joined devices** – if the user's device is hybrid Entra joined to their home tenant, the device will also satisfy the device state filters in your conditional access policies.

You may find that globally trusting these factors from any guest's tenant does not meet your security and risk management requirements. Instead, you can trust individual tenants. Note that while you only need to specify one domain name in the guest's tenant when you configure the trust settings, the trust settings will apply to the entire tenant, even if multiple domains are verified.

The Maester Tool: Understanding the configuration of the many security settings for a Microsoft 365 tenant can be challenging. The community "Maester" project aims to help tenant administrators by testing configurations against best practice. For example, one of the Maester tests validates if all conditional access policies have exceptions for break-glass accounts. See the [Maester website](#) for more information.

Guests Blocked by Risky Sign-in Policy

Tenants can control the type of sign-ins accepted by Entra ID by configuring an [sign-in risk policy](#) that blocks suspicious sign-ins once the circumstances for a sign-in reaches a set threshold. If Entra ID considers that their account sign-in is risky, a guest user attempting to sign-into the tenant can be blocked by policy. When Entra ID blocks a guest account, administrators in the host tenant cannot unblock the user's account. Instead, an administrator in their home tenant must [unblock the account](#) by taking an action such as resetting the account password or dismissing the risk detections.

Restricting Access to a Single Tenant

Throughout this chapter, we discuss several ways you can restrict user access using a wide variety of built-in features like cross-tenant access settings and conditional access. However, none of these options addresses the problem of a user authenticating to another tenant. You might wonder why this is important or how this is different from disallowing someone to authenticate by disabling their account. In the latter scenario, the user is not able to log in to the corporate tenant, but that does not prevent them from accessing other tenants, using another identity. From a data leakage standpoint, this is a potentially dangerous situation as the user can log on to another tenant and copy corporate data to a repository on that tenant. The reason why a user can log in to various tenants is that most of the endpoints are the same for all tenants, worldwide. Blocking the endpoint would not be a smart move unless you want to block access to Microsoft 365 entirely. Here is an example to further illustrate the problem.

A user, Erica, works for a company that uses Exchange Online for corporate email, and she also has a personal tenant for her personal email. When no tenant restrictions exist, Erica can log in to either or both tenants from her work computer, but there is nothing to prevent her from signing into her personal tenant while at work. To lower the risk of intentional or accidental data leakage, the security team at Erica's employer wants to prevent Erica and her co-workers from signing into tenants other than the corporate tenant while at work. As mentioned earlier, blocking the sign-in endpoint (for example, through a proxy server) would also prevent Erica from signing into her company's tenant, and thus prevent her from doing her job.

Of course, other ways exist to restrict access. For instance, an administrator can define a set of internal IP addresses from which a user can authenticate into the corporate tenant. Although this effectively prevents someone from accessing the tenant outside the corporate network, it does not solve the problem described above.

To help organizations control access, Microsoft supports a feature known as "[tenant restriction](#)." The way this feature works is quite simple. When a user authenticates with Entra ID, the authentication platform also checks for an (HTTP) header called *Restrict-Access-To-Tenants*. The value of this header holds the names of all the tenants the user can access. You also need to add the *Restrict-Access-Context* header, which specifies the GUID of your tenant, so the service knows which tenant to apply the restrictions to. If these headers hold the name of the tenant the user is trying to access, the sign-in proceeds. If not, they receive an error message and are blocked from signing in. The message informs the user that *Your network administrator has restricted what organizations can be accessed. Contact your IT department to unblock access*.

For this feature to work, there must be a proxy server between the user and the internet that performs SSL inspection. Anything that can add an HTTP header will suffice. If you want to make sure that control is always exerted over user sign-ins, including outside the corporate network, users must always access the internet through a proxy server that can inject the header. To ensure this happens, other countermeasures (such as ensuring the user cannot modify proxy settings, etc.) must be present. Otherwise, users can bypass the restriction themselves. In addition, the proxy server should be accessible from outside the corporate network if you want to restrict access to a single tenant, regardless of the user's location. One way to achieve this is to use a "proxy-as-a-service" such as ZScaler.

The necessity for a proxy server to make tenant restrictions function is a significant limitation, especially with a remote workforce. To address this challenge, Microsoft created tenant restrictions version 2. Version 2 of tenant restrictions relies on functionality that was added to Windows 10 and Windows 11 and cross-tenant access settings. Enabling the new version of tenant restrictions requires a significant number of steps, which Microsoft has [documented in detail](#). In summary, you must take the following steps:

- Configure Group Policy settings to enable tenant restrictions

- Enable Windows Firewall and Windows Defender Application Control (WDAC) functionality to block unsupported browsers and applications from accessing Entra ID
- Configure cross-tenant access settings to allow access to specific tenants or Microsoft accounts

Both versions of the feature are only useful to control the potential for data loss if you fully control the endpoint. Ultimately, Microsoft plans to replace both versions of tenant restrictions with a new “universal” version of the feature. With that said, it is a clunky way to prevent data loss; it is much less flexible or capable than Microsoft Information Protection (MIP), although (unlike MIP) it requires minimal client-side configuration.

Restricting access to a single tenant might or might not be useful. If preventing data leakage is a priority, anything you can do to make it harder for people to share information in an unauthorized manner can be helpful. Although the feature will most likely not prevent malicious users from leaking data, it can stop most regular users from (accidentally) leaking sensitive data to another tenant. Of course, it is only a small cog in a much bigger picture as many other features like DLP policies and Microsoft Information Protection help to safeguard your data.

User Settings

The User settings section of the Entra admin center includes some default settings that deserve attention. These settings are:

- **Users can register applications.** The default setting is On. You should turn this to Off to restrict the ability to create new registered apps to administrators. No good reason exists to allow users to create new apps. Leaving this setting enabled makes it easier for attackers who penetrate a tenant to plant malicious apps.
- **Restrict non-admin users from creating tenants.** By default, users can create new Entra tenants. Again, there is no reason to allow users to do this. If developers want to create a new tenant for test purposes, they can do so through the [Microsoft 365 test tenant program](#).
- **Users can create security groups.** Security groups control access to resources. User accounts should not determine access to tenant resources. Therefore, no need exists for users to create security groups, so disable this capability.

Microsoft defined the default user settings some years ago when the threat situation was not as pronounced as it now is. The user settings are a great example of why it is important to understand and challenge default settings in the full knowledge of how a tenant operates and how it is secured.

App Registrations and Permissions

Thus far we have focused on how users and their devices work with Entra ID. Entra ID also plays a very important role in supporting the integration of different Microsoft 365 workloads (for example, how Microsoft Teams gains access to SharePoint and Exchange Online), as well as third-party and in-house developed applications. Microsoft controls the permissions held by first-party applications like Teams, but the permissions that you grant third-party and custom-developed applications are controlled by tenant administrators.

Two types of permissions can be granted: delegated and application. Delegated permissions are used when an application (such as a website) signs the user in and then calls an API on behalf of the user. Application permissions are used when there is no user sign-in, such as in a background process or service. Permissions are held by the service principals of the applications. This arrangement is used because enterprise applications are managed by the developer who creates the applications. The service principal object then represents the

instantiation of the application within a tenant. An app created by a tenant is under the control of the tenant. It also has a service principal that's used to hold permissions.

Permissions are granted by consenting to different API permission scopes that are defined on various applications and resources. In Figure 2-8, a user is authorizing an application to take various actions in Entra ID, Exchange Online, and SharePoint through a process known as consent. Entra ID manages and tracks consent and brokers the issuance of tokens that enable applications to communicate and use their permissions.

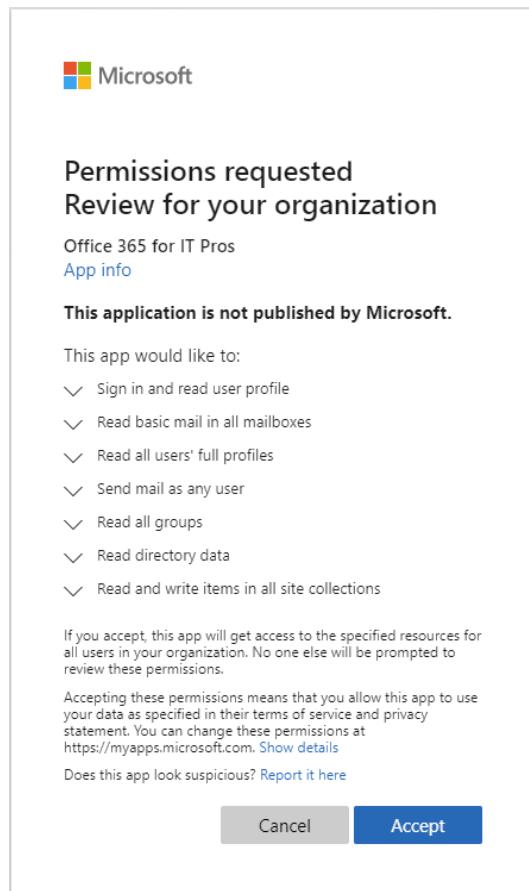


Figure 2-8: Granting Graph API permission consent to an app

Some of the permissions granted in Figure 2-8 are extremely broad and in the hands of an attacker or a poorly written application could present a significant security risk. For example, this application can read information about every user and group in the tenant, read email messages, send email as a user, and read and write any file in SharePoint. Historically, many organizations did not pay much attention to these consent requests, and they even allowed users to independently consent to certain application permissions.

Attackers attempt to use this vulnerability through avenues such as phishing attacks that induce users to grant [illicit consent](#). An [example analyzed by Microsoft in September 2022](#) explained how attackers exploited a compromised administrator account to create a registered Entra ID app in tenants and assign the app the permission to make changes to Exchange Online.

More details about how applications use permissions can be found in the PowerShell book.

Controlling Consent

To combat the risks of granting illicit consent and over-privileged applications, Entra ID lets you control what types of permissions end users can consent to and provides an approval process for users to request consent for higher levels of permission. To configure this, navigate to **Applications > Enterprise applications >**

Consent and permissions in the Entra admin center. Under **User consent settings**, you can configure what types of permission users can independently consent to.

For user consent for applications, we recommend that you choose the Microsoft recommended setting, **Allow user consent for apps from verified publishers, for selected permissions** (the default for new tenants beginning in September 2022), or the more conservative choice of **Do not allow user consent**. In a small organization, the conservative approach is likely practical, but, in a larger organization, the number of requests you will receive for relatively low-risk permissions is probably not manageable. The middle ground attempts to address this. Applications that are from verified publishers have completed an identity verification process with Microsoft and the publisher has agreed to certain terms and conditions. You can choose which permissions you consider low risk, including a curated list that Microsoft recommends. The publisher verification process helps to prevent malicious actors from registering multi-tenant applications that can request high risk permissions from end users.

If you choose a restrictive setting for either user consent or group data consent, which we recommend you do, you will need a process to manage requests. Entra ID offers a solution to this with an approval process governed through a feature called admin consent workflow. To enable the approval process, navigate to **Identity > Applications > Enterprise Applications > Consent and permissions** in the Entra admin center and configure the following settings:

- Users can request admin consent to apps they are unable to consent to – Yes.
- Who can review admin consent requests – Specify a list of users, one or more groups of users, or a built-in directory role.
- Selected users will receive email notifications for requests – Yes.
- Selected users will receive request expiration reminders – Yes.
- Consent request expires after (days) – 14.

Once you have enabled the admin consent workflow and configured the user consent settings discussed earlier, end-users will receive a modified version of the prompt in Figure 2-8 when they try to access an application requiring some permissions that they cannot grant consent for. Instead, the user will be prompted to provide a business justification and submit a request for approval. The reviewers specified earlier will receive an email notifying them of the request that they can approve or deny under **Applications > Enterprise Applications > Admin consent requests** in the Entra admin center.

Reviewing Existing Permissions

The admin approval workflow and restrictions on user consent add significant security for new requests, but they do not do anything for existing permission consents. In some organizations, the number of applications granted access to various permissions may be substantial. Some of these permissions may also be risky or even granted to an illicit application. You will need to create a process to evaluate permissions granted previously and determine if they should remain.

This [blog post](#) explains how to inventory permissions granted to Entra ID apps. The script focuses on high-priority permissions that attackers often attempt to exploit and posts the report of what it finds as a message in a Teams channel. If you have the necessary licenses, App Governance in Microsoft Defender for Cloud Apps (MDCA) aims to simplify the evaluation of permissions and provide continuous insight on the potential risks that your organization is exposed to through overly-permissioned apps.

Restrict Workload Access to Approved IP Addresses

When a tenant has app registrations that must hold sensitive or privileged access to support the functionality of a business process, you should take steps to control that access. Entra Workload Identities ([a paid feature](#))

can handle the requirement through conditional access. With this feature, you can create a conditional access policy, like the examples we discussed earlier, which applies to registered apps.

In this example, we restrict an app registration called *Office 365 for IT Pros* from being used except when run from approved IP addresses. You can use the egress IP address ranges of the data center(s) that host the application using this app registration. To configure the approved IP address ranges, go to the Entra admin center and navigate to **Protection > Conditional Access > Named locations**. If you have not configured a named location before, we discuss this in detail earlier in the Conditional Access section of this chapter.

Next, select **Security** and then **Conditional Access**.

1. Click **New policy** and name the policy "*Restrict Workload Access to Approved IP Addresses*". Under **Assignments**:
 - a. Click **Users or workload identities** and select **Workload identities** under **What does this policy apply to?**. Next, click **Select service principals** and select the Office 365 for IT Pros app registration from your tenant. Do not forget to click **Select** to save your progress.
 - b. Under **Conditions**, click **Locations** followed by **Exclude**. Select **All trusted locations**.
 - c. Under **Access Controls**, click **Grant**, and then select **Block access**.
2. Under **Enable policy**, click **On**.

Once this policy is enabled, the selected service principal can authenticate only from a trusted location that you configure. Note that the feature does not currently support service principals configured for multi-tenant use.

Connecting to LinkedIn

According to [LinkedIn](#), more than a billion people are members of their professional network. Ever since Microsoft bought LinkedIn in June 2016, the two companies have looked for ways to co-operate, including the ability to connect LinkedIn to Entra ID. By default, all tenants except those in France and Germany have a LinkedIn connection enabled. Tenants of the sovereign clouds do not support the LinkedIn connection, so you cannot use the feature if your tenant is in the China or U.S. Government clouds. Enabling the connection only allows users to decide if they want to connect their Entra ID account to their LinkedIn account. No data is ever exchanged unless authorized by the user to whom the data belongs.

To control the connection, go to the **Users > User Settings** section of the Entra admin center. You can then set the connection to allow all users to connect, some users to connect, or no users to connect. If you decide to restrict the connection, you select a security group containing the set of users allowed to connect their accounts to LinkedIn.

If the tenant allows users to access LinkedIn, a LinkedIn logo appears in the people cards displayed by applications such as OWA, Teams, and SharePoint Online. Apps can display publicly available information from matching profiles. Before LinkedIn reveals more detailed information such as job history or details about the user's connections, the user must connect to their LinkedIn account. The search can happen for both internal and external recipients and result in three outcomes:

- The person is a LinkedIn contact: You see the private profile for the person as shared with their LinkedIn contacts.
- The person has a LinkedIn account but is not a contact: You see the public profile of the person and can send them a LinkedIn invitation to connect.
- LinkedIn cannot find a match: Either the person doesn't have a LinkedIn account or several matching LinkedIn accounts are found. In this case, you can choose the best match.

The important thing to remember about the LinkedIn connection is that users control it. Although the tenant decides if the connection can be used, users decide if they want to connect their Entra ID account with their

LinkedIn account. LinkedIn users located in the European Economic Area (EEA) and Switzerland also have a setting to restrict the visibility of their profile in Microsoft 365 available in their LinkedIn [profile settings](#).

Fetching Email Addresses from LinkedIn

Another feature gained when someone connects their LinkedIn account to their account is that email addresses for first-degree LinkedIn contacts are included in the people suggestion list used by Microsoft 365 browser applications when the user addresses an email or shares documents. In addition to LinkedIn contacts, the suggested people list includes tenant and guest users and Outlook's auto-complete list. As an example of use, when you create a message with OWA and begin typing an address into the TO: or CC: field, OWA checks what you type against the suggested people list and shows any matches that it finds.

PowerShell and Entra ID

Microsoft is [transitioning away](#) from the AzureAD PowerShell module. The AzureAD module uses the Azure Graph API, which Microsoft [deprecated in March 2024](#). As a replacement, Microsoft recommends that you update scripts to use cmdlets from the [Microsoft Graph PowerShell SDK](#) module. If you are familiar with the AzureAD module, you will find the same tasks are possible with the new module, albeit with different syntax. As the name implies, the foundation for the Microsoft Graph PowerShell SDK is the set of Graph APIs, which cover much more than user accounts and groups and is constantly evolving. New features first come to the "beta" endpoint before transitioning to the stable "v1.0" endpoint. All the tasks you can accomplish in the Entra admin center are not yet available in the Graph API.

More information about the Microsoft Graph PowerShell SDK is in the PowerShell book.

Chapter 3: Tenant Management

Paul Robichaux

As the Microsoft 365 ecosystem evolved to add new features, capabilities, and apps, products adopted different administrative workflows. Depending on the task you're trying to perform, the functionality of the tools Microsoft provides may lead you towards one approach or another. Sometimes there's more than one way to perform the same task; in those cases, each approach will have its pros and cons. For example, the web-based admin interfaces described here are simple to use and make it easy to perform one-time tasks such as adding a domain name to the tenant. However, for bulk administrative tasks such as changing the department attribute for multiple users, PowerShell is more efficient, which is why we devote a complete book to this topic.

It's important to remember that in a hybrid environment where you're using directory synchronization, changes to users, groups, and other objects stored in on-premises Active Directory must occur in the on-premises Active Directory because it's the source of authority. As you learned in the Identities chapter, changes you make to cloud copies of on-premises objects won't necessarily replicate back. For example, to change a user's surname you must make the change using the on-premises Active Directory management tools and then allow directory synchronization to synchronize the change into Entra ID. The Microsoft 365 admin center and PowerShell will warn you when you try to change an attribute in the cloud synchronized from on-premises AD.

Because there are so many individual services in the Microsoft 365 portfolio, Microsoft hasn't unified administration into a single portal or a single PowerShell module, although they are making some moves to do so across Microsoft 365 and by using the Microsoft Graph as a single point of data access. It wouldn't make sense to do so because the workloads are so different; a single unified toolset would be complex, slow, and confusing to use and would limit the ability of individual product groups to optimize and improve their admin experiences. However, the inevitable process of product updates means that sometimes things change, either slowly or abruptly. For example, after Microsoft introduced the Entra brand, they have rolled the Entra ID management functionality that used to be in the Azure portal into the [Entra admin center](#). You can still reach the Entra ID management tools from the [Azure portal](#), but the "new and improved" way to do so is from <https://entra.microsoft.com>.

Part of learning to manage the service is becoming comfortable with a sometimes-confusing variety of web-based admin portals, PowerShell modules, and endpoints that we can use. In the next section, we'll start exploring some of this variety to help you understand what tools to use and when.

Cloud versus On-Premises Management

Moving to the cloud involves losing a degree of control and visibility. Microsoft's platform is sold as "Software as a Service" (SaaS), which transfers the responsibility for running the service to Microsoft. You give up access to anything relating to the underlying hardware, networking, and software. You don't get to

select the make and model of servers used to run the service, nor do you get to choose the specifications and sizing of those servers.

Storage management was always a challenge in on-premises environments. Microsoft manages the storage for Microsoft 365 applications and services, both in terms of quotas assigned to individual applications and users and overall storage performance. At most you may need to help your end-users with managing their mailboxes and sites within the quota limits that the service imposes, through a combination of user education and policy controls (e.g., retention policies). Microsoft also manages the network and Internet connectivity for the service. You only need to ensure that adequate bandwidth is available to reliably connect to Microsoft 365 across the internet. Similarly, you must manage any firewalls or other network devices such as web proxies that affect the connectivity of your users to the service.

The underlying operating system and all the software running on Microsoft's servers are also out of your hands. Microsoft surfaces a lot of service-level configuration options for you that apply to the users in your tenant, as well as some reporting tools such as message tracing. However, you simply do not get access to Windows event logs, Performance Monitor data, or any of the other system data that Windows and the applications generate. Similarly, you do not get access to stop or restart services on the servers or perform server reboots. On the positive side, you also don't need to perform any Windows patching or application upgrades.

Because tenant administrators no longer perform many common administrative operations required by on-premises servers, some IT professionals view movement to cloud and the associated loss of control as a negative. They fear the impact that the cloud will have on their careers. A more positive way to look at it is that you are allowing the same people who develop the product to run it for you within a defined set of parameters. All the time that you previously spent doing the tedious work of monitoring, managing, and fixing server hardware, operating systems, and application installations is now available for you to spend on helping to deploy features to your end-users, align the configuration of different workloads with your organization's policies, and act as a broker between your company and Microsoft as a service provider. Now when something goes wrong, a Microsoft engineer wakes at 3 am to answer a pager instead of you.

Break-Glass Administration

An obvious difference between cloud and on-premises management is that Microsoft 365 won't allow you to sign into the console of a physical computer when all else fails and you need to access a server. Other factors which can limit the ability to sign into an administrator account include a working internet connection to Entra ID, blocks imposed by conditional access policies, the ability to satisfy multi-factor authentication challenges, and so on. During the setup of a new tenant, you nominate an account to be the global tenant administrator. This account is all-powerful and should be protected with multi-factor authentication and a complex password. In general, you should not use the global administrator account for day-to-day operations. As discussed later, it is better to assign limited administrative roles to accounts to allow them to perform specific tasks.

Because an outage might interfere with the ability of administrators to sign into their regular accounts, you should create one or more "break-glass" accounts. These are highly-privileged accounts (perhaps holding the global administrator role) intended for use in emergencies with the following characteristics:

- Created in the cloud only (to remove any dependency on account synchronization with an on-premises directory). The user principal name for the account should use the tenant service domain (*tenant.onmicrosoft.com*). Consider giving break-glass accounts obscure names to draw attention away from their true purpose.
- Protected by strong authentication, including MFA. You should take care to [minimize the number of dependencies used by authentication](#) to ensure that the account is available when needed. For

- instance, you should exclude break glass accounts from conditional access policies to ensure that a policy doesn't block a sign-in attempt for the account.
- Protected with a complex account password for break-glass accounts should be complex and deliberately obscure. Because these accounts have access to the entire Microsoft 365 tenant, it's important to store the password for break glass accounts securely.
 - Subject to auditing. Of course, the administrative actions taken by the account will be captured in the system audit log, but if you are using a security monitoring tool you should probably configure it to send alerts any time the account is used. You should also ensure that you have a way to tie use of the account to a specific human to prevent misuse.

To make sure that you can access these accounts in an emergency, you'll probably want to store the password somewhere. The details of exactly how you do this will vary from organization to organization. The important thing is that the process to retrieve passwords and use the break glass accounts is proven and effective. After each use of a break-glass account, you should change its password and update the new password in the secure locations.

Tenant and Workload Management

The [Microsoft 365 admin center](#) is used to configure items shared across the applications that make up the platform, such as domain names, billing details, and license assignments. Some frequently used administrative functions are also in the Microsoft 365 admin center. For example, you can create a new cloud-only user account complete with a mailbox without opening the Exchange admin center. Users with Global administrator, Service administrator, Billing administrator, or application-specific administrator rights will have access to the Microsoft 365 admin center.

Two Quick Teleportation Tricks

Before we dive into the details of the portals, I want to share two incredibly useful navigation tools.

First is the "omniportal" developed by Microsoft's Merrill Fernando: the [cmd.ms](#) website. He's put together a list of direct links to many of the most frequently-used portal blades. Each of the blades has its own short abbreviation, coupled with an HTML redirection. For example, to go directly to the Intune portal, point your browser at `in.cmd.ms` and you'll be redirected straight to the Intune blade. Since every modern browser supports autocompletion of previously visited sites from the history, this mechanism gives you an effective and simple way to use your keyboard to get quickly to the portal of your choice.

Second is the very useful [msportals.io](#) site maintained by MVP Adam Landry. It's a comprehensive list of admin and management portals for Microsoft 365, Azure, various applications, developer tools, different parts of Defender, and support functions such as licensing. If you haven't seen the full list, you may be surprised by the number of portal pages that Microsoft has across its ecosystem.

Basic Tenant Management in the Microsoft 365 Admin Center

Figure 3-1 shows the current version of the Microsoft 365 admin center. Expect to see more changes as Microsoft continues to evolve its functionality and publish a [detailed change log](#) to help you keep track. The organization name shown in the top right-hand corner of the *Home* page of the Microsoft 365 admin center is a link. Clicking it takes you to the organizational settings page. More interestingly, if there are multiple tenants associated with a single organization, as determined by the existence of a partner-of-record relationship, there will be a small icon next to the organization name to indicate that you can switch between organizations by clicking the name. There are other cross-tenant features, such as the ability to share billing information between tenants, that you'll only see if you have a multi-tenant relationship established.

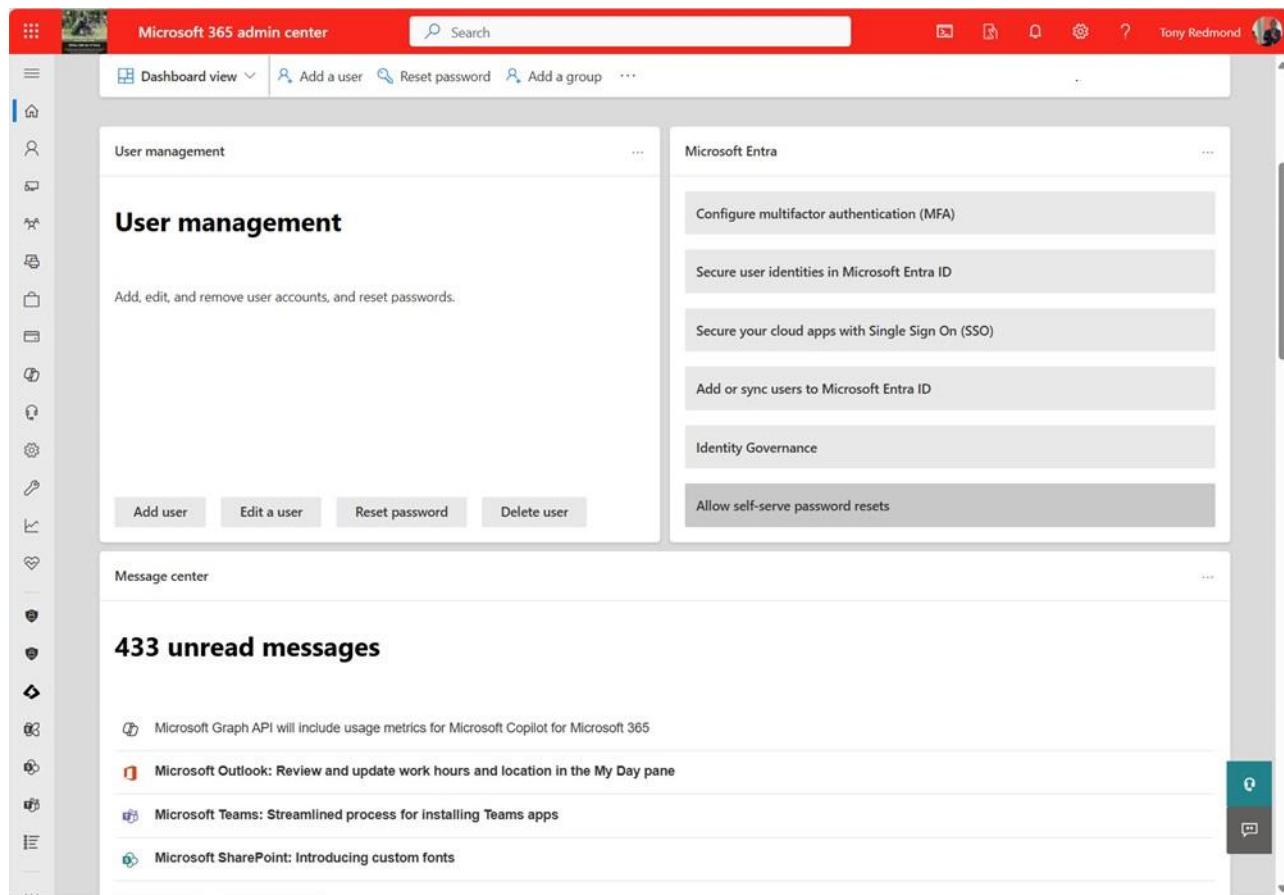


Figure 3-1: The Microsoft 365 admin center

The navigation bar at the top of the window lets you quickly switch between the standard dashboard view and the Health view (described later). You can customize the dashboard view of the admin center to display specific tiles and the order and layout for the tiles (which Microsoft calls “cards”). The default set of cards you see include cards for message center notifications, reviewing your billing, and working with support incidents. You can customize the set of cards shown in the portal by reordering them, removing them, or adding new ones with the **Add cards** link. As a customization example, tenants that synchronize Entra ID with an on-premises Active Directory can add a card showing the directory sync status to your home page. Clicking the card reveals other information about your directory sync status, including the version of the directory synchronization client (Entra ID Connect) installed in the on-premises environment.

The navigation pane on the left side of the admin center has expandable menus for different categories of tasks. The tasks that are available throughout the menu are those that Microsoft thinks are commonly performed by administrators. In some cases, a complex administrative task is provided with a user-friendly wizard in the admin center, while the workload-specific admin portal for that task will have a more complicated process involved. In other cases, admin tasks initiated from the Microsoft 365 admin center simply launch a wizard from one of the workload-specific admin portals. To manage the service, you'll have to use a mix of the native admin center functionality and the workload-specific admin centers. Microsoft frequently adds new functionality in the Microsoft 365 admin center, and otherwise rearranges things, to keep us all on our toes. You may see a small bullet icon next to new or renamed menu items when Microsoft wants to highlight changes.

For smaller tenants, you may notice a slightly different, and less detailed, “simplified view” targeted at tenants with 10 or fewer users. This view provides a stripped-down, card-based interface to a few common tasks that smaller tenants will be most likely to use.

Microsoft 365 Admin Center Functionality

Assuming your account has the necessary permission, and you view the complete Microsoft 365 admin center by clicking **Show all**, here's what you'll see:

- In the **Users** section, you can manage user accounts, contacts, guest users, and deleted users, change user license assignments, and change multi-factor authentication settings.
- The **Devices** section shows you devices that are managed by Intune (either fully or via mobile application management) and gives you access to a few simple device actions, such as removing company data. It also allows you to see and take management actions on devices that are enrolled in Windows Autopilot. (See the Intune chapter for more on device management.)
- The **Teams & groups** section allows you to create and manage Microsoft 365 teams, Groups, Exchange distribution lists, shared mailboxes, Teams policies, and security groups. You can see the properties for security and distribution lists that are homed on-premises and synchronized to the cloud, and you can edit properties for cloud-homed objects. See the Groups chapter for more detail about Microsoft 365 Groups.
- The **Roles** section lets you view and manage administrative role assignments and administrative units. You can see and manage Entra ID, Exchange Online, Intune, and billing-related role assignments, and you can create new role groups for Exchange Online. By selecting a role, you can see which users are assigned to it and what specific permissions it has. You can also create and edit administrative units, covered later in this chapter. See the user management chapter for more on role assignments.
- The **Resources** section is where you can manage room and equipment mailboxes and SharePoint Online sites (although some SharePoint links in this section just take you to the SharePoint Online portal).
- The **Marketplace** section allows you to view a Microsoft-centric catalog of additional licenses and service plans. The catalog includes a comparison tool to help you understand which specific plan or service might best fit your requirements. When you purchase licenses here, they immediately show up in the tenant.
- Tenants which have Copilot licenses will see a **Copilot** section in the left navigation bar to open a page where you can monitor usage, manage licenses, review Message center items related to Copilot, and manage some (but not all) Copilot settings.
- In the **Billing** section, you can manage subscriptions, buy and allocate licenses, and update payment details. Whereas the Marketplace section is more oriented to browsing, the controls in this section are strictly for viewing and buying, with no browsing or comparison tools.
- In the **Support** section, you can submit and monitor the progress of service requests for problems that you have encountered with your tenant. Any open Customer Lockbox requests appear here. If you have Surface devices, you can get support for them from here as well.
- The **Settings** section contains several tools for controlling the configuration of different parts of the service. For example, you use this section to manage the DNS domains associated with your tenant, what third-party applications and add-ins are available, manage Microsoft 365 Backup, how Microsoft Search works in the tenant, what individual services such as Cortana or Teams are enabled in the tenant, and what integrated applications (formerly known as "Office add-ins") are available. You can also apply restrictions to services such as preventing guest user access to Microsoft 365 Groups or Teams. Security and privacy settings for the organization are also in this section, including the password policy for cloud identities, Customer Lockbox configuration, and sharing controls. The organization profile is also configured in this section, which includes company and contact details, and the options for configuring Targeted Release (previously known as First Release) for the advanced deployment of new features. This section also contains a link that allows you to see and manage any digital partner of record (DPoR) assignments in your tenant.

- In the **Setup** section, Microsoft presents a list of specific actions you can take to set up your tenant. For example, there are quick-access buttons for configuring self-service user password reset, applying a basic set of data loss prevention rules, and starting the process of migrating user data from other services, and there are setup actions for the various Viva services included now as well.
- The **Reports** section presents a dashboard view of the usage of individual services such as Copilot, Exchange Online, OneDrive, and Teams. You'll also find detailed activity reports, plus the Adoption Score reports, as well as tools for managing organizational messages. More information about reporting is in the reporting and auditing chapter.
- The **Health** section is where you can access the Service Health Dashboard (SHD) to see the current health status of workloads in addition to details of outages, service history for the previous 30 days, and planned maintenance. The Health section also includes access to Message Center, where notifications for new and changed features in your tenant are published by Microsoft, a summary of your directory synchronization status identical to the one available in the dirsync status card, the network connectivity toolset, tools for checking on Windows update status, and controls for gathering product feedback from your users and sending it to Microsoft. These tools are discussed later in this chapter.
- The **Admin centers** section has shortcuts to other administration consoles for services that you are licensed to use, such as Entra ID, Exchange Online, the Compliance portal, Teams, and Endpoint Manager.

By default, the Microsoft admin center collapses some of these items, meaning that they don't appear at first sight; you can use the **Show all** link at the bottom of the left navbar to reveal all available options. By hovering over any top-level item, you'll see a pin icon appear; clicking it will pin that item to the left navbar so that it's visible in the condensed view.

Let's take a quick look at the other workload-specific admin portals. As a convenience, Microsoft includes links to the Intune portal (shown as **Endpoint Manager**) and the Entra admin center (shown as **Identity**) in the admin center list in the left navigation rail. These portals are covered elsewhere, so we won't cover them here.

Managing Exchange

The Exchange admin center (EAC) is a web-based console used to manage elements of Exchange Online including mail contacts, mail users, role assignment policies, OWA mailbox policies, public folders, and hybrid connectivity. Some elements, such as distribution lists and mail flow rules, are also available through other consoles. Two versions of EAC are available:

- Microsoft built the [modern EAC](#) from scratch for Exchange Online. The functionality available in the modern EAC reflects that Microsoft 365 replaces many workload-specific features (like compliance and auditing) with service-wide equivalents managed through other consoles like the Microsoft Purview Compliance portal. However, Microsoft has also deployed some features into the modern EAC that are unique to Exchange Online, such as the **Troubleshoot** section in the left navigation rail, which contains several diagnostic tools and features. The modern EAC is completely deployed in the Office 365 Commercial instance.
- The "classic" older form of the EAC was like the Exchange on-premises version. Microsoft [formally deprecated it in the commercial cloud on June 20, 2023](#), although you may still see references or screenshots of it in Microsoft's documentation.

You may not use the EAC all that much. The EAC includes a few actions that can't be done elsewhere; for example, the new EAC is the only GUI for an administrator to recover mailbox items for a user, and you can only see usage reports for dynamic distribution groups in the new EAC. There are a few features present in the classic EAC that aren't available in the modern EAC, too.

Managing SharePoint Online and OneDrive for Business

SharePoint Online has its own management portal with a URL formed from the tenant's name with an “-admin” suffix plus “sharepoint.com.” For example, a tenant named Contoso will have a SharePoint admin center URL of <https://contoso-admin.sharepoint.com>. The SharePoint admin center looks a great deal like the Microsoft 365 admin center, with a similar card-based display mechanic and left-hand navigation bar. OneDrive for Business administrative settings are now integrated into the SharePoint Online admin center. For more information on using the SharePoint admin center, see the SharePoint Online chapter.

Managing Microsoft Teams

All management of Teams is performed in the [Teams admin center portal](#). You can navigate there by going to the **Admin centers** section and then clicking **Teams**. More information about using the Teams admin center is in the Teams management chapter.

Managing Viva

Microsoft is investing heavily into the Viva employee-experience toolset. It seems like every month there's some new Viva workload or other, although in truth some of these are rebranded versions of existing services. The Viva service names and SKUs are becoming more common in Microsoft 365 admin center. For example, you may have seen “Viva Engage Core” show up as a new service plan in your existing E3 or E5 SKUs since the formal deprecation of the Yammer brand and its replacement with Viva Engage.

Microsoft doesn't yet have a single point of management for all the disparate Viva services. However, a [Viva page](#) is available in the Microsoft 365 admin center in the left navigation rail under **Settings**. This page collects many of the admin- and tenant-oriented Viva settings into a single place. In many cases, the admin center is mostly used for you to assign an application admin to part of Viva, with further configuration performed in the app itself. For example, if you navigate to the Viva Engage section of the setup page, you'll see that your actions are limited to a set of 3: assign an Engage admin, pin the Engage app in Teams, and jump to the Engage app itself to manage other settings. Microsoft is rolling out the ability for administrators to manage Viva services without requiring that the administrators themselves have licenses for the services. This work is ongoing.

As the Viva suite continues to grow, you should expect to see more integration of its admin features into the Microsoft 365 admin center. For example, there are usage reports for Viva Learning available under the **Reports** section in the admin center. However, most of the administrative controls you'll use, including those for managing licenses or roles for Viva users and administrators and configuring the settings for individual members of the Viva suite, will live within the Viva applications themselves.

As Microsoft adds features to the Viva applications, you may need to take management actions. For example, you can now [create multiple Viva Connections “experiences”](#) for different audiences. You can turn off private messaging in Viva Engage and administrators who have the Global Admin or Knowledge Admin roles for Viva Learning can delegate access to specific learning management features to unprivileged users. You'll need to keep on top of feature changes in the Viva application on your own so that you know when Microsoft introduces new features, and which ones are on by default.

In addition to the admin center, for now, you can also manage some parts of these applications directly from the applications themselves. For one example, Microsoft announced (in MC495323) that they would be adding Viva Engage admin features to the Viva Engage Teams app, so you can use the app to designate “official leaders” and to create and manage Viva Engage campaigns. Another example: to manage settings for Viva Goals, you [log into Viva Goals itself](#) with a suitably privileged account.

Managing Microsoft 365 Copilot

One area where Microsoft has tried to leverage their access to customers' Microsoft 365 data is in search. Bing for Enterprise, when enabled, can perform queries against users' data to produce search results, in much the same way Office Delve originally did. (Delve itself was finally deprecated in December 2023.) Back in 2020, Microsoft started releasing what they originally called the "Bing Enterprise homepage" experience. The experience has evolved over time, and currently features a "Work feed" tab that shows you recent documents and emails, both your own and those shared with you, as well as offering you various Viva-powered insights. Along with this homepage experience, you can search for items using Bing for Enterprise. Search results are tabbed so that you can choose between seeing work-related results or results from the general Internet.

Managing Access to Microsoft 365 Copilot

Microsoft 365 Copilot requires a separate license spanning a set of service plans, each of which can be individually enabled or disabled (as described later in this chapter). Table 3-1 lists the current service plans.

Service Plan	Service Plan SKU	Service Plan Part Number
Microsoft Copilot with Graph-grounded chat (Biz Chat)	3f30311c-6b1e-48a4-ab79-725b469da960	M365_COPILOT_BUSINESS_CHAT
Microsoft 365 Copilot in Productivity App	a62f8878-de10-42f3-b68f-6149a25ceb97	M365_COPILOT_APPS
Microsoft 365 Copilot in Microsoft Teams	b95945de-b3bd-46db-8437-f2beb6ea2347	M365_COPILOT_TEAMS
Power Platform Connectors in Microsoft 365 Copilot	89f1c4c8-0878-40f7-804d-869c9128ab5d	M365_COPILOT_CONNECTORS
Graph Connectors in Microsoft 365 Copilot	82d30987-df9b-4486-b146-198b21d164c7	GRAPH_CONNECTORS_COPILOT
Copilot Studio in Copilot for Microsoft 365	fe6c28b3-d468-44ea-bbd0-a10a5167435c	COPILOT_STUDIO_IN_COPILOT_FOR_M365
Intelligent Search (Semantic search)	931e4a88-a67f-48b5-814f-16a5f1e6028d)	M365_COPILOT_INTELLIGENT_SEARCH
Microsoft 365 Copilot for SharePoint	0aedf20c-091d-420b-aadf-30c042609612	M365_COPILOT_SHAREPOINT

Table 3-1: Copilot service plans

You can selectively disable these service plans to turn off Copilot features that you don't want individual users accessing, although (for now) you cannot enable or disable specific Copilot features (such as "Draft with Copilot" in Outlook).

Managing Copilot Settings

After purchasing at least one Microsoft 365 Copilot license, a new **Copilot** item appears in the left navigation bar of the admin center. Choosing this item will bring you to a settings page with three pivots. The **Overview** pivot shows some resource cards for various interesting items, along with a bar graph showing how your purchased licenses are allocated. The **Discover** pivot contains links to learning resources for administering and using Copilot. The most interesting pivot is the **Settings** pivot, which contains links to several Copilot settings. I write "links" because some of these items (such as the control of whether Copilot may be used in Teams meetings) are links to other admin center pages. As Microsoft adds more management controls for Copilot you will probably see this page expand.

The Free Copilot Chat Service

As it developed Copilot features for various parts of its ecosystem, Microsoft also built a ChatGPT-powered set of search tools for Bing named, not surprisingly, "Bing Chat." The original summer 2023 release of Bing Chat tools worked only on data sourced from the Internet, but in August 2023 they released "Bing Chat for Enterprise" (BCE), and then in October 2023 they renamed "Bing Chat" to "Copilot in Edge," and then at Ignite 2023 they renamed it again to just "[Copilot](#)" and released it to commercial availability on December 1, 2023. Here's how the [Copilot documentation](#) describes the product as of September 2024:

Microsoft Copilot (formerly Bing Chat Enterprise) is your everyday AI companion, providing AI-powered chat for the web... When eligible users sign in with their work or school accounts (Entra ID), Copilot adds commercial data protection ...Copilot is a public web service available to all users on copilot.microsoft.com, bing.com/chat, or through Copilot in Microsoft Edge and Copilot in Windows. Copilot is also available through the Copilot, Bing, Edge, Microsoft Start, and Microsoft 365 mobile apps.

Don't confuse this iteration of Copilot with Microsoft 365 Chat, which is what Microsoft now calls the 365-enabled Copilot tool that can read and query documents you have access to. This version of Copilot is only for browser-based search and chat.

Commercial Data Protection

The "Copilot public web service" can isolate searches from the Bing-integrated Copilot tool when you're signed in with a work account. This isolation feature is known as "commercial data protection." (CDP) When you are signed in with an Entra ID account, Copilot doesn't use any of your Microsoft 365 data. The [commercial data protection](#) capability prevents search queries from being retained or labelled with identifying data, and the queries and responses are not used for training the learning model. Here's how it works:

1. The user goes to an entry point for Copilot, such as copilot.microsoft.com, and signs in using their Entra ID account.
2. The Copilot service authenticates the user.
3. The user interacts with Copilot normally. Because she's signed in using an Entra ID account, the service knows that chat session data should be deidentified when it's passed to the Copilot orchestration service so that the orchestrator doesn't have the user's identity or organizational affiliation.
4. The orchestrator processes queries against various large language models (LLMs) and the Bing search index but cannot access any data held in the user's tenant. Graph-based grounding for Copilot queries requires Microsoft 365 Copilot.

When the user's session is over, the queries and responses are thrown away, so the standard Copilot chat history feature is disabled. Because queries and responses aren't passed to the user's tenant, they aren't subject to auditing or DLP controls.

Microsoft warns sternly that you need to leave this capability on, saying *"By turning commercial data protection off, your organizational data may be inadvertently leaked. We do not recommend turning commercial data protection off in Copilot."*

The commercial data protection service plan is included in the E1, E3, E5, and F3 SKUs of Microsoft 365 and Office 365, as well as the Microsoft 365 Apps for business and Apps for enterprise subscriptions. You can still have Copilot without this plan (e.g. if you have Copilot for Windows only, and no Microsoft 365 license), but the Microsoft 365-licensed plans all have it.

Enterprise Data Protection in Copilot

Starting in late September 2024, Microsoft is changing to a new system that they call "[enterprise data protection](#)" (EDP). It will replace the mechanism for commercial data protection described above, although their documentation does not reflect that fact. The implementation of EDP is significantly different in some important ways:

- Microsoft promises to handle all prompts and responses under its existing data handling commitments, including support for GDPR and ISO/IEC 27018. These protections aren't guaranteed under CDP.
- Copilot prompts and responses may be retained by retention policies.
- Prompts and responses can be logged and are subject to eDiscovery through the Purview toolset.
- Users won't see ads in the Copilot chat experience.

These protections are already in place for Microsoft 365 Copilot (the one you pay for)—the important point here is that EDP extends those protections to the no-charge Copilot chat service as long as the user signs in with an Entra ID account.

Copilot in Windows

Windows users can access Copilot chat through the browser. When Copilot integration for Windows first shipped, it used the Copilot app. From September 2024, users access Microsoft Copilot [through the Microsoft 365 app](#). This represents a significant change, but it allows Microsoft to deliver enterprise data protection support when for users who sign in to their PC using an Entra work or school account.

Controlling Access to Copilot Chat

Tenant administrators face somewhat of a dilemma. If you block Copilot altogether, users may still use the consumer version of Bing Chat (or other similar tools) to perform potentially sensitive searches. If you allow Copilot, people will use it for searching, but commercial data protection is supposed to keep your data from being misused. Microsoft seems to think the least bad choice here is to enable Copilot for all tenants with eligible licenses.

You use the associated commercial data protection service plan (its plan name is BING_CHAT_ENTERPRISE) to manage access on a per-user basis through the Microsoft 365 admin center or PowerShell. If you want to grant or deny users access to Copilot at the tenant level, the [documentation](#) suggests using a [PowerShell script](#), and that's now the officially supported way to control tenant-level access to Microsoft 365 Copilot in Bing, Edge, and Windows.

You can also block Bing Chat separately by mapping www.bing.com to nochat.bing.com in DNS. Mapping edgeservices.bing.com to the same subdomain applies the same behavior in the Edge sidebar.

Three Copilot Chat Scenarios

At this point, it might be helpful to run through three specific scenarios using the family of chat-based Copilot offerings. Let's consider three users: Anna's a home user with no Office licenses. Cecelia's a student with an Office 365 E3 license from her school. Erica has an Office 365 E3 license from work, plus a Microsoft 365 Copilot license with the "Microsoft Copilot with Graph-grounded chat" service plan.

Now, consider the following:

1. Anna uses her personal laptop to visit bing.com/chat and use Copilot. Her queries are not protected with commercial data protection (because she's not signed into a work Entra ID account). She does not have access to any Copilot features in Word, Outlook, Excel, or PowerPoint. Her queries can be used to train Microsoft's models, and they may generate advertising or content ranking data that Bing can use.

2. Cecelia signs into her school laptop using her school-issued Entra ID. She also visits [bing.com/chat](#). Her queries are protected by enterprise data protection, but she doesn't have access to Copilot in the Office enterprise apps or BizChat. Her queries aren't retained or used for training, and her school can't see any of the queries or responses.
3. In October 2024, Erica signs in to her work laptop using her work-issued Entra ID account. Her queries on [bing.com/chat](#) are protected by enterprise data protection. When she uses Microsoft Copilot from [microsoft365.com](#), her queries are grounded using the tenant semantic index. She has access to application-specific features in Outlook, Word, etc. Her queries are available for auditing and inspection through Purview, whether made through the chat interface or through Copilot interfaces in the individual applications.

Managing Microsoft Edge

Microsoft dedicates huge effort to make Edge a good browser. Edge is more stable and faster than Internet Explorer ever was and it boasts a steady stream of security and usability improvements. Edge is a core Windows component, of course, but Microsoft also ships versions for [macOS, iOS, Android, and Linux](#). In August 2023, Microsoft shipped a set of tools for centralized management of Edge under the umbrella "[Edge for Business](#)" brand. Microsoft's goal in introducing these tools is to allow enterprises to manage all the browser-based work that users do in a manner like what can be done with the policy tools for Office (discussed in the clients chapter), but to extend those management tools to personal use of the browser on work machines.

The Edge management tools live in the Microsoft 365 admin center; look under **Settings** in the left nav rail and choose **Microsoft Edge**, and you'll get a simple card-based interface that contains some links to Edge for Business documentation, plus links to the current set of Edge management features. To apply controls, you create one or more Edge configuration profiles, each of which can contain settings from any of [the 25 categories of policies](#) that Edge currently supports. These policies control things such as how switching between work and personal profiles work, whether users can take screenshots, which browser extensions Edge can load, and what default search provider should be used. You then assign profiles to Entra ID groups. "Managed Edge" (as Microsoft casually labels it) is still a new set of features, so they are soliciting feedback on the overall experience. Given how important the browser is in both Windows and the Microsoft 365 service, you should expect to see quite a bit more emphasis on Edge for Business coming from Microsoft in the future.

[Edge workspaces](#) are a [previously-announced](#) collaboration feature that lets any user in your tenant create a shared set of tabs that others can open. The workspace itself is saved in the creator's OneDrive. You can control whether or not users have access to workspaces by setting the corresponding Edge policy, which of course requires that you have started to manage Edge using Group Policy, Intune, or another management solution.

Managing Other Microsoft 365 Services

There are many other services in Microsoft 365 besides the "big four": Exchange, Teams, SharePoint, and OneDrive for Business. Microsoft has been adding new services at a rapid pace since it first launched the service.

Microsoft Bookings

Scheduling is a common problem for small businesses—think of the processes required to schedule an appointment with a hair stylist, veterinarian, or auto repair shop. Microsoft's tried to ease this burden both for the businesses that make up their customer base *and* the customers of those businesses by providing an app called [Microsoft Bookings](#). Bookings allows you to create publicly visible booking calendars (which are

essentially calendar-only mailboxes created by the Microsoft Substrate Management app) and define a set of teams or users that can be booked. For example, a counsellor could create 50- and 90-minute appointment options, then set up a Bookings page so that patients could choose the amount of time they wanted and pick an open slot. The Bookings engine takes into account service hours defined by the administrator, the Outlook working hours of any users assigned to the booking team, and individual users' free/busy times.

In addition to the shared bookings service, Microsoft includes a feature they call Personal Bookings. Users who are enabled for Personal Bookings receive a link that others can use to schedule meetings directly with them, similar to the popular [Calendly](#) service. For example, a product manager might create a Personal Bookings link so that customers can book product feedback sessions directly with her without the need for back-and-forth emails to find a mutually agreeable time slot.

The **Bookings** option in the **Org settings** section in the admin center allows you to control global aspects of Bookings configuration in your tenant, including whether it's enabled, whether users outside your organization can create bookings, and whether bookings pages collect certain customer data items such as phone numbers. You can also use the *Set-OrganizationConfig* cmdlet with the *-BookingsEnabled* switch.

The [Bookings page itself](#) is where authorized users can create services, manage staff assignments, and so on. Microsoft also maintains a [Teams app for Bookings](#). The settings available for enabling and disabling Bookings access for individual users are described in the user management chapter.

Microsoft Search

Microsoft Search, and its associated ecosystem of connectors and tools, has its own admin center under **Settings > Search & intelligence**. By adding [Microsoft Graph connectors](#), you can make data from external systems (including Atlassian Confluence and ServiceNow) visible throughout your enterprise via [Microsoft Search](#).

Power Platform

Power Automate and Power Apps are two of the main components of what Microsoft calls the Power Platform. Microsoft bundles the administrative elements for these components together into a [single admin center](#). See the Power Automate chapter for more information.

Dynamics 365

Dynamics 365, the latest version of Microsoft's venerable customer relationship management (CRM) system that competes with Salesforce, has a link labeled "Dynamics 365 Apps" in the **Admin centers** section. However, the link takes you to an error page if clicked while logged in to an account that doesn't have admin permissions on the organization's Dynamics 365 instance, and it takes you to the Power Platform admin center anyway.

Managing Microsoft Purview and Microsoft Defender

Microsoft 365 includes a broad set of security and compliance features. Some are included in base licenses, while others require additional licenses purchases. Microsoft's original vision was to provide a single portal to manage them all, so the original Security & Compliance Center smashed together compliance features from across the entire service with a specific focus on those that apply to multiple workloads rather than being specific to an application. Since then, Microsoft has added so many new security- and compliance-related features that they abandoned this vision and now have three independent portals for this functionality:

- [Microsoft Defender](#) portal (formerly called "Microsoft 365 Security Center"), shown as **Security** in the admin center list.

- The classic [Microsoft Purview compliance portal](#). This used to be called the Compliance center but, as part of the ongoing global rebranding of all Microsoft 365 compliance features to use the Purview name, it got a new name.
- The [Microsoft Purview](#) portal (purview.microsoft.com) appeared in December 2023 to replace the Azure Purview portal. It appears as **Compliance** in the admin center list. Microsoft is replacing the classic portal (described below) with a new version (also described below), which they began rolling out as GA in late July 2024. The new portal is the default, but there is still a toggle at the top of the portal which allows you to switch back to the legacy portal.

In addition to these portal changes, Microsoft has also renamed several members of the Defender brand family. What used to be called "Microsoft 365 Defender" is now called "[Microsoft Defender XDR](#)," and the Microsoft Defender for Cloud Apps (MDCA) product is [part of Defender XDR](#).

The portal updates all have a "getting started" interface that offers to lead you through a few of the major changes, and a way to provide feedback. Once you've dismissed this welcome section, you'll see the familiar card-based interface like the one in the Microsoft 365 admin center. You can customize the appearance of the security and compliance centers by moving the widgets around to suit the needs of your tenant; the **Add cards** button at the top of the pages will allow you to make changes.

Managing the Purview Portal

The new version of the Purview portal supports managing Purview for Microsoft 365, Microsoft Azure, Microsoft Fabric, and a variety of other platforms supported both by Microsoft and its partners. The left navigation bar is dramatically simplified compared to the classic portal, with only four items:

- **Home** shows a card-based dashboard with links to related portals and to subcategories that otherwise might be buried in a complex navigation tree. By default, there are entries for Information Protection, DLP, and Insider Risk Management, but you may see other or different cards as Microsoft or your admins make changes.
- Clicking **Solutions** produces a pop-over shortcut menu with entries for a number of specific functional solutions, which I'll detail below.
- **Learn** links to documentation for the components of the Purview family, including both admin- and developer-oriented materials.
- **Settings** provides an interface for managing settings for your account, roles and scopes, data connectors, and device onboarding and offboarding. It also contains links to settings pages for Communications Compliance, Records Management, and other subcomponents of the Purview family.

The **Solutions** item is where you'll do most of your work. The full page is subdivided into six sections. Each of the items here takes you to some part of the Purview ecosystem, and some items may overlap because of Purview's implementation of features such as data loss prevention.

The first section is labeled **Core** and contains two items:

- **Audit** allows you to search the service audit logs.
- **Settings** is another entry point to the settings item in the left navigation rail.

The **Risk & Compliance** section holds the following items, all of which take you to the corresponding Purview interface for managing their settings.

- **Communication Compliance**
- **Compliance Manager**
- **eDiscovery**
- **Information Barriers**

- **Records Management**

The **Data Governance** section has the **Data Catalog** and **Data Lifecycle Management** items.

The **Data Security** section contains the following:

- **Data Loss Prevention**
- **Information Protection**
- **Insider Risk Management**
- **AI hub** (currently in preview) is meant to be a central location for Purview compliance monitoring of use of Microsoft Copilot, ChatGPT, and other generative AI solutions. To make full use of it, you'll need to [install the Purview browser extension](#), which is used both for insider risk detection (on Chrome, Edge, and Firefox) and DLP item detection (on Chrome and Firefox). You can also use the AI Hub section to manage onboarding devices to Defender for Endpoint, which will give you some additional capabilities for controlling end user access to various public generative AI tools.

The **Resources** section is another link to the Purview documentation set, and the **Related portals** section is merely a collection of links to other portals (including Priva, Fabric, Entra, and the Service Trust portal).

Microsoft has extensively rearranged items across product features to make navigation more consistent. For example, the classic portal had a single item labeled **Classification**, but the new portal has a separate **Classifiers** navigation item added to the individual features that use classifiers. If you're experienced with the classic portal, you may find the new experience jarring. Microsoft's published a [guide showing where items from the classic portal have moved to](#) in the new portal.

Managing the Classic Purview Compliance Portal

The classic Compliance portal (contains the following sections in its left navigation bar.

- **Compliance Manager** combines a scoring system (known as Compliance Score) with a set of recommendations that you can apply to improve your score. Microsoft also includes assessment templates for specific compliance regimes (such as GDPR or US state-level data breach notification laws) that you can run against your tenant to see how you do. For more on this, see the compliance chapter.
- **Data classification** is where an organization manages the application of retention and sensitivity labels to control the protection and retention of user content through tools like the Content explorer and Activity Explorer. The compliance chapter covers retention labels and the policies used to distribute labels to workloads. The information protection chapter covers sensitivity labels.
- **Data connectors** create and manage connections to outside data sources that you want to include in your compliance coverage. For example, you can purchase a license to a connector that allows you to ingest data from AT&T's SMS network to archive and apply compliance policies to employee text messages.
- **Alerts** is where you view security alerts for the tenant. These alerts are created by alert policies, which allow you to set conditions that match the activity for which you would like to be alerted. There are dozens of alert conditions available covering a wide range of possible security concerns such as malware detection, file and folder sharing, DLP policy matches, permissions changes, and many more. The auditing and reporting chapter covers activity alerts and alert policies in more detail.
- **Policies** – This is intended to eventually be the primary management location for all your compliance and governance policies, including policies for data loss prevention and alerting. For example, this section gives you links to manage DLP policies for content stored or transmitted through Exchange Online, Teams, OneDrive for Business, and SharePoint Online.

- **Roles & scopes** - View role assignments that allow users access to compliance functionality and data. You can assign compliance roles (but not Entra ID roles) from this section. Users who hold the Global administrator right will have access to the Purview and Defender admin centers. You can use the roles listed in the Permissions tab to grant selective access to other users.
- **Trials** is essentially like the old SkyMall catalogs that used to grace every seatback pocket on commercial flights in the US; it's where Microsoft advertises trial versions of services that they hope you'll buy.
- **Solutions** – This section collects the tools you can use to take various compliance-related actions. For example, the audit logs, content searches, data loss prevention, and information protection toolsets are all linked from here. The best place to start is probably the **Catalog** section, which provides a simple grid view of different compliance-related tools in Microsoft 365 along with short explanations of what they do.

Managing Microsoft Defender XDR

[Microsoft Defender](#) (Figure 3-2) is a complex beast, and we're not going to cover the entire product suite in this book. The unified Defender portal has replaced the previous Security Center as well as the Office 365 Advanced Threat Protection portal. The sections and capabilities you see in your tenant may vary according to the licenses you've purchased, the region hosting your tenant, whether it's a commercial, academic, or government tenant, and what other services you've configured.

Figure 3-2: The Microsoft Defender portal

The Defender portal's left navigation rail divides into at least three sections-- there are currently nine sections visible in my tenant, but what you see in your tenant may vary. You can customize which items are shown with the **Customize navigation** link at the very bottom.

The top section covers the broad functional categories that are available in the Defender suite. These options appear for every tenant:

- **Home** returns to the main Microsoft Defender page.

- **Incidents & alerts** shows you data about security incidents that Microsoft has detected in your tenant.
- **Actions & submissions** collects data about messages that users have reported as spam, phish, or malware. By default, entries from the last 7 days are shown, but submitted messages are kept for up to 30 days. For any user-submitted report, you can forward the report to Microsoft and tag it as clean, malware, phish, or spam, or you can use the message to start an automated investigative process.
- **Trials** contains links to other Microsoft security and compliance services that you might want to try.
- **Partner catalog** contains links to selected Microsoft partners selling products or services related to security.

If you have assigned Defender licenses to accounts (either by buying them or starting a 90-day trial), you'll see additional categories:

- **Hunting** lets you perform security-related queries to look for suspicious activity, as well as configure custom detection rules to specify things that you consider suspicious.
- **Actions & submissions** adds an Action center that lets you review messages or attachments that look suspicious (or emails reported by users) and then optionally send them to Microsoft for further analysis.
- **Threat intelligence** combines information from the Microsoft Security Research Center and your tenant to give you a view of whether your tenant may be (or is!) under attack by specific known threats. It also contains informational articles about other threats and threat actors, including those related to non-Microsoft products. For Microsoft 365-related threats, the analytics shown include related incidents, the number of alerts against your tenant for that threat over time, and information about the specific emails related to the attack that Defender blocked.
- **Learning hub** contains an extensive set of documentation, videos, and other learning materials to help you figure out how and when to use the Defender suite.

One of the interesting features of the Microsoft Defender portal is that it unifies data formerly stored across modules; for example, if you had both Defender XDR and Microsoft 365 Defender for Endpoint, you'd have to look in two separate places to get a comprehensive view of incident data. Now all the incident data (or actions, or hunting rules, etc.) across all Defender workloads are collected into a single interface.

The **Exposure Management** section covers some specific items that Microsoft thinks will help you reduce your exposure to external attacks, including ransomware. The Secure Score reports covered later in the chapter are now here, along with tools for showing [possible attack paths](#) and a set of collected metrics specific to attack surface reduction.

The **Assets** section is next, at least if you have existing Microsoft Defender for Cloud Apps (MDCA) or full Defender XDR licenses. This section allows you to see and control objects, including identities, associated with cloud apps that you're managing.

The **Endpoints** section contains controls for Defender for Endpoint and its components, including Defender Vulnerability Management. You'll see this section even if you don't have Defender for Endpoint licenses; unlicensed tenants will see a "try now!" infobar at the top of the content area.

The **Identities** section is the front-end to Defender for Identity, so collects settings and metrics related to identity protection (led with an oversized, ugly, and needlessly-animated graphic showing how many cloud, on-prem, and hybrid user accounts your tenant contains).

The **Email & collaboration** section is next. Every Office 365 customer will see some of the options here; some specific options (such as the Campaigns item) require the Defender for Office 365 P2 SKU, which you may or may not have purchased.

- **Investigations** lets you view the results of [automated investigation](#) processes triggered either by the service itself or by you, in response to items shown in the **Explorer** pivot or
- **Explorer** lets you query messages to look for specific patterns; you can filter and query by date or content, and there are predefined pivots that will show you what the service has characterized as phishing messages, malware, or campaigns. One interesting view in Explorer will show you all the URLs in the selected set of messages, which is interesting in a creepy sort of way when you realize how many clickable objects show up in users' inboxes each day.
- **Review** shows a simple card-based interface that gives you easy access to the Action Center, quarantine, and user blocking portions of the portal.
- **Campaigns** shows how the service has categorized phishing messages that appear to be part of structured campaigns. Microsoft [says](#) that a campaign "is a coordinated email attack against one or many organizations" and having a view that shows which campaigns may currently be targeting your users is very useful in responding quickly.
- **Threat tracker** allows you to create, edit, and view the results of queries for specific email-based threats.
- **Exchange message trace** redirects to the message tracing tools in the EAC, described in the Mail flow chapter.
- **Attack simulation training** lets you run "benign cyberattack simulations" in Microsoft's words. The goal is to let you simulate various kinds of phishing attacks through SMS, web pages, and emails to see how your users respond and tailor your user education, policies, and response policies to improve your security. This feature requires licensing for Microsoft Defender for Office 365.
- **Policies & rules** contains links that give you access to assorted security policies from throughout the Microsoft 365 platform. For example, there are links to alerting policies, device configuration and compliance policies for Intune (see the Intune chapter), and anti-malware and anti-phishing policies from Defender ATP.

If you've purchased Microsoft 365 Defender for Endpoints, or Defender for Cloud Apps, you'll see other sections shown in the left nav bar as well. For example, Defender for Endpoints adds categories for device inventory, vulnerability management, and device configuration management under its section in the left navbar labeled **Endpoints**. Microsoft has more details on how Defender for Endpoint is integrated with the new Microsoft Defender XDR interface [in this article](#).

Below any add-on sections from Microsoft products you've purchased, you'll see a standardized set of additional options:

- **Reports** accesses security-related reports including summaries of mail flow, user-reported phish or spam messages, and potentially compromised users. You can't customize these reports; mailflow reports can be scheduled and mailed, or you can download any of them.
- **Audit** lets you search the unified audit log; you can also see and change any audit retention policies applied to your tenant.
- **Health** contains links to the Microsoft 365 message center and service health dashboard.
- **Permissions** and **Settings** do what you'd expect—note that these sections are both very bare-bones since most of the other interesting permissions and settings controls are in the primary Admin center.
- **More resources** contains a card-based set of links to other portals and tools in the Microsoft ecosystem that you might find useful.

Unified RBAC in Defender

It's a bad idea to have too many users with elevated permissions in your tenant. The Defender suite introduced a new problem for tenant admins: the security team needs permission to do security tasks in Defender, but they shouldn't have admin access to other parts of Microsoft 365... and vice versa. To solve

this, Microsoft has introduced what they call the "[Microsoft Defender XDR Unified RBAC model](#)." In this unified model, you can centralize permission management for several of the Defender products, along with Microsoft Secure Score. The unified RBAC model allows you to create and manage custom roles, and you can mix unified RBAC roles with the standard Entra ID role assignments. Unified RBAC is off by default; you'll have to [enable it](#) before it will do anything useful. Before enabling it, you should create the roles you want to use, which you can either do from scratch or by [importing existing roles from Defender products](#) you already have.

You'll need to review the documentation to get the complete details, but the main points to be aware of while creating roles are that:

- Defender permissions come in two flavors: "read" and "manage." You'll normally assign the read permission to users who should be able to read or see security data; only assign the manage permission to users who should be able to modify settings or take security actions.
- You can scope roles to specific Defender applications. For example, you can create a role that only grants the "Security data basics (read)" permission only to Defender for Office 365 data.
- For now, some Defender for Office 365 capabilities that are based on Exchange Online role assignments can't be managed with unified RBAC.
- If you only have Defender for Office 365, you can only use unified RBAC if you have Defender for Office P2 licenses.

Managing Azure Services

The Azure management portal administers other Microsoft cloud services for your tenant, or for separate Azure subscriptions that your organization also has. The link in the Microsoft 365 admin center takes you to the [Entra admin center](#). You can navigate from there to the entry point for the [Azure portal](#) to manage the other Azure services that your tenant uses such as Azure Automation and Microsoft Sentinel, and manage Intune mobile device and application policies.

Among the most common management operations are tasks such as creating new user accounts, updating their properties, and managing their permissions. As you learned in the Identities chapter, Microsoft 365 supports standalone and hybrid identities in a variety of configurations. The thing that all identity types have in common is that the service relies on Entra ID, so it's helpful to have some familiarity with the Entra ID management tools.

When you open the Entra ID section of the Entra portal, you'll see that it has categories for managing users, groups, roles, devices, Entra Connect, and password reset (along with several other categories). It also has links to controls for conditional access policies, reports for risky logins and suspicious sign-ins, and troubleshooting tools. A complete exploration of this section is far outside the scope of this book, but we cover selected parts of Entra ID elsewhere. It is well worth your time to explore the settings described in the Identities chapter, as many features and settings exist to improve the security and functionality of your environment that you may not be familiar with.

Miscellaneous Administration Tasks

There are several tasks that administrators may need to perform from time to time in the service. Microsoft often moves features around within the various portals, so you may find the tasks in these sections evolve as the portals evolve.

Using the Advanced Deployment Guides

A set of Microsoft "[advanced deployment guides](#)" are available in the Microsoft 365 admin center. These are similar in nature to the interactive guides that Microsoft used to provide with on-premises Exchange: they're

integrated with the service and organized in a logical progression so that you can use them to build out your environment. The [list of guides](#) shows several dozen, including guides for Configuration Manager integration with Office apps, Viva Engage deployment advice, and Teams Phone deployment guidance.

The guides are available through the **Setup** item in the admin center left navigation rail. When you visit the deployment guide page, you'll see a summary showing your current adoption and secure scores and a categorized list of guides. For example, you might choose the "Add or sync users to Microsoft Entra ID" guide from the "Configure scenarios" category. When you choose a guide, you'll see a wizard-based interface that leads you through specific steps, including links to tools in the various admin center; the interface will monitor your progress through the guide so that you can come back and resume work later if for some reason you're interrupted. Some of the guides are more useful than others, but for many common scenarios, the guides can provide a valuable starting point if you're not sure exactly how to set up a feature or what order the required steps must be performed in.

Controlling Microsoft's Communications with Your Users

Many administrators don't want to allow Microsoft to communicate directly with end users in the tenant. They believe (and I agree) that the tenant administrators should control the nature, timing, frequency, and content of communications, if any, between service providers and users—after all, the individual users in an enterprise tenant aren't the customer, the organization is. Microsoft has received quite a bit of justified criticism for bombarding users with messages about Microsoft services and features, including some messages that are very similar to advertisements. An example of the kind of email that Microsoft might send is a "welcome to Copilot" email generated when you assign a user a Microsoft 365 Copilot license, either in the admin center or through group assignment or other means. This message may have value to the end user, or it may not, but the tenant administrators should retain control over whether Microsoft is able to send it in the first place.

The **Org settings > Microsoft communication to users** gives you a small degree of control over this behavior by providing a checkbox that allows you to give Microsoft permission to "receive email from Microsoft about how to use Microsoft 365 products." This wording is vague, intentionally so, and there's no way for you to specify any more granular set of permissions. However, a link from this settings page ([which points here](#)) allows you to send canned "training" emails on various topics. For example, the "Outlook mobile" topic includes marketing copy, photos, and a download link that try to convince users of the benefits of using Outlook mobile. You may or may not find these emails useful, but they will only be sent if you explicitly ask for them *and* you have allowed Microsoft to send mail directly to users.

Customizing the Microsoft 365 Interface

One of the big selling points behind Microsoft 365 is that it has a consistent and familiar interface, both for users and administrators. Microsoft doesn't want any of us going overboard with interface customizations; they have included a few features to help tailor the Microsoft 365 client interfaces to the needs of specific organizations though.

Customizing Notification Emails

In general, you can't customize the contents of emails sent out by the service. These emails might include digests (such as the Viva Insights digests) or notifications. By default, they will come from domains associated with Microsoft (such as *sharepointonline.com*); However, Microsoft allows you instead to select one of your own verified domains for these messages. This is a bit of stage magic, in that the messages aren't truly being generated by your domain, but they will appear to users as though they come from your verified domains. That means two things: users won't see the messages tagged as [EXTERNAL], but also, if

your domain security settings (including SPF and DMARC records) are wrong, they may not be delivered at all. This feature is currently opt-in, and you can enable it by following the [instructions here](#).

Creating Custom Help

Tenants can create a custom help card to be displayed alongside the standard help text revealed when a user clicks the question mark (?) icon in a browser while accessing an application. The idea is that you can provide users with tenant-specific information to allow them to seek help if they have a problem. To create a custom help desk card, open the Microsoft 365 admin center and go to **Settings -> Org settings** and then click the **Organization profile** pivot. Click the edit icon beside **Help desk information**.

The screenshot shows the 'Help desk information' configuration page. At the top, there is a note: 'Streamline user support by adding your organization's contact information to the Office 365 help pane. It will appear beneath default help topics.' Below this is a link 'Learn more about adding your org's help desk info'. A checked checkbox 'Add your help desk contact information' is present. The form fields include:

- Title ***: Office 365 Book Support People
- Contact information ***:
 - Phone**: +1 650 561 4136
 - Email**: bookSupport@office365itpros.com
 - URL**: http://support.office365itpros.com
 - Book Support**: (This field is empty)

Figure 3-3: Populating custom help desk information

The admin center displays the input screen shown in Figure 3-3 and you can enter:

- A title.
- Phone number details.
- Email address.
- Web page.

The next time a user signs in using a web browser, they see the custom help desk card when they access help.

Office 365 supports a single custom help card per tenant. You can't, for instance, have location-specific help information presented to users. For this reason, if you manage a tenant that has users distributed in multiple locations or countries, you should make sure that the information provided in the custom help card is valuable for all users. For instance, it does not make sense to direct a user in Japan to a help desk in the U.S. if that help desk is unable to speak Japanese or is only available during U.S. working hours.

Custom Tiles

When users sign into the Microsoft 365 portal, or when they click the waffle menu (the App Launcher) from a browser application such as OWA, a list of tiles for the applications and services to which they have access

appears. Users can select apps to appear in the launcher from their My Apps page, which lists the apps known to the tenant. The apps that appear in My Apps come from several sources:

- Standard apps licensed from Microsoft as part of the plan assigned to the user account. For example, OneDrive for Business and Stream.
- Apps that are developed for or by the tenant. Administrators then configure the app to assign it to individual users. These might be line-of-business applications that are registered in Entra ID or applications written by ISVs and stored in the Azure application marketplace, such as DocuSign, DropBox, or Citrix GoToMeeting.
- Apps created with the Office 365 API Tools for Visual Studio that allow users to sign in using their Microsoft 365 credentials. These apps automatically show up on the My Apps page.
- Web apps from AppSource that support single sign-on.

Custom tiles are available to accounts that have an Exchange Online mailbox and are the simplest and easiest way to customize the App Launcher. Essentially, a custom tile serves as a pointer to a web page. The URL defined as part of a custom tile can bring a user to a SharePoint site, Microsoft 365 Group document library, external website, or any other page accessible through a URL. The custom tiles that are defined for a tenant are listed in the My Apps page displayed to users and can be pinned to the App Launcher from there.

To add a custom tile, login to the Admin Center and navigate to **Settings -> Org settings**, and then click the **Organization profile** tab, then choose **Custom tiles for apps**. Click + and you'll be able to add a custom tile by specifying the name of the tile, the URL that the tile should invoke when clicked, a description (purely for administrative purposes), and a URL for an image for the tile icon. The image must be in JPEG format and should be sized at 50 x 50 pixels. It is easiest if the image file is stored in a SharePoint library as this means that it is accessible to users. In addition, make sure that all users have at least read-only access to the tile image. If users don't have access to the image file, a blank space is shown for the tile in the My Apps library.

Hiding launcher tiles: Many administrators want to hide specific applications from users by removing the application tiles in the app launcher for all (or some) users in the tenant. Unfortunately, there's no way to do this. The list of tiles the user sees is dynamically built based on the licenses you've granted them. Users may add and remove tiles themselves but there's no way for you as a tenant administrator to do this in bulk. If you don't want users to use an application, instead of hiding it in the launcher and hoping they don't stumble across it, you'll have to remove the license (or deactivate the application) for those users. You can also hide [all custom tiles](#) or set up [application collections](#) that have predefined sets of tiles for users to see.

Managing Themes

Microsoft has long offered the ability to apply themes or skins to various applications. This ability started with Outlook Web Access in Exchange 2000 or so, although creating themes for on-premises OWA was always sort of a hit-or-miss proposition and wasn't generally supported. With the move towards cloud-based services, Microsoft has provided a more robust theming mechanism that allows you, or your users, to select themes that apply to the Microsoft 365 admin center and various applications. There's a similar facility in the [Microsoft 365 Apps](#) as well. The drawback? You can't customize these themes very much.

If you open the **Organization profile** settings for your tenant in the Microsoft 365 admin center (under Org settings), you can select **Custom themes** to edit items like:

- The corporate logo for display on Microsoft 365 web pages. The selected logo file must be sized precisely at 200 x 30 pixels and be less than 10 KB. Files in SVG format are best because these are supported by mobile apps. You can also associate a link that users go to when they click the logo.
- The navigation bar color. This should match the color of the background image.
- Text and icon color. This should highlight text and icons when overlaid on the navigation bar.

Of the other available settings, the most important one is probably the **Prevent users from overriding their theme** checkbox. If for some incomprehensible reason you need to exert a kindergarten level of control over your users' choices of theme, this is where you'd do it.

Speaking of themes: Microsoft occasionally releases new ones for users. Currently, there are more than 50 themes available to users under the gear settings icon. Some themes are whimsical, while others are merely solid-color sets.

You can create up to five separate themes of your own and then [assign them to members of specific Microsoft 365 Groups](#). Microsoft originally referred to this as "conglomerate branding" but now seems to prefer the term "group branding." Each of the themes can have a unique experience, including separate company logos (and a logo variant for dark mode).

Branding

SharePoint Online has a set of tools for applying consistent branding (including colors, logos, and even fonts) to your SharePoint Online sites. Known as [Brand Center](#), these tools have their own one-time setup feature in **Settings > Brand Center**. From this page, you can create the Brand Center site for your organization and assign permissions that allow brand managers to create and manage assets, which you can then use in SharePoint-based apps.

Sending Organizational Messages

Sometimes your organization may need to send messages to some, or all, users to tell them something about their use of the service. The old-school way to do this for the admin to send email to the users directly. To support a higher level of abstraction, Microsoft has several ways to send organizational messages to users. Some are available to you as a tenant admin, while Microsoft reserves others for their own use. Here's the current set:

- Microsoft may send service notifications, suggestions for third-party applications, Windows Tips, and other (possibly annoying) messages directly to users. In Windows 11, you can use Intune to allow or deny specific categories of messages.
- Microsoft may send other types of messages (such as "Try the new Outlook!") directly to users. The frequent queries about whether you'd recommend the Office apps or Windows to a friend fall into this category. You can't block these, which is a real shame.
- You can configure Adoption Score-related organizational messages, as described later in this chapter in the section on Adoption Score. The intent of these messages is for you to send messages based on user adoption and activity of specific features.
- If you're using Intune, you can use it to send branded, personalized messages to users through Windows 11 components such as the Notification Center. You can read more about this capability in [Microsoft's documentation](#) but we won't cover it further here.
- You can send custom, branded [organizational messages through the Microsoft 365 admin center](#).

This last category deserves further explanation; it's currently in preview but it will eventually become the primary way for you to communicate with groups of Windows 11 users in the service. If you navigate to **Reports > Organizational messages** in the admin center, you'll see actions that allow you to create a new message, create an urgent message, or review information about how your previously-sent messages are performing. This feature allows messages to be created by users who hold the Global admin or [Organizational Messages Writer](#) roles. For now, there are no additional Windows or Office licenses required to use this functionality but Microsoft's documentation notes that they may require specific license levels for this capability in the future.

When you create a new message, you enter a wizard-based process that starts with you choosing a category for your messages such as “onboarding” or “tech updates.” The category is informational, not prescriptive. You next choose where you want the message displayed: in the Windows 11 notification center, in the Windows 11 taskbar, or as hotspots over a custom desktop image. Notice that all 3 of these options only work on Windows 11 devices.

Currently, you must create your own message contents, although Microsoft has promised to offer editable templates in the future. Figure 3-4 shows an example of message creation. Currently you must specify valid values for all fields, including the logo.

The screenshot shows the 'Create a message' wizard interface. On the left, a vertical navigation pane lists steps: 'Messages' (selected), 'Objective', 'Location', 'Template', 'Customize' (selected), 'Recipients', 'Schedule', and 'Finish'. The main area is titled 'Write your message'. It contains fields for 'Title' ('Try Copilot for Copilot!'), 'Body' ('You can put Microsoft Copilot to work to help you figure out which Copilot to use! Try it now.'), 'Add button text' ('Try it'), 'Add link' (URL 'https://www.thisisfake.com' with an 'Open link' button), and 'Add your organization's logo' (a placeholder for a 64x64 pixel file). To the right, a 'Preview' section shows a sample notification card with the title, body, button, and link. A note says 'This is an example of what the users will see.'

Figure 3-4: Creating a new notification message shows you a preview of what users will see

Once you write the message, you can choose groups to include or exclude and specify a time window when users should see it. Thankfully, as part of this process you can also specify the interval at which users should see the message—for example, if you choose “once a month,” users will see the message once. If they dismiss it without interacting with it, they’ll see it again a month later. You could also choose a more obtrusive interval (such as “weekly ten times”) if you prefer.

After you’ve completed writing the message, it still requires approval from someone in your organization who holds either the Global admin or Organizational Message Approver role. Users cannot approve messages they created, even if they hold the appropriate roles; this is a useful safety measure. Once a message is submitted, the creator can withdraw it before approval, or the approver(s) can approve or reject it.

After you’ve approved at least one message, you’ll be able to see statistics about the messages, including how often they’ve been presented to users, how often users have clicked through them, and the clickthrough rate. This data is aggregated, so you can’t tell whether a specific user has seen or interacted with any message. Activity data can be viewed in the dashboard or exported to a CSV file.

There are a few additional nuances, such as the ability to copy an existing message and resubmit it as new, but this basic write-create-monitor cycle is the fundamental flow.

Service Administration Apps for Mobile Devices

Microsoft ships a tenant management app for Android and iOS. The management apps can perform common administrative tasks from a PC or mobile device including editing or removing users, resetting passwords, turning email forwarding on or off, and viewing service health information. You can review billing alerts, items posted to the Message Center, and service health notifications. In fact, you can have the app post push notifications when specific service health notifications are issued. However, the management apps do not support managing any aspect of a hybrid configuration.

ServiceNow Integration

As much as Microsoft might wish it otherwise, ServiceNow is the most popular IT service management (ITSM) solution in the world. It's common for Microsoft 365 administrators and support desk staff to have ServiceNow open in one tab with various Microsoft admin portals open in other tabs. In a welcome move, Microsoft published an [app in the ServiceNow app store](#) that provides some integration between the two. If you install the app in your ServiceNow instance, you can review SHD items and open new tickets with Microsoft, and people can use the ServiceNow virtual agent to perform some limited self-service actions. This integration is a useful capability and it'll be interesting to see what Microsoft does to enhance it in the future.

Managing Integrated Apps

Microsoft has worked for literally decades to make Office an extensible platform, both because it enables them to extend and improve the platform but also because it enables their partners to do so, which in turn helps to retain customers. This strategy has continued into the present day, leading to the new **Integrated Apps** page under the Settings tab. The controls here allow you to select and deploy add-ins that run inside various Office clients. Figure 3-5 shows the view from a sample tenant. To use these app management features, you must use an account that's assigned the Global Admin, Global Reader Admin, Exchange Admin, or Azure Application Administrators role.

The screenshot shows the 'Integrated apps' section of the Microsoft 365 Admin Center. At the top, there's a header with 'Home > Integrated apps' and a 'Dark mode' toggle. Below the header, a section titled 'Popular apps to be deployed' lists several add-ins with their logos, names, descriptions, 'Get it now' buttons, and 'View details' links. Below this, a table lists currently installed add-ins with columns for Name, Host products, Status, Test deployment, and Last modified. The installed add-ins include MURAL, SurveyMonkey, YouTube, Zoho Projects, Power BI, and monday.com.

Name	Host products	Status	Test deployment	Last modified
MURAL Take ideas from imagination to activation with MURAL in Microsoft 365.	Office, Outlook, Teams	OK	No	2023-09-26
SurveyMonkey Seamlessly capture feedback and view results for better decision making.	Office, Outlook, Teams	OK	No	2023-09-26
YouTube Search for videos on YouTube	Office, Outlook, Teams	OK	No	2023-09-26
Zoho Projects Create and manage projects effectively with the collaborative Zoho Projects	Office, Outlook, Teams	OK	No	2023-09-26
Power BI Uncover insights in your data.	Office, Outlook, Teams	OK	No	2023-09-26
monday.com Create, open and update monday.com items without leaving Microsoft.	Office, Outlook, Teams	More apps available	No	2023-09-26

Figure 3-5: The Integrated apps view lets you centrally install and publish Office add-ins to users

You may notice that the caption at the top refers to applications developed by Microsoft partners, yet some of the applications (such as FindTime) shown in the list are from Microsoft. If you use the **Get apps** button to jump to the AppSource marketplace for Microsoft 365 Apps add-ins, you'll find several dozen add-ins, many of which come from Microsoft, so don't let the "partner" wording fool you.

Any add-in written to use the [correct set of APIs](#) can be deployed and managed here. The beauty of this approach is that a well-written add-in for, say, Outlook will work in any recent version of Outlook, including the desktop, mobile, and web versions. The advantage of using the **Integrated apps** page is that you can select an add-in, optionally create a test deployment, and then specify which users can access the app (just you, the entire organization, or a list of users or groups you specify). Because these apps are add-ins downloaded and run by the client application, you don't have to do anything further to deploy these capabilities to users.

Managing Feature Releases

Microsoft uses a series of "rings" to control the release of new features. In general, the first ring is the development team, the next is Microsoft, the third is composed of tenants who have nominated themselves by signing up for "Targeted Release," and the last is general availability (also known as "standard release"). This approach varies by workload; individual applications, such as Teams or Planner, may use more rings in their deployment model.

"Standard release" is the term Microsoft uses when they make a feature available to all tenants licensed for the functionality. Tenants who opt for Targeted Release see new features (or updates to existing features) a few weeks ahead of general availability. However, for some new applications, the period covered by Targeted Release can extend over several months.

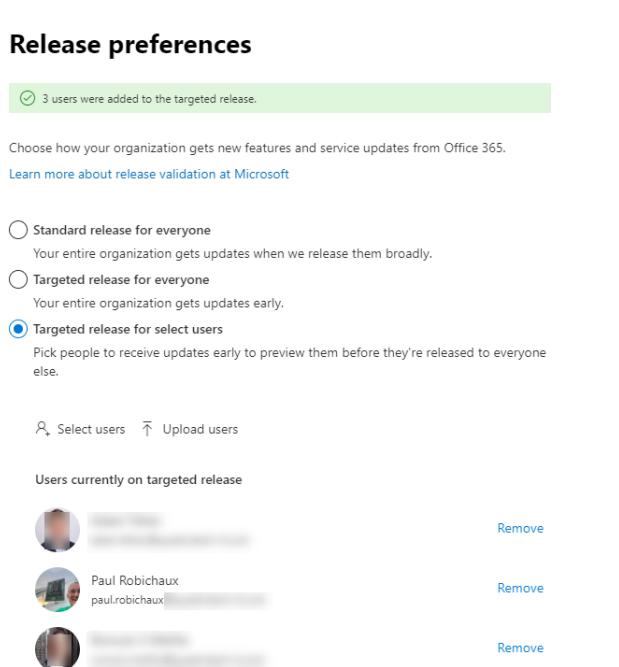


Figure 3-6: Enabling Targeted Release for a tenant

The ability to control how new features become available to tenant users is through **Release preferences** in the **Organization profile** pivot, available through the **Settings > Org settings** section of the Microsoft 365 admin center. Three options are available:

- Standard release for everyone.

- Targeted release for everyone.
- Targeted release for selected users (Figure 3-6).

The last option allows the administrator to nominate specific individuals while the remainder of the users continues to access the functionality available in the standard release. For example, you might decide that only the IT department should be exposed to a new application to allow some experience to be gathered about its functionality and so drive a decision about how it might be used within the organization. You can either select individual users or upload a file of users to enable; the file should be a plain-text file with one user UPN on each line.

Switching an account from Targeted Release to Standard Release or vice versa can take up to 24 hours before the switch is completed. Keep in mind that putting a user in Targeted Release just enables their ability to see or use a feature; client-side features implemented in the Microsoft 365 Apps software won't be visible to the user until she downloads the appropriate version of the software. Depending on your organizational policies, this may add an extra delay before the new features become available.

Although Microsoft's goal is to move features from Targeted Release into general availability reasonably quickly, the exact period between the two phases can vary from feature to feature. Timings can be affected by user feedback, bug reports, or the discovery of flaws such as performance or scalability issues that must be addressed before a feature can be made available to all. The shortest period is a week or so. The longest (to date) is six months. The rate of change also varies within applications. Exchange Online tends to see more new features over a certain period than SharePoint Online, but Teams outstrips them both—thankfully, Microsoft has added Teams to Targeted Release, at least in the commercial cloud offerings.

Even when a feature is released to general availability, it doesn't mean it shows up everywhere at once. It can take a few weeks before every tenant in every data center sees a new feature. The exact speed of deployment depends on the results of Targeted Release deployments, plus other factors such as local market support. Microsoft also often staggers feature release dates by geography. In general, features tend to appear first in North America, the UK, Western Europe, and Australia, then in other areas. For example, more than two years after the first release of Teams phone calling features, the feature isn't available worldwide yet.

Another factor in feature availability is the type of tenant you have. In general, enterprise tenants get features first, and education and government tenants (including those in GCC and 21Vianet) come later, if at all. The small-business versions of Microsoft 365 fall somewhere in the middle. Keep in mind that Microsoft appears to believe that they will make the most money by delivering all their features to all tenants everywhere, so this is their aim; when they don't make a feature available in a region or to a type of tenant, it's either because engineering, operational, or legal constraints exist to prevent it or because the feature requires enough investment that it may not be profitable for them to deploy it.

When new features arrive in your tenant, they will almost always be enabled by default for all users with the necessary licenses, regardless of your Organization Profile settings. That includes features such as Microsoft Teams and Copilot that Microsoft added as service plans to current products; in other words, Microsoft added the features to existing licenses such as Enterprise E1, Enterprise E5, and so on, rather than creating separately licensed services like Intune or the various Dynamics 365 services. Applications that don't require a separate license are also usually enabled by default. Note that over time, some applications may change their licensing status; as one example, Whiteboard, which originally had no license, is now a licensed service plan within the Office 365 SKUs, which means that tenants can control if users have access to Whiteboard by granting or denying that specific service plan.

Features released in Public Preview before General Availability are not enabled by default; however, they will become enabled once the feature reaches General Availability. The approach of enabling features by default

makes adoption easier but is a concern for organizations that have strict change management procedures, or those who want to control the rollout of new features so that they can provide appropriate training to their IT support staff and end-users. It is important to maintain awareness of the changes that are rolling out to customers by monitoring your Message Center notifications and keeping an eye on other sources of early information such as the [Microsoft 365 roadmap](#).

Mastering Targeted Release: Targeted Release allows tenants to gain faster access to new functionality. However, there is a downside to the value gained by seeing new features earlier than the norm. Microsoft tests new code before making it available through Targeted Release, but it is well known that frayed edges (bugs) can appear in new software when exposed to the stresses of production workloads. Other common challenges include new features showing up in user interfaces without warning or any sign as to how they should be used with little or no available documentation. Selective Targeted Release is available to allow some users in a tenant to access new features earlier, but this option is sometimes not supported by an application.

To mitigate these downsides of Targeted Release, some companies run two tenants: a "production" tenant for most users and another trial tenant configured as Targeted Release for a small subset of users responsible for testing new software as it appears. This is analogous to the situation often found in the on-premises world where customers keep a test environment to deploy new builds of Exchange as Microsoft makes them available.

It is important to realize that the appearance of a new feature to tenants who have enabled Targeted Release does not mean that the feature will be made available for all tenants soon afterward. Microsoft can and does use time to gain knowledge of how customers use a feature and can adapt and change the feature over an extended period before deciding that the software is suitable for general consumption and ready to be rolled out globally. Targeted Release is a large-scale beta program, and no assumption should be made when or if any feature will be available just because Microsoft makes the functionality available to tenants configured for Targeted Release.

Managing User Feedback

Getting useful feedback from users is one of the key challenges of making software. Just like every other software company, Microsoft is eager to collect feedback from its users; it uses that data (which might include direct feedback, crash logs, survey results, or metadata about application usage) to see what people think about its products and services and how they can be improved. It may seem sometimes like the Microsoft 365 product teams aren't listening to the feedback their users generate, but nothing could be further from the truth—it's just that getting good-quality feedback is difficult, and at the scale of the service, it's also difficult to parse and interpret it.

There are several interlocking sets of settings that control what happens to this feedback and who can see it:

- The native Windows, macOS, Android, and iOS crash-dump systems all have controls over whether crash logs from an application failure are automatically shared with the application vendor; in general, I encourage users to enable these settings so that the vendors can identify patterns of crashes caused by OS updates, product bugs, and so on.
- Most of the Microsoft 365 apps have an "[in-product feedback](#)" feature (usually in **Help > Feedback**) that lets users submit feedback directly to Microsoft while using Excel, Outlook, or other apps. T
- Teams has a "Give feedback" feature in its desktop and web clients, and a similar feature in the mobile versions, that you can control with the `Set-CsTeamsFeedbackPolicy` cmdlet.

The admin center includes a **Product feedback** item under the **Health** section in the left navbar; here you'll see all of the feedback that users have submitted. However, before you see anything, users must submit some feedback... and before they can do so, you must enable that by creating a feedback policy with the Office cloud policy service, as described in the clients chapter. You can specify whether users can submit feedback, whether Microsoft can follow up with users who do so, whether users can see and delete their

previously submitted feedback, and whether the feedback may contain log files, content snippets, or other organization-specific metadata that might potentially be sensitive.

Teams Room System devices may prompt for feedback at the end of meetings, and these prompts aren't subject to the Office cloud policy service settings. These feedback surveys don't gather any personally-identifiable information, which is good, but for now, you can't turn them off, which is less good.

There's also a feedback mechanism that you can use to gather net promoter score (NPS) data from your users. It uses the same policy mechanism as the product feedback system described above but collates the data and uses it to present NPS data that you may find helpful as a guide for your adoption and rollout planning. They've made various other tweaks to this feature (including labeling feedback as positive, neutral, or negative and showing some analysis of the number of NPS reports submitted from various sources) and there is probably more to come here.

Somewhat confusingly, there's a *completely different* mechanism for anyone to submit general feedback for a range of Microsoft 365 services. The [homegrown feedback portal](#) uses the Dynamics 365 Customer Service module, and the portal's design makes it easy to submit and share ideas with engineering groups.

Managing Licenses, Plans, and Billing

Everyone who wants to use an application besides the administration tools needs a license. Because Microsoft controls all aspects of the service, they can be more insistent on this point than they are with on-premises Client Access Licenses (CALs). You cannot use an application like Exchange Online without a license and an account that has its license removed will end up losing all its data. License management is therefore an important part of administration, with the goal being to ensure that you have enough licenses to allow people to work while not paying for unused licenses. The **Billing** section in the admin portal allows you to buy licenses, see and manage the licenses you have, and get various types of billing notifications.

The screenshot shows the 'Licenses' section of the Microsoft Admin Center. At the top, there are navigation links for 'Home > Licenses' and a 'Dark mode' toggle. Below the header, there are three tabs: 'Subscriptions' (which is selected), 'Requests', and 'Auto-claim policy'. A note below the tabs says: 'Select a product to view and assign licenses. Each product below may contain licenses from multiple subscriptions. [Learn more about assigning licenses](#)'.

Below this, a link 'Go to Your products' is provided to manage billing or buy more licenses. The main area displays a table of products with columns: 'Name', 'Available licenses', 'Assigned licenses', and 'Account type'. The table includes the following data:

Name	Available licenses	Assigned licenses	Account type
App governance add-on to Microsoft Defender for Clou...	23	2/25	Organization
Enterprise Mobility + Security E5	239	11/250	Organization
Microsoft Defender for Cloud Apps	0	1/1	Organization
Microsoft Fabric (Free)	Unlimited	3	Organization
Microsoft Power Automate Free	9997	3/10000	Organization
Microsoft Stream Trial	Unlimited	0	Organization
Office 365 E3	11	14/25	Organization
Power BI Pro	0	1/1	Organization
SharePoint Syntex	1	4/5	Organization

Figure 3-7: Managing licenses in the Products and Services section of the admin portal

The **Licenses** option in the Billing section in the admin portal provides an overview of the licenses available to, and used by, a tenant (Figure 3-7). Note that some Office 365 E5 licenses are unassigned. This might

become an issue if the situation persists because Microsoft charges for every license monthly even if no one uses the license.

Note: There are several ways to buy licenses. Depending on what subscriptions you have, and whether you have a licensing agreement with Microsoft, you may buy licenses directly through the web portal, through a reseller or partner, or directly from Microsoft. For partner and Microsoft purchases, the license term and cost are whatever you negotiate; for purchases directly through the portal, the licenses you buy cover a 12-month term, but you may pay for them monthly or annually. In either case, you pay up front. Microsoft doesn't give refunds for unused licenses. As you add licenses, you will see them "roll in" at renewal time. For example, suppose that on January 1 you create a new tenant and buy 100 Office 365 E5 licenses. Then in March, you buy another 100 licenses. Come January 1 next year, all 200 licenses will renew at the same time.

The usage reports in the Microsoft 365 admin center provide you with a basic view of who uses the various services, with varying levels of detail available for different services. For example, the Copilot and Visio reports allow you to see who's using (or not!) the expensive add-on licenses those products require, so you can make better decisions about how to allocate them. The **Requests** and **Auto-claim policy** pivots under the **Licenses** view are covered in the user management chapter, as they deal with automating (at least partly) the process of assigning licenses to specific users.

You can also perform some license management tasks in the **Your products** section under the **Billing** section, as shown in Figure 3-8. Functionally the two areas of the portal are very similar, allowing you to assign licenses or buy more if you have no unused licenses. The "Settings & actions" section in each license card allows you to take appropriate actions, including installing the Office desktop apps (if licensed) or assigning licenses to users. The **Your products** section can also show Azure subscriptions, purchased third-party applications, and usage benefits associated with enterprise agreements (EAs) or other purchase contracts.

Product name	Assigned licenses	Purchased quantity	Subscription status
App governance add-on to Microsoft Defender for...	2	25	Expired: 5/31/2023
Enterprise Mobility + Security E5 Trial	11	250	Active: Expires on 6/22/2023
Microsoft Defender for Cloud Apps	1	1	Active: Renews on 10/9/2023
Microsoft Fabric (Free)	3	1000000	Active
Microsoft Power Automate Free	3	10000	Active
Microsoft Stream Trial	0	1000000	Active
Office 365 E3 for MVP Trial	14	25	Active: Expires on 8/2/2023
Power BI Pro	1	1	Active: Renews on 10/20/2023
SharePoint Syntex MSIT Trial	4	5	Active: Expires on 1/2/2024

Figure 3-8: The Your Products view shows licensing and subscription data

The other items in the **Billing** node allow you to select and set up payment methods for your bills, choose who gets billing notifications and in what language and format, and buy new products—but all of these options are simple enough that we won't discuss them further here.

For more information on how to assign licenses to users, see the user management chapter.

Managing Network Connectivity

Each of the workloads in Microsoft 365 has its unique requirements for connectivity. There are two basic invariants: every service needs reliable and correct DNS information, and every service needs to be able to pass traffic on TCP port 443 to allow TLS-protected HTTP communications. Individual services may have additional connectivity requirements for various features. This seems easy to deal with in theory... right up until users start complaining that some feature or another in their clients isn't working properly.

Some years ago, Microsoft introduced a tool called the Exchange Remote Connectivity Analyzer (ExRCA) for troubleshooting on-premises connectivity for MAPI and Exchange ActiveSync. Over the years that tool has grown in scope and power and is now known as the [Microsoft Remote Connectivity Analyzer](#). It currently supports more than two dozen tests for Exchange, Teams, on-premises Skype for Business and Lync, and Office 365.

Currently, the analyzer supports the following tests on the Exchange Online tab. Some tests require you to provide valid credentials for an active Office 365 account that's licensed for the workload you're testing because the test requires logging into a mailbox or Teams account; others (such as the Outlook Mobile modern authentication test) require an email address but not a password:

- DNSSEC/DANE: this test checks the DNS records you have defined using the same DNS resolution path that Exchange Online users. If any of these tests fail, so will DANE resolution for your domain.
- Exchange Online custom domain test: this test validates whether the specified custom domain is correctly set up and has valid MX records for mail flow into the service.
- Exchange ActiveSync test: this set of tests emulates a mobile device and makes Exchange ActiveSync requests for synchronization to ensure that EAS network traffic works properly.
- Synchronization, notification, availability, and automatic replies test: this set of tests checks various Exchange Web Services (EWS) network flows that are used by Outlook clients.
- Service account access test: this test verifies whether the specified account is correctly configured to use Exchange impersonation for service account-level access to mailboxes.
- Outlook connectivity test: as its name suggests, this test suite does an end-to-end test of all the steps performed by the Windows Outlook client for it to connect over RPC or MAPI over HTTP.
- Inbound SMTP email test: this test checks whether the DNS and network configuration of your tenant is correct so that outside servers can send mail to it.
- Outbound SMTP email test: the inverse of the inbound SMTP test, this test checks whether your outbound IP address has correct reverse DNS, Sender ID, and real-time block list (RBL) settings.
- POP email test and IMAP email test: these tests perform the same steps that a POP or IMAP client takes to verify connectivity.
- Free/busy: this test verifies that a cloud mailbox can access on-premises free/busy data, and vice versa.
- Outlook Mobile hybrid modern authentication test checks to see whether you've correctly set up hybrid modern authentication between Exchange Online and your on-premises Exchange environment.
- Mailbox provisioning test: this test checks to ensure that the specified mailbox is correctly provisioned in the service and that all the required directory attributes have valid values.

The Exchange Server tab has many of the same tests as Exchange Online, with one unique addition: an SSL test that validates whether the selected endpoint has the correct certificate and is compatible with the TLS 1.2 enforcement settings currently in use by the service.

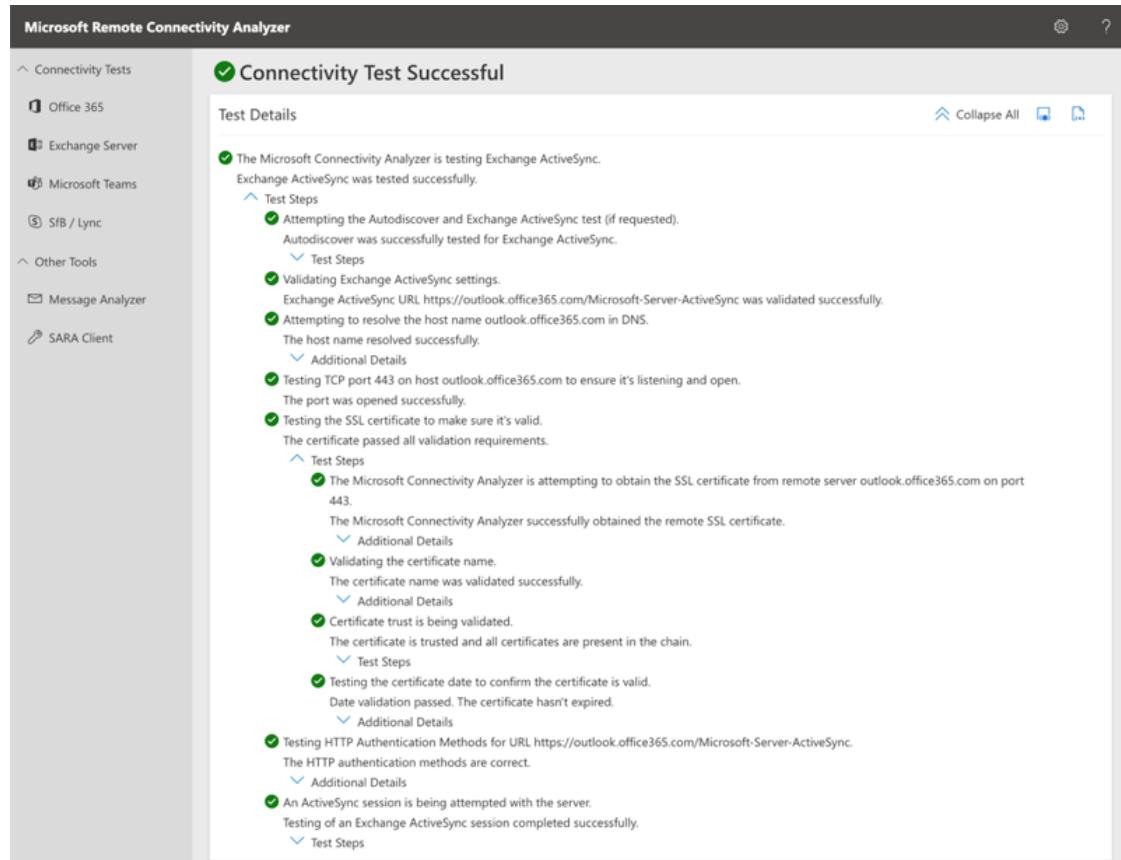


Figure 3-9: Running a test with the Microsoft Remote Connectivity Analyzer

On the Microsoft Teams tab, there's a separate set of tests:

- Teams DNS connectivity: this test checks for the presence and correctness of the DNS records needed for Teams connectivity.
- Teams sign-in: this test verifies that the client is able to sign in to the Teams service and get a valid authentication token.
- Teams Calendar Tab: this test verifies that the Teams service can connect to an Exchange mailbox.
- Teams PSTN Calling Dial Pad: tests whether the Teams PSTN calling system is properly configured for the user to enable them to dial PSTN calls.
- Teams Presence Based on Calendar Events: this test will check to see if Teams can read calendar items and use them to update Teams presence.
- Teams Exchange Integration: this test checks whether the Teams services can connect to Exchange mailboxes; you can run this against either on-premises or cloud mailboxes.
- Teams Meeting Delegation: this test checks whether a specified account has the right permissions to schedule Teams meetings on behalf of a delegate.
- Teams Meeting Recording: this test verifies whether the specified account has permission to record a meeting and store the resulting recording.
- Teams Channel Meeting: this test checks to see whether the specified account can schedule a Teams channel meeting.
- Teams Voicemail: use this test to verify that the selected account can retrieve and store voicemail messages.
- Teams Android Desk Phone Sign-In: tests whether the selected account is able to sign in using a Teams desk phone running Android. If you run this test using an account that has Global admin permissions, additional tests will be performed.

- Teams Room Sign-In: checks whether the selected account is able to sign in as a Teams Room account. This test requires the test account to have Global admin permissions.
- Teams Federation and Interoperability: tests the specified account to verify whether it is able to use federated chat with an external organization.

The analyzer's tests are very simple to use. In general, you'll supply an email address or DNS domain, provide a password if required, and run the test. RCA presents the results of each test in a clear, easy-to-understand format (Figure 3-9). In most cases, these tests alone will give you enough information to figure out the specific element of your network, DNS, or on-premises environment that's misconfigured and lead you to get it fixed.

Monitoring

Although Microsoft 365 removes much of the responsibility for ongoing support and maintenance for its applications away from administrators, the need still exists for tenants to know how well the services function and if any technical issues exist that might affect the availability or quality delivered by a service at any time. The Microsoft 365 admin center includes mechanisms to understand the current health of applications while third-party applications are also available to increase and improve the quality of monitoring. Service health and other important notifications are available in the left pane of the Microsoft 365 admin center, in the **Health** section.

The Service Status Page

Microsoft maintains a service status page at status.microsoft.cloud. This page currently lists three categories of status information: status of the Microsoft 365 admin center, status of the Power Platform admin center, and status of Microsoft Azure (certainly a broad item to cover!) Each category has links to the corresponding admin center; this page is clearly meant to be the place where you go when you suspect that one of the admin centers is broken or unavailable.

The Health Dashboard

The screenshot shows the Microsoft 365 Health Dashboard. At the top, there are navigation links for 'Home' and 'Health dashboard', and a 'Enable Dark mode' button. A message bar at the top indicates a recent WebKit update impact on SSO for Microsoft 365 services with a 'See Details' link and a close button. Below this, a section titled 'Service health and usage' displays the current health status of various Microsoft 365 services over the last 30 days. The table includes columns for 'Apps and services', 'Health', 'Unique active users', and 'Product usage'. Services listed include Exchange Online (2 advisories, 1 user, 7% usage), OneDrive (Healthy, 1 user, 7% usage), SharePoint (Healthy, 0 users, 0% usage), Microsoft Teams (3 advisories, 0 users, 0% usage), Yammer (Healthy, Not available, Not available), and Microsoft Forms (NEW, Healthy, Not available, Not available). At the bottom right, there are 'Help & support' and 'Give Feedback' buttons.

Apps and services	Health	Unique active users	Product usage
Exchange Online	2 advisories	1	7%
OneDrive	Healthy	1	7%
SharePoint	Healthy	0	0%
Microsoft Teams	3 advisories	0	0%
Yammer	Healthy	Not available	Not available
Microsoft Forms <small>NEW</small>	Healthy	Not available	Not available

Figure 3-10: Viewing the current Microsoft 365 status in the Health Dashboard

Remember that earlier I mentioned the ability to switch to the Health view from the top navigation section of the admin center. When you choose **Health** from that switcher or choose **Health > Dashboard** in the left rail of the Microsoft 365 admin center, you'll see a dashboard like that in Figure 3-10.

This is *not* the same as the Service Health Dashboard described in the next section, although it could potentially replace the SHD someday. For now, the Dashboard summarizes the overall state of your apps and services, shows infobars to indicate any issues that may need your immediate attention, lists recommended actions in case of problems, and shows you how many active users may be affected by any workload-specific advisories.

Service Health Dashboard

The **Service health** menu item under the **Health** section of the Microsoft 365 admin center takes you to the Service Health Dashboard (SHD). Microsoft uses the SHD to communicate the current health status for each of the services consumed by your tenant. Each service is displayed with an icon showing whether it is currently healthy, has an active incident that is causing an impact on customers (in other words, something is broken), or has a non-incident advisory. Advisories represent conditions Microsoft wants you to know about but aren't confirmed as active incidents, such as planned maintenance scheduled for different regions. Figure 3-11 shows how the SHD displays the current service state and any known problems.

The screenshot shows the Microsoft 365 Service Health Dashboard. At the top, there's a header with 'Home > Service health' on the left and 'Enable Dark mode' on the right. The date 'Aug 29, 2024, 2:25 PM CDT' is also at the top right. Below the header, there are tabs for 'Overview', 'Issue history', and 'Reported issues', with 'Overview' being the active tab. A note below the tabs says 'View the issues and health status of all services that are available with your current subscriptions. Learn more about Service Health'. There are buttons for 'Report an issue' and 'Customize' on the left, and 'Change view' on the right. The main area is titled 'Active Issues Microsoft is working on' and contains a table of incidents. The table columns are 'Issue title', 'Issue type', 'Affected service', 'Updated', and 'ID'. The table rows list various issues, mostly categorized as 'Advisory'. Below this, there's a 'Service status' section with a table showing the status of different Microsoft services. The services listed include Microsoft 365 apps, Microsoft 365 suite, Microsoft Defender for Cloud Apps, Microsoft Intune, Microsoft Teams, Microsoft Viva, and OneDrive for Business. Each service row shows the number of advisories. At the bottom right of the dashboard are two buttons: 'Help & support' and 'Give Feedback'.

Issue title	Issue type	Affected service	Updated	ID
Some users on version 128 of the Microsoft Edge browser may not be able to load the start page at launch	Advisory	Microsoft 365 suite	Aug 29, 2024, 2:18 PM CDT	MO877207
Some users may be unable to edit some SharePoint Online classic site pages	Advisory	SharePoint Online	Aug 29, 2024, 12:53 PM CDT	SP861751
Users may not receive app protection policies applied for apps that rely on specific policies	Advisory	Microsoft Intune	Aug 28, 2024, 5:27 PM CDT	IT82136
Users may hear an echo if embedded audio is enabled when using PowerPoint Live in the new Microsoft Teams	Advisory	Microsoft 365 apps, Microsoft 365 suite, Microsoft Teams	Aug 28, 2024, 4:54 PM CDT	MO752474
Some users may not receive the "Password encrypted file" label for password-protected files	Advisory	Microsoft Defender for Cloud Apps	Aug 28, 2024, 9:22 AM CDT	C5872233
Users may be unable to promote SharePoint Online sites using the Promote feature in Microsoft Viva Engage	Advisory	Microsoft Viva	Aug 26, 2024, 2:52 PM CDT	MV873555
Some users may incorrectly receive a security warning when opening Excel or PowerPoint files in SharePoint Online	Advisory	SharePoint Online	Aug 26, 2024, 12:28 PM CDT	SP867513
Some users may incorrectly receive a security warning when opening Excel or PowerPoint files in OneDrive for Business	Advisory	OneDrive for Business	Aug 26, 2024, 12:27 PM CDT	OD867515
Users may be unable to import PST files using Drive Shipping in any Microsoft 365 service	Advisory	Microsoft 365 suite	Aug 16, 2024, 4:53 AM CDT	MO805029

Service	Status
Microsoft 365 apps	1 advisory
Microsoft 365 suite	3 advisories
Microsoft Defender for Cloud Apps	1 advisory
Microsoft Intune	1 advisory
Microsoft Teams	1 advisory
Microsoft Viva	1 advisory
OneDrive for Business	1 advisory

Figure 3-11: Viewing the list of current incidents in the Service Health Dashboard

Using the **Customize** button, you can customize the SHD to only tell you about the state of services you care about. You can control this in two ways: what you see in the SHD, and what items Microsoft sends you email notifications about. For instance, if you don't use Intune, it's unlikely that you will care about knowing when Intune has an outage. You should check the customization settings every so often, as Microsoft occasionally adds new workloads and features to the set of SHD items.

Clicking on an incident displays extra information, including ongoing details of the investigation for an incident, which may span multiple messages posted by Microsoft over a period. After Microsoft resolves an incident, they often inform customers what happened in more detail through the publication of a post-incident review (PIR). Microsoft uses Azure-based machine translation to translate advisories; if you enable this feature and then use the admin center in a language other than English, the service will try to translate the incident title, user impact, and incident history.

Sometimes the SHD alerts administrators about issues that require some sort of action. An example might be that you have a certificate that's about to expire. Issues that require administrative intervention are in the "Issues in your environment that require action" section and, as the name implies, aren't problems with the service... but they will turn into problems if you don't take the required action to resolve them. The service sends notification emails when new issues are detected that pertain to your environment. Individual administrators can turn this behavior off as described below. Microsoft will probably continue to roll out new features to detect environmental issues over time, so you should make checking this item a regular part of your work.

Because of the sheer scale of the service, you can expect that some outages are happening *somewhere* in the service at any given point in time. The SHD is a view of problems determined by Microsoft as potentially affecting your tenant, rather than every single issue impacting any tenant across the service. It is also possible that your tenant experiences an issue that the SHD does not show. With that said, it is common to experience problems with the service that affect your users or your entire tenant without seeing it in the SHD.

Microsoft's automated monitoring systems are sometimes slow to detect a problem. In some cases, multiple customers need to report issues and escalate the issues beyond level 1 support teams before Microsoft accepts the issues as confirmed incidents. At that point, Microsoft might add details of the incident to the SHD. Furthermore, you might be experiencing an issue with your tenant that is due to a misconfiguration on your part, not a service fault. For example, if you misconfigure your DNS records and your Exchange Online recipients stop receiving emails, that is not something that the SHD will alert you to because it is not a fault with the service itself. Regardless of any limitations or issues with the timeliness of information, the SHD is a useful resource for administrators.

Microsoft continues to develop the capabilities and intelligence behind the SHD. For example, when logging a new service request the portal tries to proactively inform you of known issues, as well as notifying you when Microsoft detects actions by your users that may lead to a support request such as clients connecting with out-of-date versions of Outlook. Microsoft also uses telemetry data and machine learning to detect issues, to reduce the amount of time between an incident occurring and the first notification posted to the SHD. There is also a feedback mechanism built into the SHD so that customers can rate the accuracy and usefulness of the information that Microsoft communicates to them.

Reporting an Issue

You can use the button labeled "Report an issue" at the top of the SHD to register a problem with services such as Exchange Online, SharePoint Online, and Teams. Microsoft says that these reports are correlated with other telemetry data and used to trigger internal investigation (and presumably verification) of potential problems so they can decide which ones are serious enough to pass on to the engineering team and treat as "incidents," the formal name for service problems that require investigation and repair. It remains to be seen how useful this feature will be either for tenant administrators or Microsoft; the risk of false alarms seems high, so the prudent course (which Microsoft also recommends) is to continue to file support tickets in addition to using "Report an Issue."

Highlighting Incident Notifications in Outlook

The idea behind incident notifications is simple: when you have Outlook for Windows open for an account that has Microsoft 365 global administrative privileges, the service will post notifications in a new admin notifications pane to tell you about potential problems in your tenant. You might be excused for not having known about this feature before for a simple reason: good security practice dictates that you don't use your normal work account—you know, the one you're probably running Outlook against—for administrative tasks. If you've followed the normal best practice of assigning separate accounts for your global administrator role holders to use for day-to-day work, you may never see these notifications. Now that you know this feature exists, it might be worth testing it with your global admin accounts to see if you find it worthwhile. You can control visibility of these notifications with the **Help > Admin notifications** option in Outlook for Windows (subscription version).

Getting Incident Notifications via Email

Tenants can opt to receive email notifications of incidents. Even though this capability lags far behind the monitoring notifications provided by third-party products, it's still good to have. If you want to receive email notifications, enable them by going to the SHD and clicking the **Customize** icon, then choosing Email, then checking the "Send me email notifications for service health incidents" checkbox. Settings changes may take up to 8 hours to take effect, and of course, when you don't receive an email announcing an outage, it may mean that there *is* no outage, or that one is happening but that it affects mail flow to your specified recipients in some way.

Receiving Updates for Active Incidents

When you open an individual incident notification, you may notice a link labeled "Manage notifications for this issue." You can use it to specify up to two email addresses that Microsoft will use to send updates on that specific incident, including any status changes or resolution information. This isn't quite the same as the "Send me email notification for service health incidents" checkbox mentioned above—the "Manage notifications" link will send you updates only for the specific incidents where you've enabled it.

Programmable Access to Service Incident Information

Microsoft offers the [Microsoft Graph-Service Health and Communications API](#) to provide programmatic access to:

- Notification messages for service updates posted to the Message Center.
- Incident and advisory messages posted to the Service Health dashboard.
- Overview of current workload status.
- Historical incident information.

If you're curious, this [PowerShell script](#) is an example of how to fetch the same set of messages displayed in the Message Center from the API and process them into a form that can be consumed in different ways, such as posting to a Teams channel, export to Power BI, or formatted in an HTML page.

Other Sources of Service Information

Besides the global status page at <https://status.cloud.microsoft>, users have access to a simple end-user-facing status page at <https://portal.office.com/servicestatus>, although it's not much use for identifying issues. You may also find [the Azure status page](#) useful.

Message Center

The Microsoft 365 admin center dashboard also includes a view of the most recent messages from the Message center. The various product and service operations teams use the Message center to notify customers of changes such as updated features and user interfaces, as well as changes that may interrupt

service such as IP address range changes. Items shown in the Message Center are supposed to be specific to a tenant rather than the more general view of what is changing found in the roadmap.

To make sure that you don't miss anything important, you should access the Microsoft 365 **Message Center** from time to time to review the notifications posted there (Figure 3-12). If you find something interesting in the notices, you can select **Share** to send the notice to someone else via email and include a personal message to add some context about the change. The email includes the complete text of the update notice. Microsoft added tags to notifications, along with controls to let you filter by tags, the services affected, or the state of the notifications. Tags include "Major Update," "Admin Impact," "New Feature," "Data Privacy," and "User Impact." These tag names are self-explanatory, but they are nonetheless useful to help you filter and sort through the steady river of notifications issued by the service.

The screenshot shows the Microsoft 365 admin center interface with the 'Message center' page selected. At the top, there's a navigation bar with icons for Home, Search, and various settings. Below the navigation is a breadcrumb trail: Home > Message center. On the right side of the header, there are links for 'Enable Dark mode' and a user profile. The main content area is titled 'Message center' and includes a brief description: 'Each message gives you a high-level overview of a planned change and how it may affect your users, and links out to more detailed information to help you prepare.' Below this, there are two tabs: 'Inbox' (selected) and 'Archive'. A search bar shows '621 items' and a 'Search' button. Underneath, there are filters: Service, Tag, Message state, Relevance, Status for your org, and Platform. The main area displays a list of 10 notifications:

Service	Last updated	Act by	Relevance	Status for your org
Microsoft Copilot (Microsoft 365)	29 Aug 2024		Medium	
Exchange Online, Microsoft 365 Apps, Microsoft 365 for the web	29 Aug 2024		High	
Microsoft Teams	29 Aug 2024		Medium	
SharePoint Online	29 Aug 2024		High	
Windows	29 Aug 2024		Medium	
Windows	29 Aug 2024		Medium	
Microsoft Power Automate	29 Aug 2024		Medium	

Figure 3-12: Message Center notifications about functionality updates

Message center notifications show the affected workloads, and the number of affected users per workload, in some Message Center notifications. This data helps administrators to prioritize handling of those changes. Microsoft consolidates or separates notifications for different workloads from time to time; for example, in September 2024 they began bundling all Azure Information Protection-related notifications into the "Microsoft Purview" category.

The "Relevance" column attempts to rate each new MC post by how relevant it is to your specific tenant, based on user and admin activity, what features and licenses you have deployed, and other factors. The "Status for your org" column shows whether a change has been announced ("Scheduled"), partially deployed to your tenant ("Rolling out"), or completely deployed to your tenant ("Launched"). Updates for services you don't have licenses (or active users) for will have a blank value in this column.

As described in the Planner chapter, you can also have Message Center notifications synchronized to Planner, so you can track every change and make sure that any change which might impact your organization is assigned to the appropriate people for action.

Major Updates

The **Major updates** tag in Message Center features major changes to a service. Microsoft posts these updates at least 30 days before they come into effect. To decide whether a change falls into this category, Microsoft considers how the change might affect users and the tenant with questions such as:

- Does the change affect **the way people work daily**? For example, the introduction of the Focused Inbox changed the way that people deal with new emails. Changes to meetings, delegations, and sharing and access control are also in the "daily productivity" bucket.
- Does the change affect **how the tenant customizes the service**? For example, if Microsoft changes a theme or web part, it might affect how pages render and overwrite a change made by the tenant.
- Does the change **increase or decrease capacity**? A good example is when Microsoft changed the default storage quota for mailboxes (for enterprise plans) to 100 GB. Another example is the change in how OneDrive for Business manages storage quota.
- Does the change affect **what users see**? Any change that might affect the ability of a help desk to support users or change how users access functionality is a major update. A minor branding change such as the replacement of "Office 365" with "Microsoft 365" for the Admin Center is not in this category but forcing people to use content searches instead of workload-specific searches is. Changing a URL used by a feature also falls into this category.
- Does the change introduce **a new service or application**? Microsoft needs to tell tenants when they launch a new application like To-Do or Teams.
- Does the change **require administrative action**?
- Does the change involve **the storage location for data**? Often, applications launch with storage in the U.S. As the roll-out proceeds across the world, storage moves into other data center regions. Customers need to be told where their data is stored, such as when Teams moved its data services into the U.K. or India data center regions.

Once you see a notice about a major forthcoming change, it's a good idea to search for more information such as the blogs written up by people who have tested the change or already have the change in production in their tenant. Independent information added to Microsoft formal documentation creates a more complete picture of what you can expect to see happen in your tenant.

Message Center Preferences

Despite Microsoft's efforts to improve the relevance of Message center items, some of the messages appearing in your tenant's Message center might not be directly relevant to you. For instance, if you do not use Office 365 Mobile Device Management, you are probably uninterested in any of those messages. You can filter the messages you see by clicking the **Preferences** link and selecting the services you want to know about.

Message center preferences include the choice to have Microsoft send you a weekly email digest of new messages. Even if it is not a substitute for keeping your eyes open and looking out for information about developments inside the service, the weekly digest is a practical way to stay updated with Microsoft announcements. By default, Microsoft has historically sent the weekly digest to the global administrator for the tenant and addresses the note to both the primary and backup email addresses for that account. A third address is also available for use as the tenant wishes. You can use this address to send copies of the mail digest to a distribution list, a Microsoft 365 Group, or to a team channel for other people to learn about

changes. If you do not wish to receive the mail digest, uncheck the boxes for one or more of the addresses and save your preferences. Users who are granted an admin role will get the digest for four weeks as a trial.

Users holding specific administrative roles can also receive update notifications. Originally, only global administrators could see Message Center messages, but as of now users who hold roles such as Teams administrator or Exchange administrator receive messages (which they can opt-out of) for the workloads they manage.

Automatic Translation

Update messages are composed in English. Administrators who use non-English languages can have the Microsoft 365 admin center translate messages to another language by selecting their preferred language through the admin center settings (cogwheel). If some difficulty occurs in understanding the translated version of a message, you can choose to view the message in English selecting English from the drop-down list of available languages. This is a dynamic choice that reverts to the language selected in settings when you navigate away from the Message Center.

Network Connectivity Health Monitoring

It makes sense that Microsoft would know a great deal about network connectivity health at the service level, and they're making a subset of what they know visible in the admin center. The **Network connectivity** link under the **Health** section in the left navigation bar shows you data from client-side telemetry to illustrate the performance and quality of your sites' connectivity to the Microsoft network. Microsoft collects these data in four ways:

1. Enable Windows Location Services (WLS) on at least two machines in each location that are running Windows OneDrive clients (provided you have version 19.232 or later). When you do this, all the OneDrive clients in your domain will aggregate to the same metro area—that is, if you have 50 computers in Huntsville, they will appear as a single location at the city level. Microsoft also rounds location information obtained from WLS to the nearest 300-square-meter grid square.
2. Use the Locations tab to define a list of locations and corresponding public IP addresses; Microsoft will group clients whose service traffic enters their network from this public IP as "belonging" to that location.
3. Have users run the [Microsoft 365 network connectivity test](#) manually.
4. Have users run the Office Support and Recovery Assistant (SaRA) manually, as described in the clients chapter.

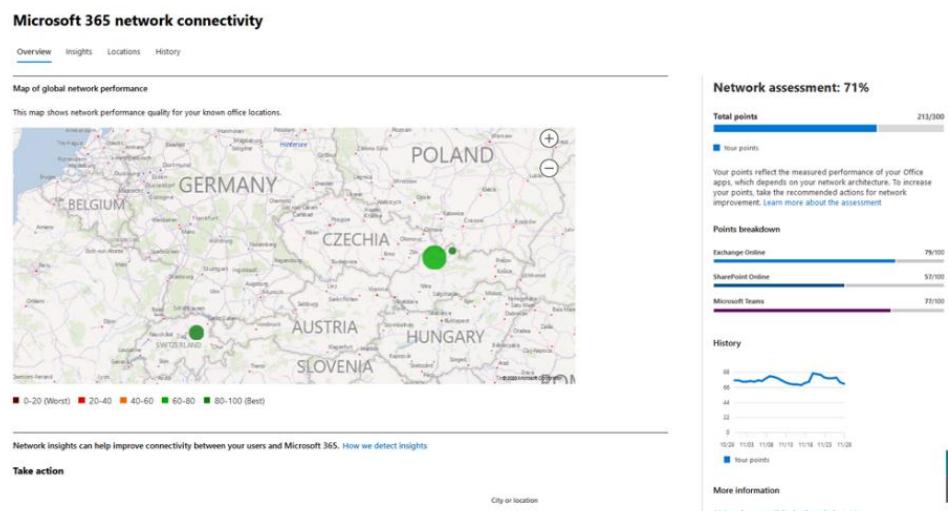


Figure 3-13: The network connectivity view shows you what Microsoft knows about your network quality

The resulting data is presented as a performance map and a series of scores, along with a list of recommendations, as shown in Figure 3-13. Microsoft has plans to continue enhancing this connectivity map by ingesting more telemetry signals from clients and refining the machine learning models that are used to produce insights and recommendations. This is exactly the type of application for which “big data” gathered at a very large scale can provide interesting results; the larger the number of clients that report for any given area, the more resolution Microsoft has for identifying potential network problems.

Workload-Level Health Monitoring

Exchange Online and Google Gmail together delivered the practical reality of email as a utility service that “just works.” With that said, sometimes email and other cloud services *don’t* “just work,” so demand thrives for solutions to help administrators get early warning, and better insight into, problems that affect email routing and delivery. The huge wealth of telemetry that Microsoft gathers throughout the service is mostly reserved for internal use; it wouldn’t do you any good to know the temperature of an individual disk sitting somewhere in an Exchange server pod anyway. However, Microsoft is slowly moving to provide first-party tools to help answer the most common concerns service administrators have: is there a problem? If so, is it *my* problem or *Microsoft’s* problem? And what do I do about it?

[Exchange Online health monitoring](#) was the first monitored workload, and monitoring has expanded over time to [cover Teams and Microsoft 365 apps](#). To use these monitoring features, you must have at least 5,000 licenses of Microsoft 365 or Office 365 E3 or E5 licenses, and at least 50 of those users must be regularly active monthly.

If your tenant meets these criteria, you’ll see health data shown on the **Health > Service health** page. The data collected by the service includes a list of advisories or incidents, plus links to show specific scenario-based data that may help identify problems in one of three categories: problems with the service itself (labeled as “Infrastructure” by Microsoft), problems with third-party network connectivity, and problems with your infrastructure (labeled as “Your org”).

Right now, Exchange Online has the most health monitoring data available. You can see rolling 30-minute counts of the number of users who have logged in (using either basic or Modern Authentication), the number of messages delivered without delay (the time count starts from when the service receives the message), and the number of active users. This last metric deserves a bit more explanation: Microsoft counts an active user as one who has read at least one email using a supported client (all versions of Outlook, plus the native iOS and Android mail clients). A user who sends mail, syncs mobile device folders without reading anything, creates a task item, etc. won’t be counted as active. This leads to the unfortunate possibility that at times when you’d normally have low message reading activity, you might find that the health monitoring system doesn’t indicate a problem.

In addition to these Exchange Online metrics, you may see service advisories for specific operations, including [mailboxes that are nearing their quota](#). The content of these advisories are specific to their operations; for example, the auto-expanding archive advisories tell you when individual mailboxes are close to the 1.5 TB size limit for auto-expanding archives. The set of service advisories may change over time.

Besides the Exchange Online content, you’ll see additional data for Teams, the Microsoft 365 desktop apps, and Microsoft 365 web apps. Whereas the Exchange Online dashboards show health indications (along with the you-or-Microsoft indicator of whose problem it is to solve), these other dashboards focus more on metrics. For example, the Teams dashboard shows you how often the Teams client was launched or how many chat messages were sent in the preceding 30 minutes, but it’s up to you to correlate this with any reports of problems you see online or receive from users.

For now, there are no real alerting or notification capabilities built into this dashboard. As a place to check when you suspect that there might be a problem, this is a useful tool, but as a means of getting early warning of a newly emerging problem, it will require some refinement to be useful since you won't get a proactive notification.

Health Monitoring for Priority Users

In addition to the overall tenant health monitoring features, you can see health information for [priority accounts](#). You can tag users as VIPs by adding them through the **Users > Active users** view, or by adding them in the **Setup > Organizational knowledge** view. If you'd rather use PowerShell, you can call the `Set-User` cmdlet with the `-Vip` flag, like this:

```
Set-User Tony.Redmond -Vip:$true
```

Once you designate an account as a priority user, you'll see some additional health monitoring data, plus the ability to generate alerts when a priority user's account has mail flow problems. You can designate any licensed user as a priority user.

If you have assigned an account a Microsoft Defender for Office 365 Plan 2 license, you can also benefit from a feature Microsoft calls "priority account protection." This is essentially a set of additional quarantine reports and filtering options that let you more easily sift through and deal with quarantined messages sent to your priority users. For example, alerts on accounts that are marked as priority accounts display a unique tag in the alert list.

Better Network Connectivity with Informed Routing

Microsoft gathers a cornucopia of network performance data across the service that it uses to tune its internal networks and to present the data described in the preceding section. They've been working on an additional use for this data, too: using it as a feedback mechanism to help you tune *your* network. If you're using a supported software-defined wide area network (SD-WAN) solution, a feature called [informed network routing](#) allows your on-premises SD-WAN equipment to read network data coming *from* the service. The basic idea behind informed network routing is that the service (especially the front doors you connect to) can provide real-time feedback on the performance and reliability of your connections to the service, and your SD-WAN can reconfigure itself as needed to optimize traffic flow to the service. It's a fascinating idea, but as of October 2024 it only works with a single vendor's SD-WAN solution. As Microsoft expands the scope of what this feature can do, it will be interesting to see how much practical value it provides for organizations that are comfortable allowing performance metrics from a single service to drive their network configuration with minimal human intervention.

Monitoring Systems

As with many Microsoft products, there is a [System Center Management Pack for Microsoft 365](#). Organizations that are running System Center Operations Manager (SCOM) can create alerts and monitoring dashboards for the health of their tenant. Tenants who do not use SCOM implementation can consider a solution based on the various Microsoft Graph APIs available for monitoring and management. You can develop your scripts or software solutions based on the information available through the API or invest in a third-party monitoring solution that can do it for you. Examples of third-party monitoring products include MessageOps Monitor, Analyzer for Office 365, and 365 Command by Kaseya.

Monitoring Software Update Status

Like nearly every other software vendor, Microsoft places great emphasis on regularly releasing updates to address software functionality and security flaws. Microsoft, Quest Software, and numerous other companies

make solutions to monitor, plan, schedule, and enforce the deployment of updates, but most enterprise customers are essentially allowing clients to download their own updates. We discuss the distribution and control mechanisms for Microsoft 365 Apps updates in the clients chapter; you're probably familiar (as a user if not an admin) with the Windows Update mechanism for delivering updates to computers running Windows. To make update management a little easier, Microsoft includes a new, and fairly rudimentary, page in the Microsoft 365 admin center (**Health > Software updates**) that shows you information about the state of Microsoft 365 Apps and Windows updates for managed machines in your tenant. This report is available directly at [this link](#).

The report will show you three things, based on devices that are running Windows and have Microsoft 365 Apps installed using a license that belongs to your tenant:

- How many devices have the most recent security updates.
- How many devices are missing one set of security updates.
- How many devices are missing two or more sets of security updates.

However, it won't show you *which* devices are missing *which* updates—for that, you'll need to use the Microsoft 365 Apps admin center described in the clients chapter. If you don't see any data here at all, that probably means that you haven't enabled [diagnostic data collection](#), which is where the service gets this information.

Service Requests

Service requests are problem reports filed with Microsoft, although you are almost certainly going to be working with third-party support engineers under contract with Microsoft rather than blue-badged Microsoft employees. [Telephone support](#) is also available if urgent problems occur. Because a lot of configuration and other information will need to be given to support engineers, it is logical that calls should be made only by users with administrative access to the tenant.

When you submit a service request, it is routed to a Microsoft support center covering the Microsoft 365 region for the tenant. The support request is examined by a support engineer who will probably call the tenant administrator to discuss the reported problem and to look for added information to help diagnose its cause. Because of the scale of the worldwide service, Microsoft follows a carefully structured approach to gathering and checking facts about service requests. At times, it can be frustrating for a tenant administrator when a support agent asks them what appears to be much the same question several times or to be asked to test components that are known to be failing, but it is all part of the process. Eventually, the problem will either be solved or escalated to second-level support (this can take several days) and, if necessary, to the product group that supports the workload where the problem exists. Remember, support engineers cannot make changes to code or to how the service works as this kind of intervention can only happen through a process controlled by the product group. Microsoft is rightly cautious about making changes because a small change made for the benefit of a single tenant might have a ripple effect elsewhere within the service that impacts multiple tenants. In general, support engineers can only access tenant data when you allow them to do so. The need to preserve customer confidentiality and privacy is paramount, even if this slows things down at times. You should mentally prepare yourself to be asked to look up and provide data that you might think the service engineers should already have access to.

Naturally, before you add a new service request, it is a good idea to do some troubleshooting of your own as you might discover the answer much faster than through the Microsoft support process. Use your favorite search engine to check for obvious solutions and, if nothing turns up, try asking a question in a community forum such as [Microsoft Q&A](#) (the allegedly-official support site) or the [Microsoft Technical Community](#). Don't be lazy and expect someone else to do the work to solve your problem. Always take the time to investigate and share information in your requests to prove that you have done some troubleshooting for

the problem and the results of your investigation. People in support forums generally want to help, but only if you are prepared to help yourself first. Even if the support forums do not help, the information you gather in your investigation will give invaluable background to the Microsoft support engineers who work on the service request.

Creating a New Service Request

To add a new service request, click **Support** and then **Help & support** from the Microsoft 365 admin center. You'll then go through a three-step process.

In the first step, you enter a few search terms, and the admin center will suggest some potentially helpful articles. Microsoft's intent here is to get you to solve your problem, whenever possible, using the search results instead of opening a support case. Microsoft uses a mixture of machine learning and telemetry that they have for your tenant, and searches against their support databases to find potential solutions based on the text you enter. As is typical of Microsoft search technologies, the quality of results here may vary widely. If you don't find any relevant or useful results, you can click the **Contact support** link to go to the second step.

In step two, you give some details about the problem you need help with. You'll need to specify who should be contacted, their email address and phone number, and whether you prefer an email or phone response. You can also specify a preferred language.

When you click the **Contact me** button, your request will be queued for action. The wait time for a response is usually quite short, but it will depend on the number of cases that the support representatives are dealing with. IT professionals love to complain when they have been let down by a poor support experience, so you will always find stories of very long waits for a call back from Microsoft. If the delay for a call back is too great a risk for your organization, you should consider a Premier Support contract to get faster support. You can request a specific callback time, which will help reduce the frustration inherent in playing phone tag with support engineers, and if you specify your time zone, they might even honor it (hopefully avoiding late-night phone calls).

When you send a support request, if the phone number or email address you supply isn't listed in your organization profile, Microsoft will send a unique PIN to the registered email addresses that *are* in the support profile. This helps reduce the risk of spoofing but means that, if you're not watching for the PIN, your support case may languish until you've supplied it. Microsoft recommends making sure that customers update their profile email and phone details to avoid this problem. On November 1, 2023, they started enforcing this requirement for all administrators, so you can no longer open new support requests without supplying the PIN.

You can add attachments such as screenshots or network traces to support requests; these, along with the contents of the problem description field, are the only real ways that your assigned support engineer will have to learn about the problem before you talk to them. Be sure to be clear and descriptive.

When Microsoft receives a service request, they assign it a service request identifier such as 10312033. You should give this identifier to Microsoft whenever you communicate with the support team, as it allows them to track the progress of a service request through Microsoft's support and escalation systems. You should also receive a message from the support engineer assigned to the service request. The subject of this message has some tracking information to capture the interaction between support staff and tenant administrators in Microsoft's support databases. To keep a record of the case as it unfolds, reply to the message whenever you have something to add or want to request an update. It is a good idea for you to keep your record of interactions with Microsoft just in case this data is necessary to prove that a problem hasn't received enough or timely attention.

The details that you add to a service request can be extraordinarily useful to the support engineer assigned to handle the case. You should give information such as:

- Detailed steps to reproduce the problem. If the problem surfaces in different ways, include steps for each way that you know to reproduce the issue.
- Is the problem still evident after you sign out and sign back into Microsoft 365? An expired token can cause a failure to connect to a service, so it's important to check that the account with the problem is authenticated.
- Scoping information for the problem's impact. Does it affect one user, all users, or something in between? Are all the affected users in the same geographic region?
- If the problem occurs only in one location, is there something special about how users connect to the service or the Internet from that location?
- Has anything changed recently? For example, have you made any configuration changes that might be related to the problem?
- Did this functionality ever work, or did it stop working at some point?
- Screenshots showing any error messages that are visible to users.
- PowerShell commands and the output from those commands to help support engineers to understand the problem.
- Background information such as the version number of clients (including browsers) that are affected by the issue. Make sure that you use a browser supported by Microsoft 365 and try to replicate the problem on different browsers to narrow the conditions under which the problem appears. For instance, the Edge and Chrome browsers can behave differently from the Brave Browser. Does the problem occur with all browsers or just a specific browser? Can it be reproduced on multiple workstations or just one that is running a certain version/build of an operating system? Does the problem happen if you open a private or incognito browsing session?
- If the problem affects a hybrid component, details of the hybrid connection and other associated components such as how directory synchronization is performed and whether single sign-on is used.

Just like in any support system, the various kinds of problems that can occur need different periods to resolve. Some issues might never be resolved because they need substantial engineering investment that Microsoft considers unjustified or unnecessary. Microsoft should resolve straightforward problems in a day or so, but to be brutally honest, as the service grows, any problem that can't be addressed by a simple troubleshooting script is likely to linger. It's very difficult to attract and retain good support engineers, and Microsoft has struggled with doing so over the last few years. Problems that need engineering intervention or more detailed diagnostic data, or that are simply complex, will need more time. Microsoft is usually good at keeping tenant administrators up to date with the progress of service requests through email. Updates are posted to the service request and are visible through the Microsoft 365 admin center. And if things go quiet, you can always email the assigned engineer to ask for an update.

Gathering Tenant Information

While you work through a service request with Microsoft, you might be asked to give some information about your tenant, usually to allow the support engineer to understand what version of the software the tenant is running. Remember that a tenant can choose to use software released to the Targeted Release or Standard Release rings or a mixture of both. Even within these rings, Microsoft deploys software at different intervals to reach every tenant in all regions. It is impossible to deploy new software to everyone at the same time, so it is important to know what configuration is active within a tenant when you meet a problem.

The Microsoft 365 admin center doesn't provide a built-in way to gather and report tenant configuration, so you must use PowerShell for this purpose. Two cmdlets are especially important. The *Get-OrganizationConfig* cmdlet returns information about Exchange Online and some generic tenant data while *Get-SPOTenant*

returns information about SharePoint Online. You will find examples of *Get-OrganizationConfig* in use for different purposes in other chapters, but we will concentrate on its use to report tenant data here. The information reported by the cmdlet changes over time and is difficult to review on-screen. It is usually best to dump the output to a text file and review it with an editor, which will also make it possible to extract information to share with Microsoft support. In the following example, the first command lists several important settings that might be of interest when troubleshooting a support case while the second redirects the output to a text file.

Get-OrganizationConfig

```
Name : office365itpros.onmicrosoft.com
ObjectVersion : 16500
ReleaseTrack : FirstRelease
SharePointUrl : https://office365itpros.sharepoint.com/
MapIHttpEnabled : False
IsLicensingEnforced : True
IsTenantAccessBlocked : False
IsTenantInGracePeriod : False
RBACConfigurationVersion : 0.1 (15.20.218.12)
AdminDisplayVersion : 0.20 (15.20.218.12)
ServicePlan : BPOS_S_E15_0
```

Get-OrganizationConfig > Config.txt

For instance, settings such as the *RBACConfigurationVersion* and *AdminDisplayVersion* will tell engineers what version of the software runs inside the tenant. The *ReleaseTrack* setting shows if the tenant uses Targeted Release for all or some users, while the *ServicePlan* setting shows the basic plan configured for the tenant.

SharePoint Online does not report as much configuration data for a tenant as Exchange Online does, but the devil might be in the detail when engineers are debugging a problem. Here is what the *Get-SPOTenant* cmdlet reveals:

Get-SPOTenant

```
StorageQuota : 44032
StorageQuotaAllocated : 20174
ResourceQuota : 10900
ResourceQuotaAllocated : 1900
CompatibilityRange : 15,15
ExternalServicesEnabled : True
NoAccessRedirectUrl :
SharingCapability : ExternalUserSharingOnly
DisplayStartASiteOption : True
StartASiteFormUrl :
ShowEveryoneClaim : True
ShowAllUsersClaim : True
OfficeClientADALDisabled : False
ShowEveryoneExceptExternalUsersClaim : True
SearchResolveExactEmailOrUPN : False
RequireAcceptingAccountMatchInvitedAccount : False
ProvisionSharedWithEveryoneFolder : False
SignInAccelerationDomain :
```

Sometimes, you might be asked for the tenant identifier. This is a unique value for the tenant used in different places by Microsoft 365 and Entra ID. One way to retrieve the identifier is to use the *Get-MgOrganization* cmdlets. This example uses *Get-MgOrganization*:

Get-MgOrganization | Format-List Id, DisplayName

ObjectId	DisplayName
-----	-----

a662313f-14fc-43a2-9b7a-d2e27f4f3478 Office 365 for IT Pros

The *ObjectID* reported by the cmdlet is the tenant identifier. This is important information to have because it's the unique value used by Microsoft 365 to identify the tenant. You'll need to know this information if you ever want to sign up for a Microsoft beta program.

Alternatively, input your tenant domain name into this [website](#) to retrieve the identifier. The site uses information published on the internet to allow OAuth 2.0 sign-ins to function to report the tenant identifier.

Customer Lockbox

When Microsoft support personnel are working on an issue for you, they may need access to some user data to resolve the problem. These situations are rare, as most of the support operations performed by Microsoft are automated. Where possible, any support tasks performed by support engineers are isolated from customer data. However, there will always be some cases, such as when Microsoft support is trying to help a customer with problems with mailbox contents, that access to the user data is necessary.

Customer Lockbox is an extension of Microsoft's Lockbox system for managing "just in time" access to the service infrastructure by support staff. Multiple levels of authorization are required before support staff can gain access. Upon approval, the support engineers receive access limited in scope and duration to the minimum needed for the task. Lockbox also includes comprehensive audit logging of any activities performed by support staff.

Under normal circumstances, support engineers receive approval from a Microsoft manager to access customer data. When a tenant enables the customer lockbox feature, an added approval by the customer is necessary before Microsoft support can access user data (this requirement does not cover access to system data such as logs). Microsoft sends the Customer Lockbox request as an email notification which administrators or users with the customer lockbox approver role can approve or deny in the **Support** section of the Microsoft 365 admin center. Access requests have a time limit (12 hours by default), and a scheduled cleanup task removes the support personnel's access automatically upon resolution of the issue or when the time expires.

Actions performed by Microsoft support or by the automated systems used in the service are captured in the audit log for the tenant. Like any other audit log records, they are accessible using PowerShell or APIs to allow third-party security monitoring systems to extract and include data in reports and dashboards.

To enable Lockbox for a user, the user must have an Enterprise E5 license or the Advanced Compliance license. Lockbox is generally available in all supported workloads.

Protecting Data with Encryption

Encryption is a complicated subject. The legal, technical, operational, and business implications of where, when, and how data are encrypted could easily fill a series of books. Microsoft uses two primary strategies for encrypting data: some data are encrypted in transit, and some are encrypted while at rest.

In general, encryption works best when it is automatic and ubiquitous, and Microsoft has done pretty well at building ubiquitous transport and at-rest encryption into the service (as [detailed here](#)). For example, by default, all communications to and from the service are protected with TLS, and servers running the Microsoft 365 applications all use BitLocker to protect their physical disks. However, Microsoft offers several additional [encryption services](#) that may be of use to you. For example, you can require the use of mobile-device encryption on Android and iOS or iPadOS devices through Intune, and you can create conditional access policies that only allow encrypted devices to connect to various services. If you have the infrastructure for it, you can enable or require the use of S/MIME for messages, and so on. Keep in mind that not every

encryption feature is globally available; Microsoft 365 tenants in particular regions or government-associated clouds may not have the same features as commercial tenants.

Service Encryption

The basic level of data-at-rest encryption provided in Microsoft 365 is called [service encryption](#). Along with the Windows-standard BitLocker tool, Microsoft has built a tool called [Distributed Key Manager](#) to ensure that the BitLocker recovery keys are protected and secured. Microsoft [describes DKM's function](#) by saying:

"Only members of a specific security group in Active Directory Domain Services can access those keys to decrypt the data that is encrypted by DKM. In Exchange Online, only certain service accounts under which the Exchange processes run are part of that security group. As part of standard operating procedure in the data center, no human is given credentials that are part of this security group and therefore no human has access to the keys that can decrypt these secrets."

The good news is that, even if you never change any default settings, every file and message stored by the service will be encrypted by Microsoft using the BitLocker and DKM combination.

Customer Key

One of the longest-running arguments in the encryption world is "who holds the key?" As you might imagine, some organizations want to retain complete control over the use of encryption in their enterprise. This is usually for one (or both) of two reasons: they either don't want encryption used by an attacker to lock up data or they don't trust a third-party service provider (which in this case would include Microsoft) not to peek at their data. One solution to this is to encrypt data using a key that only the customer has access to. Microsoft offers a capability known as [Customer Key](#) (CK) that allows you to hold the root keys used by the service encryption system. You create keys and upload them to Azure Key Vault, then create data encryption policies (DEPs) that specify which keys to use to encrypt which data items. Microsoft manages encryption keys for any services that don't have DEPs defined.

You can currently define three types of DEPs:

- **Exchange Online mailboxes:** these DEPs are applied per mailbox and only encrypt the mailboxes they're applied to; when you apply a DEP to a mailbox, the mailbox is moved and then encrypted as part of the move.
- **SharePoint Online and OneDrive for Business:** this DEP type applies to content stored in SharePoint or OneDrive, including Teams files. You can create a single DEP per tenant unless you're using multi-geo, in which case you can create one per geo.
- **Multi-workload DEPs** apply to multiple workloads and components for all users in the tenant. You can encrypt additional Teams data (including 1:1 chats, group chats, meeting chats, conversations in channels, chat notifications, and images and videos). When you create a DEP at the tenant level it is applied in addition to, not as a replacement for, any DEPs that are currently in force on Exchange, OneDrive, or SharePoint data. The tenant-level DEPs will encrypt all data held by Exchange Online, meaning you no longer have to assign DEPs to individual mailboxes; for Teams, you can only encrypt data created after the time the policy is applied (meaning you can't encrypt historical data).

The [setup process](#) for CK is quite complex, so you should carefully consider whether you have the needed skill set and operational maturity to make use of it; it's easy to create a situation where your data items are encrypted in ways that might render them unusable in the future if you lose access to a particular key.

Double-Key Encryption

Microsoft also supports another encryption mechanism that uses *two* keys: one that Microsoft has, and one that only your organization has. Data protected with this mechanism (known as [Double-Key Encryption](#), or

DKE) is encrypted twice: first with your key and then with Microsoft's. Microsoft never has access to your key, so they can never read your protected data. For this reason, though, data protected with DKE can't be processed by several useful service features, including transport rules, content search, and eDiscovery. Sensitivity labels (see the information protection chapter) can apply protection to files using DKE.

DKE requires you to set up a key-management system of your own, build and install a connector, and deploy sensitivity labels that end users can use to tag specific documents as needing DKE protection. Microsoft makes the point very clearly that DKE is only intended for the most critical items that need the heaviest protection and isn't intended to replace the use of CK or other protection mechanisms for everyday use.

Protecting Items with Information Protection

Microsoft 365 already includes a broad set of features for protecting messages, documents, and containers. As described in the information protection chapter, you can create sensitivity labels to automatically mark specific items as requiring protection; you can use [Purview Message Encryption](#) (previously known as Outlook Message Encryption, or OME) to enforce encryption for email messages under various conditions, and you can apply rights-management restrictions to control which users can do what with specific items based on their origin, location, or sensitivity. Microsoft broadly lumps these capabilities together under the heading of "information protection"; the encryption features enabled in their information protection solution are intended to reduce the risk of accidental or purposeful disclosure of sensitive data to unauthorized people, but they aren't necessarily intended to protect against other threats.

Reporting

Microsoft 365 includes a few different sets of reports that may prove useful. The Microsoft 365 Admin center contains a reporting section with an activity dashboard and a handful of reports that give organizations a view into the adoption level for the different services they buy with their subscriptions. For example, the email activity report might show a healthy amount of usage, justifying paying for Exchange Online mailboxes, while the SharePoint or OneDrive for Business reports might show a different level of usage that prompts the organization to either reconsider the licensing of that feature or embark on an adoption project to encourage more use. Similarly, the Activations report lets an organization analyze the consumption of licenses bought for their end-users. For example, if you assign international calling licenses to users who do not use them, then you can reassign the licenses to other users who need them rather than buying more licenses.

In addition to these canned reports, there are two more detailed and more flexible reporting tools that you should know about. The first is the Adoption Score toolset, which tells you what users are doing with the service. The second is the Secure Score toolset, which is part of Microsoft 365 Defender and gives you a synoptic view of your tenant's security.

See the reporting and auditing chapter for more information about reporting and auditing, including the Microsoft 365 Usage Analytics pack for Power BI and some third-party reporting alternatives.

Adoption Score

Microsoft used to have a comprehensive set of measurements that it labeled as "Productivity Score." To describe these measurements as "unpopular" would be a master of understatement; the original feature pulled data from individual users' activity in the service and from their calendars, and combined it with service telemetry, to synthesize a series of measures that allegedly showed how productive users were being.

Adoption Score default behavior: Adoption Score is enabled by default. If you don't want to use it, you'll have to disable it using the [Adoption Score privacy controls](#).

While the idea of an overall score measuring the productivity of an organization seems tantalizing at first thought, there are some problems with this approach. It immediately calls to mind the mostly-obsolete discipline of [scientific management](#), with its rigid emphasis on measuring every activity of every worker and continuously iterating to remove all inefficiencies of process or execution. There are good reasons why most organizations don't ruthlessly try to optimize every minute of workers' work times (not least of which is the importance of good labor relations in industries or countries where workers' unions are common). On top of this, the Productivity Score feature raised many questions of data quality, relevancy, and user privacy that were asked, pointedly and often loudly, by end users, organizations, the press, workers' unions, and other entities. Microsoft [backtracked and modified the feature](#) so that it no longer showed user-specific data. That didn't change the fact that most of the data about what users are doing remained available to administrators. Now Productivity Score is dead, replaced by Adoption Score, which relies on many of the same data points but presents and packages the conclusions differently. Figure 3-14 shows the Adoption Score page.

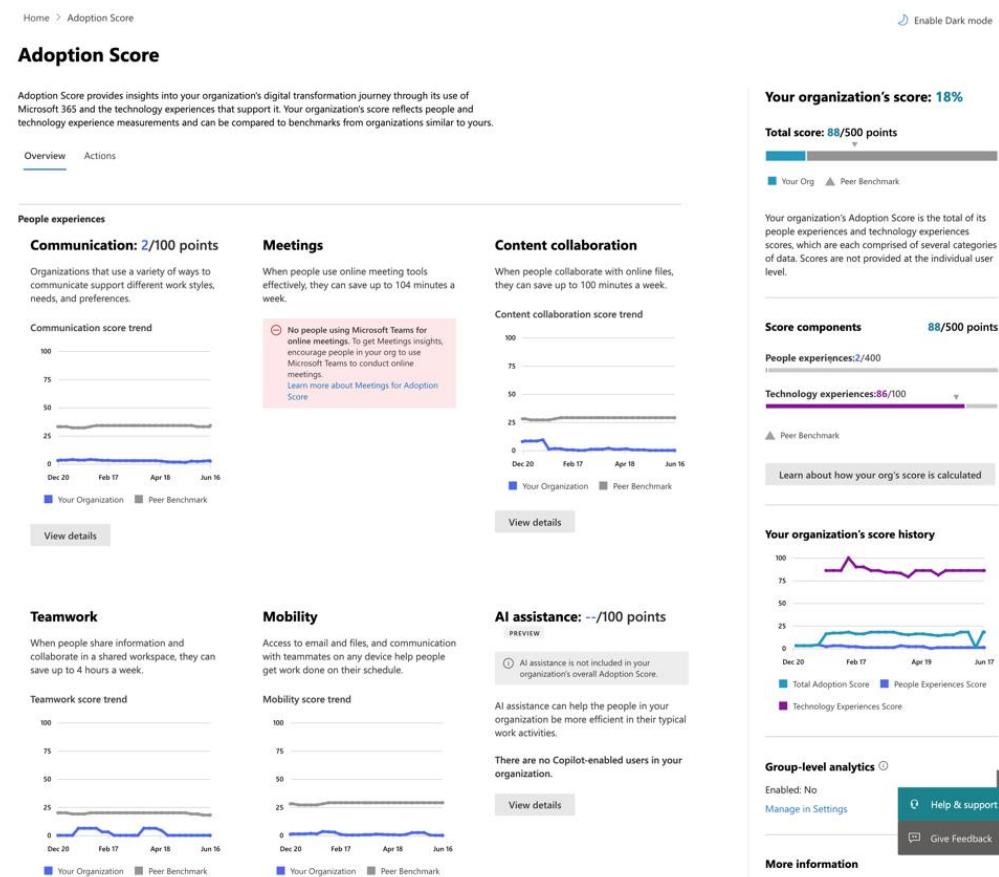


Figure 3-14: The Adoption Score summary shows organizational and people scores

Microsoft calculates the overall score based on two categories of metrics: a people experience score and a technology experience score. Each scorecard on the summary page has a more detailed page that breaks the overall score into its components. For example, the "Communications" card summary page includes metrics showing whether people are using @mentions in email and whether they are using Teams channels to communicate—and, if so, how much. Expect to see lots of work here as Microsoft tries to identify and package the key metrics that truly show value for enterprises. For example, Microsoft changed tack and [broke the "meetings" component](#) of the people experience score into multiple sub-scores—meaning any previous scores are no longer useful as a basis of comparison. This change was actually quite useful since it allowed you to see scores for pre-, intra-, and post-meeting activities (such as the percentage of meeting

invitations that included an agenda). In general, the more granular and transparent the Adoption Score metrics are, the more useful they'll be for you.

The Teamwork, Communication, Content collaboration, Meetings, and Mobility people experiences all support aggregation and filtering based on Entra ID attributes. For now, you can filter on the Company, Department, Country, State and City attributes. Before you can enable filtering on each people experience, you must complete a check to verify whether the data looks correct. For example, in my test tenant, only 8 of the 28 users have a value for the Country attribute and so Microsoft flagged it as possibly inaccurate. Once you're happy with the quality of the reported data, you can enable filtering for that experience.

As part of the Copilot rollout, Microsoft has added an "[AI assistance](#)" category that's intended to show how and how often users are taking advantage of Copilot features. Its data isn't included in your adoption score. For now, this category's data reflects usage of the summarization and content creation features. You won't see much useful data unless and until you have a good number of Copilot users who are actively making use of those features. Filtering isn't yet supported for this category.

Microsoft is working to make the Adoption Score data more actionable by enabling administrators to take actions based on the scores; this starts with a feature called "Adoption Score organizational messages." This feature allows administrators to create a custom message (for example, "QUIT EMAILING ATTACHMENTS AND USE ONEDRIVE FOR SHARING!!!!") and then automatically display it to users whose adoption score for that specific feature indicates they aren't meeting the desired goals. Administrators can't see exactly who received the message. The admin experience is [described in Microsoft's documentation](#) in more detail. Note that Microsoft is planning on consolidating Adoption Score organizational messages with tenant-wide organizational messages (described elsewhere in the chapter) sometime during late 2024.

Each Adoption Score category also may have recommended actions associated with it. These are controlled by Microsoft; they will show whatever actions they think are appropriate based on what your users are doing (or not doing) in that category. For example, the Communications category may show an action labeled "Encourage people to communicate using Teams". All of these actions currently depend on sending organizational messages, but Microsoft may add other types of actions in the future.

Usage Reports

Usage reports (described in more detail in the auditing and reporting chapter) are intended to show you some high-level summary data about what your users are doing. For example, Usage page (available through **Reports > Usage**) in my test tenant shows the number of active users using Microsoft 365 Apps, Exchange SharePoint, Teams, and Viva Engage, as well as cards showing various activity levels (including the number of files stored in SharePoint, the number of Office activations, and how much user activity has taken place in Viva Learning). The left navigation rail allows you to see more detailed reports for various Microsoft workloads, including Copilot, Teams Premium, Microsoft Edge, and Visio. The included usage reports are basic; they will give you some metrics about what users are doing, but you will need to use PowerShell or Graph (as described in the auditing and reporting chapter) to get more detailed reports if you plan to take any actions based on the data.

Microsoft Secure Score

Microsoft acknowledges that it can be difficult for an administrator to understand how to best secure a tenant. Many places exist in administrative consoles where you can tweak settings that affect how things work. In addition, a multitude of data exists within applications that administrators should check on an ongoing basis. Therefore, it makes sense to measure a tenant against a set of predetermined standards and score the tenant based on the actions taken to increase security. At the same time, Microsoft 365 can flag outstanding actions to the administrator, who then decides whether to implement the action and so increase

their tenant score. This feature was originally called Microsoft Secure Score, and, after a few false starts, that seems to be the name used throughout Microsoft 365 now for this functionality. The Secure Score dashboard allows administrators to:

- Understand the actions that contribute to the current tenant score.
- Understand how they can improve their score by completing various actions.
- Track and document the progress of their score over time.

Secure Score now lives in the Microsoft 365 Defender portal. Users who have been granted Global admin or one of the security-specific roles can see this dashboard, and you can also use the Defender unified role-based access control (RBAC) mechanism to grant access to it. Here's how it works.

Microsoft Secure Score

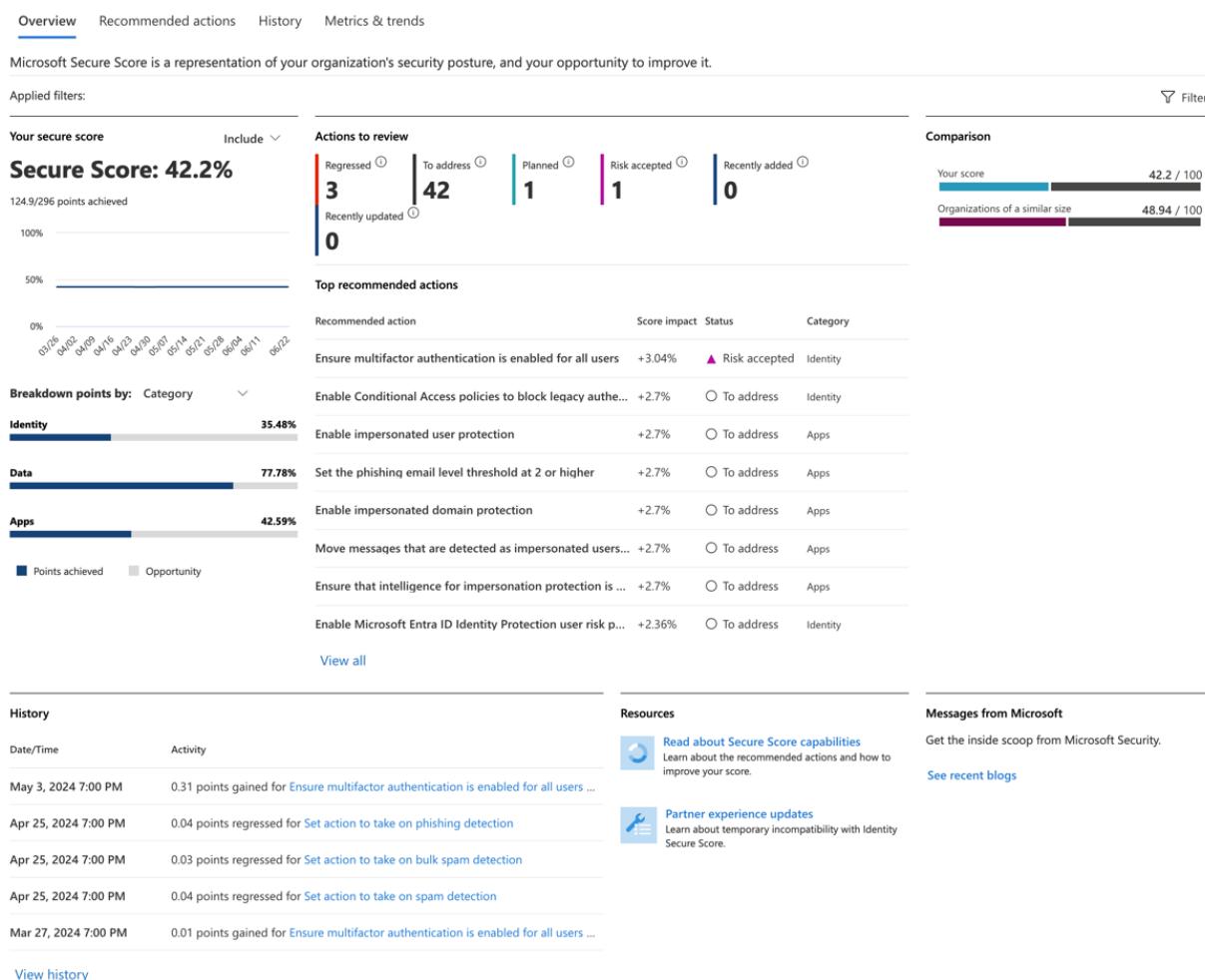


Figure 3-15: Viewing the Secure Score for a tenant

When you go to <https://security.microsoft.com/securerescore> or click the **Secure score** link in the left navbar of the security portal, you'll see a dashboard like the one shown in Figure 3-15. This version represents a significant change since its introduction in that the score is now shown as a percentage instead of a raw number of points, and it is gradually incorporating data from more settings and workloads across the Microsoft 365 platform. This dashboard summarizes your overall security score, calculated based on inputs drawn from multiple sources in the tenant including Entra ID, Enterprise Management + Security (EMS), and various Defender services, in whichever combination you have them. As you enable more security features, your score goes up. The dashboard includes a list of recommended actions that, if taken, will increase your

score. Keep in mind that some security features will increase your score but will irritate users or make it harder for them to do their jobs.

As you consider taking actions to raise your score, it's tempting to immediately find the items with the highest percentage and implement them first. While this is not a terrible idea, you need to keep in mind that your individual organization may have significantly different needs than Microsoft's ideal. For example, its location, its security maturity, and the industry it's in are all factors that affect the kinds of threats it faces, and therefore the kinds of actions you should take. The scoring metrics can be a valuable guide, but they are not infallible.

Over time, Microsoft has gradually changed the Secure Score measurements and recommendations, so a tenant's score will fluctuate even if you don't change anything. For example, in July 2024 they added new recommendations for removing permissions and rotating passwords for Entra Connect; your score will reflect whether you already implemented these recommendations even if you didn't change anything. They may also rename items or move them around; in general, you may find that you can't directly make a precise comparison between Secure Score values over time. However, you can use the history section of the dashboard to see what changes you (and any other administrators in your tenant) have made, and this may help you track Microsoft changes that affect your score.

The **Include** dropdown allows you to choose different benchmarks to measure your score against, and the filter icon lets you choose categories of score items that will, or will not, be included when the score's calculated, while the other areas of the dashboard show actions that you may want or need to take to improve your overall score. The pivot at the top of the dashboard lets you see specific actions that Microsoft recommends taking to boost your score, as well as a history of what your score has looked like over the last 90 days.

Suppose you configure Microsoft Information Protection to allow tenant users to protect confidential content; that adds 5% to your score. Even better, if users store documents in OneDrive for Business, adding AIP is worth 10%. Although you can argue that OneDrive for Business is a more secure location for documents than a local hard drive or a network file share, assigning double value to this measurement seems like more of an encouragement to do better. Other controls are easier to understand and more fundamental in terms of security—for instance, administrator accounts should use multi-factor authentication.

Secure Score combines percentages awarded for the measured aspects into a tenant score. The "Comparison trend" chart shown under the **Metrics & trends** pivot widget in the dashboard shows your organization's score compared to other organizations with a similar number of licensed seats and other organizations in the same industry you're in.

In addition to the base Secure Score mechanism, Microsoft also calculates a [separate identity security score](#) for Entra ID. Here's what Microsoft's [Chris Hallum said](#) about the apparent disparity between the identity score and the "real" Secure Score:

"The vision for Microsoft Secure Score is that it will be the centralized user experience for all security-related points and Improvement Actions across Microsoft 365 and Azure workloads. Individual products can include a secure score experience scoped to their workload however they must align to the Microsoft Secure Score design patterns and branding. They must also forward their score and improvement action data to Microsoft Secure Score so that it can provide the end-to-end super set the view for an organization's security posture."

Reviewing your identity score data, along with the list of [best practices recommended for Entra ID administrators](#), and then making appropriate changes can quickly boost your Secure Score overall and for identity management.

When you review individual actions, you'll see a comprehensive page showing lots of information about the action including a description of the proposed change, what state the service thinks you're in now, what the user impact of the proposed change is, and any historical information about changes to this setting in the past. You can mark individual actions with an action plan that tells the system what you plan to do about the risk; Microsoft also helpfully includes a list of implementation steps, although they have some room to improve the display of HTML content there.

It's also the case that the Secure Score mechanism may fail to notice and score an action you're already taking or may recommend actions whose true impact can't be scored. For example, the "Review permissions & block risky OAuth applications connected to your corporate environment" score item promises 15 percent if you use Defender to "block access to a risky OAuth app," but the precise definition of "risky" is missing, so presumably you can earn 15 percent by blocking *any* OAuth app.

Interestingly, Microsoft 365 keeps the score data for only 3 months, so if you want to see longer-term trends, you'll have to track the scores yourself. You can [access Secure Score data through Graph](#) to facilitate this.

The engineering team responsible for Secure Score constantly reviews threats and operational processes to ensure accuracy and relevance. Microsoft assesses feedback from the tenants as they analyze tenant scores to understand any gaps and weaknesses that might exist and fix the issues. The score for a tenant is likely to change over time as Microsoft adjusts its scoring scheme and measurements. Administrators should review their tenant's Secure Score regularly to ensure that they leave no gaping holes for attackers to exploit.

The Experience Insights Dashboard

The [Experience Insights dashboard](#), currently in preview, is meant to give you sentiment and user-satisfaction insights into your tenant. At present, you can enroll in this preview if you have at least 2000 user accounts. When you enroll, users who hold the User Experience Success Manager role can see aggregated organization-level data and selected parts of the Microsoft 365 admin center, including the Experience Insights dashboard.

If you have the Global admin or Global reader roles, when you log into the admin center you'll see a one-time prompt inviting you to visit the Experience Insights dashboard. If a user who has the Reports reader role logs into the admin center, they will go to Experience Insights by default. A relatively new role, User experience success manager, allows holders to see both the Experience Insights and Adoption Score modules.

If you can view the dashboard, you'll notice that it shows you summary and detailed views of data about application licensing and usage—which users use the applications they were assigned licenses for? The dashboard also includes some of the previously-mentioned NPS and feedback data currently visible to all tenants. For some apps or services (Teams being one notable example), you may be able to see more detailed usage data for individual features. The **Suggested training** view shows which support.microsoft.com articles logged-in users read and how they related to other support articles. This is meant to give you some insight into what topics your users are seeking help with. The **Actions** view tracks the actions you've taken and correlates them with changes in app activity, user feedback, or NPS.

No timeline has been announced, but Microsoft has said that they're working on rolling Experience Insights out to smaller tenants.

Backing Up Office 365

Do you need to back up your Office 365 data? This is a complex question. Interestingly, no one questions the value of backup for on-premises data. Why are things different in the cloud?

On one hand, many experienced administrators believe that it isn't strictly necessary to take backups of cloud-based data. Until fairly recently, Microsoft has encouraged this attitude by highlighting their native data protection tools. Microsoft themselves only take limited backups for SharePoint Online. They don't take backups of Exchange Online, Teams, Planner, the Viva suite, or other applications. Because Microsoft doesn't provide APIs specifically designed for backups for their cloud applications, backup vendors must resort to using protocols or APIs not intended to stream large quantities of data to copy data across the Internet to another data center (whether in Azure or another cloud provider). In addition, cloud applications are often interconnected in ways that don't exist on-premises. The result of this interconnection is that some workloads are much easier to back up and restore. Backing up the documents from a SharePoint site is relatively straightforward but restoring them in such a way that Microsoft 365 Groups and Teams work properly is a different challenge.

On the other hand, many organizations believe that backups are a good thing because they want to have a method of restoring user and configuration data should the need arise. The need might arise from what I've started to call "the four Ms":

- Malicious changes, such as those made by ransomware or a disgruntled employee.
- Mistakes, such as the infamous mass deletion of Teams chat messages caused by an administrator who misconfigured KPMG's retention policies.
- Mishaps at the cloud service provider—a more polite way to say "data loss caused by Microsoft".
- Migrations often benefit from having a comprehensive backup of the "before" state in case problems occur during the migration.

As further ammunition, some companies cite [Microsoft's Shared Responsibility model for cloud services](#) and point to its assertion that customers are always responsible for their data. In other words, Microsoft takes no responsibility for protecting data and it's up to customers to ensure that they can recover. It is not correct to say that Microsoft takes *no* responsibility; a better way to phrase things is that Microsoft invests heavily, and works hard, to ensure that *they* won't lose *all* of a customer's data, but they don't guarantee that they will *never* lose *any* of it, and they don't promise to help you if *you* lose it.

What If You Do Nothing?

Before deciding to use any backup solution, we should understand how out-of-the-box features can reduce the risk of data loss and where gaps might exist. You can think of this as the "do nothing" question: what level of data protection do you get if you don't buy or configure anything and just rely on the data protection measures in the service?

The short answer to this question is simple: the level and scope of protection for different workloads varies. Some are well-protected, and some are not protected at all.

When Exchange first introduced the concept of "native data protection," with multiple copies of each mailbox database substituting for keeping backups, many administrators were horrified, but in practice, this approach has worked very, very well when implemented properly. Email is generally considered a well-protected workload because Exchange native data protection, combined with retention policies, help mitigate the risk of loss. Retention policies cover information in:

- Exchange mailboxes and public folders.
- SharePoint Online sites and OneDrive for Business accounts, including video recordings of Teams meetings and all Stream content.
- Teams channels (regular, private, and shared) and chats (personal and group).

For greater protection, preservation locks can secure retention policies and stop administrators from being able to change retention settings. Putting all mailboxes on litigation hold will preserve their data if a rogue

administrator deletes some user accounts. And you can lock Exchange Online down further by using [Privileged Access Management](#) to limit what administrators can do to specific time-limited operations.

In fairness, though, these measures protect you against data loss but they don't deliver some of the other benefits of backup—for example, maintaining a physically separate copy of your data isn't something that retention policies can help with, and of course there are many objects (such as Entra ID conditional access policies) to which retention policies don't apply.

It's also fair to point out that some Microsoft data protection features (such as auto-label policies that find and apply retention labels to sensitive data) cost extra. That is, they require the purchase of additional licenses. As you consider the cost of a third-party backup solution you may find it cheaper to buy the backup instead of upgrading your user licenses, especially if the tenant supports many users with low-cost licenses (like Office 365 E1 or A1, or Microsoft 365 F3). On the other hand, if you need some extra features that are only available in a higher-priced plan, you might decide to use the money that would otherwise be spent on a backup service to take advantage of the high-end protection features bundled in that plan.

Backup Considerations

When we discuss the service from a backup perspective, the following aspects should be considered to decide what data should and can be backed up. Knowing what data to backup and why the backup is necessary will drive the choice of the backup technology to use. You should consider:

- Backup of the **base storage workloads**: SharePoint Online, Exchange Online, OneDrive for Business, and the configuration and user information held in Entra ID.
- Backup of **applications that use Azure** for all or part of their storage: For example, how do you handle the text and graphics for Teams messages stored in Azure Cosmos DB or the tasks and plans used by Planner?
- Backup of **applications that use multiple components** such as Teams, Planner, and Groups. The lack of backup solutions capable of dealing with workloads outside Exchange and SharePoint is currently the biggest challenge facing those who consider using third-party backups.

In addition, you should consider:

- **How are backups processed?** A backup product might be able to process the volume of data generated by a small tenant and struggle to process the volume created by a large tenant. The backup application must move data from Microsoft's data centers to the backup location, which might mean that the data must travel via the internet, so network considerations and the ability of the backup vendor to process inbound data come into play. On the other hand, if the backup location uses Azure, the data might stay within the Microsoft data center network and the transfer is faster and easier, but you may have to pay ingress and egress fees to move the data.
- **What APIs are used for backups?** Microsoft 365 includes many APIs that can interact with mail, documents, tasks, groups, and so on. However, not every API can stream large volumes of data to a backup destination, so some testing should occur to ensure that a backup application can handle the quantity of data produced by a tenant, especially at peak load.
- **What data are backed up?** Some backup vendors have ported their on-premises products to work in the cloud. Applications like Teams and Planner don't have on-premises equivalents, so on-premises backup products can't deal with their data. Thus, you might select a product that can copy Exchange Online mailboxes and SharePoint Online documents but ignores everything else. You'll be much better off looking for cloud-native products that are explicitly designed to work on Microsoft 365.

- **How often is the data backed up?** A daily backup might be enough to deal with small tenants, but constant and ongoing backups (trickle mode) might be necessary to process the quantity of data produced by large tenants.
- **Where is the backup data stored?** Most backup vendors propose using their own cloud data center to hold backup data. This approach is perfectly acceptable if it meets the customer's data at rest and data sovereignty requirements. Unsurprisingly, few backup vendors can aspire to the same widespread distribution of data centers that Microsoft has, but a growing number of backup vendors use Azure or Amazon Web Services bulk storage as a backup target. Some vendors claim that having backups in Azure is preferable (for speed and security) because data travels across the Microsoft data center network from the service to the backup location while transfer to Amazon involves an internet connection.
- **How accessible is the backup?** If the backup is in the cloud, what SLA does the vendor give about its availability to restore? Is the SLA limited in terms of the amount of data, number of mailboxes or sites, or any other factor?
- **How easily and rapidly can the data be restored?** Having a backup copy of data is one thing; being able to restore it is another. How quickly can data be brought online within an application from the backup copy? Can the data be merged with live data, or will it overwrite what's there (for example, does a complete document library need to be restored). Another factor to consider is how much effort is needed on the part of the backup vendor and tenant administrators to restore data. The ideal situation is to have a restore process that automatically connects to the backup source and inserts the data into the target repository in such a way that it is immediately usable without further administrator intervention.
- **Can data be restored in context?** Restoring a single mailbox or single document library is straightforward. It is much more complex to rebuild a compound entity like a Group, plan, or Team as it was at a point in time. This is because those entities depend on multiple components, each of which must be restored in such a way that the links between the different components are preserved and accurate. Data that cannot be restored in context might still be valuable, but it will be raw and need manipulation before it is fully usable again. Another interesting question is posed by protected content (encrypted email, documents, and other items) as the backup solution must be able to backup and restore this content too. It's also wise to ask about the granularity of restored data to ensure that it is possible to restore something like a single document into a SharePoint Online document library.
- **How much does the backup cost per user per month?** What basis is used for this calculation (per site, mailbox, licensed user, etc.). How does the cost vary as additional applications are included in the mix?
- **Does the backup vendor comply with any industry or regulatory standards that might apply to your tenant?** Such regulations include the European Union General Data Protection Regulation (GDPR), the U.S. Health Insurance Portability and Accountability Act (HIPAA), Service Organization Control (SOC), and the U.S. Federal Risk and Authorization Management Program (FedRAMP).

In short, backing up cloud application data is not simply a matter of stretching the application-centric technology and techniques used to process on-premises data. The complexity and interconnectivity of Microsoft 365 make it a radically different environment that demands a different approach to backup.

Backup for Exchange Online

Microsoft is deadly serious when it says that native data protection is the best approach for Exchange. This means that four copies of each database exist, including a lagged copy, and that data is spread across at least two data centers to ensure resilience. Users must recover deleted items if they make a mistake and if they don't do this before the default 14-day retention period (extendible to 30 days), they won't be able to

retrieve the data. Microsoft runs hundreds of thousands of mailbox servers to provide Exchange Online as a service, with all servers deployed in Database Availability Groups, and this architecture has worked quite well to protect against large-scale data loss.

Third-party software companies offer online cloud-based backups that can extract data from Exchange Online and send the data to their repositories. However, the cost of these services might not be justified for the benefit gained, especially if data is protected by features such as litigation holds. Other issues to consider include if the backup product can deal with expandable archives and encrypted content. Being able to stream data out of Exchange Online is easy (usually, backups use Exchange Web Services to connect to mailboxes and read their contents); it can be much more challenging to restore data in such a way that it is usable. For instance, if the mailbox holds email encrypted with Microsoft Information Protection sensitivity labels or S/MIME, how will the user be able to access this content in a restored mailbox?

Don't use backup utilities that extract mailbox data and store it in PSTs. This is a terrible idea from a performance, logistical, data protection, and compliance standpoint.

Backup for SharePoint Online

Unlike Exchange Online, SharePoint Online doesn't have native data protection built into the product. Accordingly, Microsoft takes backups for SharePoint Online site collections (these backups cover OneDrive for Business too). Here is what happens:

- Microsoft backs up the content in site collections approximately every 12 hours. The backups are kept for 14 days.
- Tenant administrators have no control over these backups or restores. If a restore is necessary, it can only be started by contacting Microsoft support. Microsoft will ask you to choose the best time for the restore (i.e. a time when the required information was known to exist in the site collection). Determining that time can be quite a challenge—and of course there is no guarantee that Microsoft will have a backup matching your requested time.
- Microsoft cannot restore a single item, folder, document, list, or library. A full site restore is the only option. The restore is targeted at the URL for the site collection and will therefore overwrite whatever data currently exists in the site collection. This is because their backups function at the database and table level, not at the level of individual items. If you need to preserve data in a site collection that is to be restored, you must copy or move all the information that exists in the collection before the restore is done and then readjust the content afterward as needed.

Before running to ask Microsoft support to restore a site collection, it's important to understand that SharePoint Online allows information to be recovered in three other ways:

1. The **Restore this library** option (in the settings menu for document libraries) allows site owners and administrators to recover files within a document library to a point in time within the last 30 days (OneDrive for Business has a similar feature). Restore this library is intended to deal with scenarios such as a mass deletion of files by a disgruntled employee or the infection of files through malware. If you know when an incident happened, you can restore the library to a point just before the incident occurred. Restore this library depends on [versioning](#), the ability to store different versions of files created over time. The versions can be created through the auto-save functionality built into the Microsoft 365 desktop and online apps or the files can be saved explicitly. If you don't enable versioning for a document library, you might not be able to roll back to previous versions of files. If only one version of a file exists and it's the one that is compromised, SharePoint won't be able to recover it.
2. Deleted documents and other items are held in the [SharePoint recycle bin for up to 93 days](#). SharePoint's recycle bin is in two parts. The site recycle bin is available to users and is sometimes

called the first phase recycle bin. If items are removed from the site recycle bin, SharePoint moves them into the site collection recycle bin (second phase). Administrators can retrieve items from the site collection recycle bin. After the 93-day period elapses, background jobs remove files from the site collection recycle bin. If you can't restore a file because it's outside the 30-day window

SharePoint Online allows users to restore a deleted item from the recycle bin for a document library, you can look in the site recycle bin and retrieve the file from there.

3. If a site is under the control of a retention policy, SharePoint keeps items removed by users or automatically by background jobs in a special hidden library called the Preservation Hold library. The items stay in the Preservation Hold library until their retention period expires, which could be several years. Administrators can retrieve files if needed from the Preservation Hold library. See the compliance chapter for more information about data governance for SharePoint Online.

Although SharePoint gives administrators and users the ability to retrieve files deleted in error or corrupted in some way, two factors deserve consideration when deciding if external backups are necessary. First, some user education is needed to make people aware of how to use the **Restore this library** feature and how to recover deleted files from the recycle bin. Second, the methods of recovery listed above require manual intervention to restore content to sites. Better automation, the ability to deal with multiple sites at one time, and more granular restores are reasons advanced by third-party backup vendors to justify the purchase of their products for SharePoint Online. The basic idea behind these solutions is to use remote agents that make scheduled connections to applications like SharePoint Online to grab information and copy it out to some other data center or cloud service.

Remember that SharePoint Online includes many other elements than just documents and lists such as customizations made to the search schema or term store. It's a good idea to ask your potential backup vendors what other SharePoint Online elements they can back up—losing e.g. the term store could cause a major problem.

The decision whether to invest in a third-party backup solution for SharePoint Online largely depends on how much faith you put into the way that Microsoft manages SharePoint data and the perceived risks that exist. The increasing prevalence of ransomware raises the question of how you might recover from an attack, short of paying the ransom. The usual proposed solution is to restore to a point in time before the infection occurred. This might be possible with the functionality built into SharePoint Online (if you catch the problem early) but broad-scale recoveries from malice or mistakes might be easier with a third-party backup. As in the case of any ISV solution, you should test products thoroughly to ensure that they meet your needs, including aspects such as security, privacy, and data at rest.

Backup for Teams, Planner, and Other Apps

Traditional backup products address the need to copy information belonging to an individual workload. For example, you take backups to protect data in on-premises Exchange databases or SharePoint sites. The different nature of the service creates problems for this approach because new functionality is built by combining features taken from different workloads. Take Planner as an example. Data is held in group mailboxes managed by Exchange Online, group document libraries managed by SharePoint Online, and the Tasks service running in Azure.

Teams is similar in the way that it brings data and functionality together from multiple sources to deliver to users and introduces still more complications. For instance, Teams can use Planner as one of its resources. Currently, there is no comprehensive public API available meant for backing up Teams or Planner data; some structural information (for example, the channels in a team) can be extracted using the Graph API, but no API exists to allow the totality of user data to be backed up from Teams and its associated apps.

This makes Teams the [most challenging of all Office 365 applications](#) from a backup perspective. This is slowly changing; for example, Microsoft has [released a Teams export API](#), but it only handles 1:1, group chat messages, channel messages, and reactions, meaning that there are still several other data items (and many metadata items) that aren't available through the API and thus cannot be reliably backed up or restored. Worse, this API carries a charge to the customer—that is, if you use a backup product that calls the export API, you will incur a charge for every message read through the API. To force usage of this API, Microsoft [has deprecated the ability of Exchange Web Services \(EWS\) to read Teams compliance items](#) from user mailboxes, a method that some vendors have used; it would not be surprising if in the future Microsoft restricts the existing Graph `getMessage` endpoint by throttling it further.

Worst of all, there is no corresponding *restore* API to match the export API. It is critical to understand that your ability to restore Teams data will probably fall far short of your expectations, as Microsoft has *no* supported APIs for ingesting Teams channel content with original metadata. Ask any vendor you're thinking about working with to demonstrate a full end-to-end backup and restore cycle on a Team that you choose before you pull out your credit card.

Note: Backing up the compliance records captured for Teams chats and channel conversations in Exchange Online is not enough – the items are incomplete and cannot be restored into Teams chats or channel conversations in a usable fashion.

Likewise, no backup APIs exist for Planner or Stream so care should be taken when considering how to extract information from these applications for backup purposes.

Protection Against Ransomware

Despite the cautious attitude to third-party backup technology for Office 365 expressed here, it is possible to make a case to use backups to protect against the consequences of a ransomware attack. Historically, the biggest target of ransomware has been on-premises directory and application servers, then user documents and data. For example, many large-scale ransomware attacks compromised on-premises email servers by rendering them unbootable and encrypting their disk volumes—the individual mail messages and mailboxes themselves weren't separately affected. However, ransomware is a real and persistent threat for OneDrive and SharePoint deployments, apart from the risk posed to Active Directory servers on-premises. For these reasons, it is worthwhile considering using backups to have copies of data available should a ransomware attack succeed against your tenant.

While it's tempting to assume that a superior defense will prevent attacks from escalating to the point where backups are required, the increasing number, scope, severity, and sophistication of ransomware attacks have all made it clear that no one can count exclusively on defensive measures to prevent ransomware in the first place. While organizations should make sure to secure their tenants by following basic best practices (including eliminating basic authentication as far as possible, using multi-factor authentication for all accounts, and educating users about techniques such as phishing), backup remains your ultimate measure of defense.

Microsoft 365 Backup and Microsoft 365 Backup Storage

Microsoft addresses the perceived customer demand for backup by offering their own backup tool, Microsoft 365 Backup, for Exchange Online, SharePoint Online, and OneDrive. Microsoft 365 Backup entered public preview in mid-January 2024 and was released to general availability on 31 July 2024. In addition to the Microsoft-branded backup tool, Microsoft is also making the storage and API layers available for third-party backup vendors to use, so when you see third-party ISVs that offer support for "Microsoft 365 Backup Storage," that's what they're talking about.

Microsoft's backup engine is optimized to solve the problem of how to efficiently do large-scale, high-speed restores to help with ransomware recovery. They use two primary means to do this: Exchange Online mailbox changes are captured via the same copy-on-write process used to implement legal hold, and SharePoint and OneDrive make snapshot copies of the underlying databases that hold the data to be protected. Both mechanisms generate copies of data that are held entirely within Microsoft's network (specifically within the geographic region where the original tenant is based). They are not directly readable by administrators, and there's no way to copy or export them. Microsoft highlights that all backup data is held within the Microsoft security boundary and is never exported outside of its local region or exported or shared with third parties.

Restores can currently be performed at the SharePoint site level, the OneDrive account level, or on individual mailbox items. Because restores aren't performed using Microsoft Graph, they can run much faster than with conventional backup solutions, but you're trading high restore performance for coarse restore granularity, and restores do not start instantaneously, with a built-in provisioning delay affecting even small restores.

Pricing and Billing

One key item of note in Microsoft's solutions is their [pricing](#): Microsoft charges per "restorable gigabyte." The simplest way to think of this is that you can total the sizes of the items you want to protect (so the site size or OneDrive account size reported in the admin center usage reports, or the size of each protected mailbox, including its Recoverable Items subtree) and multiply that by the per-gigabyte price. Once you protect an item, if the item size goes up, you'll pay more to protect later versions; if the item size decreases, you still pay the original price because the original item is still being protected. That is, if you back up Anna's 10GB OneDrive today, and then tomorrow she deletes data so that her OneDrive now only contains 2GB, you'll still be charged for 10 recoverable GB. If next week she adds another 25GB of data (making the total 27GB), you'll be charged for 35GB starting at that point: the 10GB of original data, plus the 25GB of added data.

Snapshots made using Microsoft's tool are currently retained for exactly 12 months, although allowing a selectable retention period is one of Microsoft's priorities. There's no integration, current or planned, between the retention labeling mechanism built into the service and backups (except that retention labels applied to documents and mail items are backed up and restored).

Microsoft has established a price of US\$0.15/GB for storage consumed by their own product, and they offer a [pricing calculator](#) to help you estimate the cost. If you buy a third-party solution that uses Microsoft 365 Backup Storage, the pricing may be different (and the ISV may absorb the cost themselves or pass it on to the customer).

In either case, before you can use the new mechanism, you must establish a [Syntex pay-as-you-go](#) billing account. This requires an Azure pay-as-you-go subscription (with an associated payment method) and a resource group in that subscription. You can use an existing subscription if it supports PAYG. After you've set up the subscription, to enable Microsoft 365 Backup, go to the **Setup** area of the Microsoft 365 admin center, scroll down until you find the "Files and content" category, and click **Use content AI with Microsoft Syntex**. That will take you to a page with a prominent **Manage Microsoft Syntex** button. Click it and you'll see a list of available Syntex features. From that list, you can set up Backup by clicking its name and accepting the terms of service.

Creating Backup Policies

Backup for each supported workload is controlled by the associated protection policy for that workload. In the preview, you can only have one policy for each workload, although you can add multiple sites, users, or mailboxes to the workload policy as you like. At first, all 3 workloads will show a small icon labeled "Not set up," accompanied by a **Set up policy** button. When you click that button, you'll be able to choose specific items to protect. For Exchange you can pick users or select security or distribution groups; for SharePoint

you can choose individual sites or specify a naming pattern to use, and for OneDrive you can pick users. In all cases you can also upload a CSV specifying the items to cover.

Once the policy has been created, Microsoft does some currently-unspecified background provisioning that takes roughly 15 minutes per 1000 items; once that provisioning completes, the policy will begin to protect data.

Snapshots run automatically. You can't see any data about when they run or what happened during the run, although the summary page in the admin center will tell you if any problems have occurred.

Restoring Data

To restore data, you choose a workload and then specify a point in time (the "recovery point objective," or RPO) from which you want to restore. The snapshot closest to that RPO time will be used for the recovery. SharePoint and OneDrive support what Microsoft calls "express restore points," which are simply snapshots that can be restored with minimal provisioning delay. All data for the selected OneDrive users or SharePoint sites will be restored; for Exchange Online restores, you can choose to restore all data or specific items from a chosen time window of up to 14 days based on sender, recipient, keywords in the subject, or the presence of attachments.

Third Parties and Microsoft 365 Backup Storage

Customers can use either the Microsoft 365 Backup product or a third-party product that uses the Microsoft 365 Backup Storage layer. You can't use both at the same time. Only one product at a time can use the storage layer, although you should be able to switch products without losing your snapshot history. The details of how each third-party vendor will integrate with Microsoft 365 Backup Storage are up to the individual vendors. A set of onboarding APIs allows third-party products to [register as backup providers](#); each registration request requires a tenant administrator to approve the registration. When approved, that registration will start a seven-day grace period, at the end of which control over the backup APIs will be passed to the newly registered application.

How Service Changes Affect Backup Technology

Backup technology changes over time to improve functionality and make it easier to backup and restore Microsoft 365 data. It's also true that the service's feature set changes over time, which can make it harder for an organization to copy all the data in use. For instance, the lack of a suitable API to extract Teams data for backup is a problem for tenants who use Teams. Likewise, if you enable auto-expanding archives for Exchange Online mailboxes, you might find that your selected backup product is unable to process this type of archive mailbox.

Technology changes at a fast cadence, especially in the cloud. The need for external backups might not be the same today as it was a couple of years ago. For this reason, it's wise to review your backup strategy (or rather, the need for backups) on an ongoing basis to make sure that your organization only uses what is necessary instead of following the dogma that often comes from on-premises systems.

Chapter 4: Managing User Accounts

Paul Robichaux

In the on-premises world, a user's account typically contained both identifying information (such as a security ID, or SID), plus all the settings that applications and devices need to decide what the user can do. As part of their effort to make Microsoft 365 fully hybrid, Microsoft has effectively split apart this traditional binding. As described in chapter 3, Microsoft 365 user identities control only authentication to the service; other metadata associated with user accounts, such as Office 365 licenses or management roles assignments, control how the user may interact with the service. These two sets of data no longer must be stored in the same place. For example, Exchange and Teams have their own separate shadow copies of some user attributes that they use for its own purposes. In this chapter, we'll discuss how to manage the accounts themselves and the most important metadata associated with them.

Managing User Accounts in the Microsoft 365 Admin Center

Many of the day-to-day admin tasks you'll deal with involve user accounts. The **Users** option in the left navigation bar of the Microsoft 365 admin center is where you'll manage users, contacts, guest users, and deleted users, apply different filters to view only the set of users you need to work with, and quickly take common actions on those accounts. For example, the view in Figure 4-1 uses the licensed users filter to exclude guests and other unlicensed users; the drop-down menu shows actions that you can take on the current selection.

These pages give you quick access to the users and contacts in your tenant, whether synchronized from an on-premises Active Directory or natively homed in the cloud. When you look at the details for an individual user, you can, with one click, delete the user or block them from signing in or changing their password; with a few more clicks, you can easily assign roles, change their multi-factor authentication settings, and perform other common individual tasks.

Display name	Username	Department	Actions
Vasil Michev (Technical Guru)	Vasil.Michev@o	Information Technology	<ul style="list-style-type: none">Reset passwordExport usersLicensed u...Change viewDirectory synchronizationManage priority accountsTeams setup status
Tony Redmond	Tony.Redmond@	Global HQ	
Terry Hegarty	Terry.Hegarty@o	CEO Office	
Sean Landy	Sean.Landy@o	Information Technology	
René Artois	René.Artois@o	Sales	

Figure 4-1: Viewing licensed users in the Active Users section of the Microsoft 365 admin center

Where you initially create user accounts matters a lot. Some properties are cloud-only (such as the set of assigned Office 365 licenses), whereas others (such as the password hash) may either be cloud-native or synced from the on-premises Active Directory, depending on where the account lives. The admin center tools hide much of the complexity of setting properties for user accounts. You can view and change most properties without worrying about where the account lives. However, you can't use the admin center to edit some key properties of on-premises accounts synchronized to the cloud using Azure AD Connect. For example, you can't edit a synchronized user's first or last name or change their email addresses, as those attributes are authoritative from the on-prem directory.

When you create a user from the admin center, the account is always created in the cloud. You must specify some basic information about the user; you can have the service generate a password for you or you can specify one, and you can assign any of the licenses you've already purchased for the tenant. You may also save the user configuration as a template to speed up the configuration of future users with similar settings. Templates allow you to specify profile information such as location and department, the service domain, and the licenses to assign.

Remember that creating an account through the Microsoft 365 admin center results in a bare-bones account. Many other actions might be necessary to make the account fully functional for its owner to use. These actions include:

- Assigning additional or non-standard licenses (like Teams Premium or SharePoint Syntex) that only certain accounts in your tenant should have.
- Adding the account to distribution lists, Microsoft 365 groups, and Teams.
- Assigning administrative roles to the account. Role assignment is part of the Microsoft 365 user account creation process, but organizations often prefer to manage administrative roles through a process like Entra ID Privileged Identity Management.
- Adding a manager for the new account.
- Setting up multi-factor authentication for the account.
- Amending mailbox regional settings. Because scheduling depends on accurate times, it's important that the mailbox has the correct time zone.
- Adding a photo to the account.
- Sending a [welcome message](#) to the new user.

In larger organizations, it's common practice to automate account creation and onboarding to perform all the actions listed above and more. You can do this with PowerShell, Graph API, or any number of other tools. Apart from anything else, scripting account creation usually results in a higher level of standardization and accuracy in the directory, which is a big advantage if the organization uses dynamic distribution lists or dynamic groups that depend on accurate account properties to calculate membership. When scripting account creation, the input information about the new user might come from a HR or other onboarding system. The PowerShell chapter includes details of how to script the actions necessary to transform a simple user account into a fully functional Microsoft 365 account.

Microsoft continues to gradually roll out better integration between different user-related actions. For example, when you delete a user, you can optionally choose to also remove that user's licenses and/or mailbox delegate permissions or grant another user access to the deleted user's OneDrive files or email, using a simple set of checkboxes. You should expect Microsoft to continue adding support for these kinds of multi-step operations under the banner of "improving efficiency" throughout the admin center experiences.

Directory Accuracy and Completeness

Many Microsoft 365 features depend on the directory storing accurate user data. The most basic example is the user profile card displayed throughout Microsoft 365 and the organization information exposed in the

Org Explorer (see below) An inconsistent directory creates user frustration and might stop some features working properly such as when applications execute queries against Entra ID to locate sets of objects. For instance, adaptive scopes used with retention or communication compliance policies calculate the users for policies to process by reference to user account properties. Dynamic Entra ID groups use account properties to build the membership of dynamic groups and teams.

To ensure that directory information is kept updated, some companies use their HR system as the directory of record and have a direct feed between it and Entra ID, with updates in reporting relationships, job titles, phone numbers, and so on synchronized periodically. Others use third-party products like [Live Tiles Directory](#) to find and fix problems in Entra ID. For instance, you might find inconsistent use of account properties like city or state, and province. Another frequent problem is missing values for properties like department or office. If you don't want to use a commercial solution to check Entra ID, you can build your own checks with PowerShell like the script [described in this article](#).

Historically, we know that directory information has a nasty habit of degrading over time. Company restructuring, people changing jobs and locations, the impact of mergers and acquisitions, and even the effect of work from home all conspire to introduce inaccuracies into directory data. For that reason, it's important to check the directory for missing and inaccurate data periodically.

The Org Explorer: The [Org Explorer](#) maps directory information to create a guide to the organization structure and the roles held by individuals. The Org Explorer is available in several applications, including Teams and Outlook. To view the Org Explorer, an account must have a license that includes the People in Viva service plan such as the Microsoft Viva Suite.

Enabling Self-Service User Management

Any Microsoft 365 user can log into [portal.office.com](#); this is often how users get access to desktop application software. Most users don't know this, though, and fewer still understand the difference between the Entra ID and Microsoft 365 portals, the *My account* link, and what data and actions are available from each.

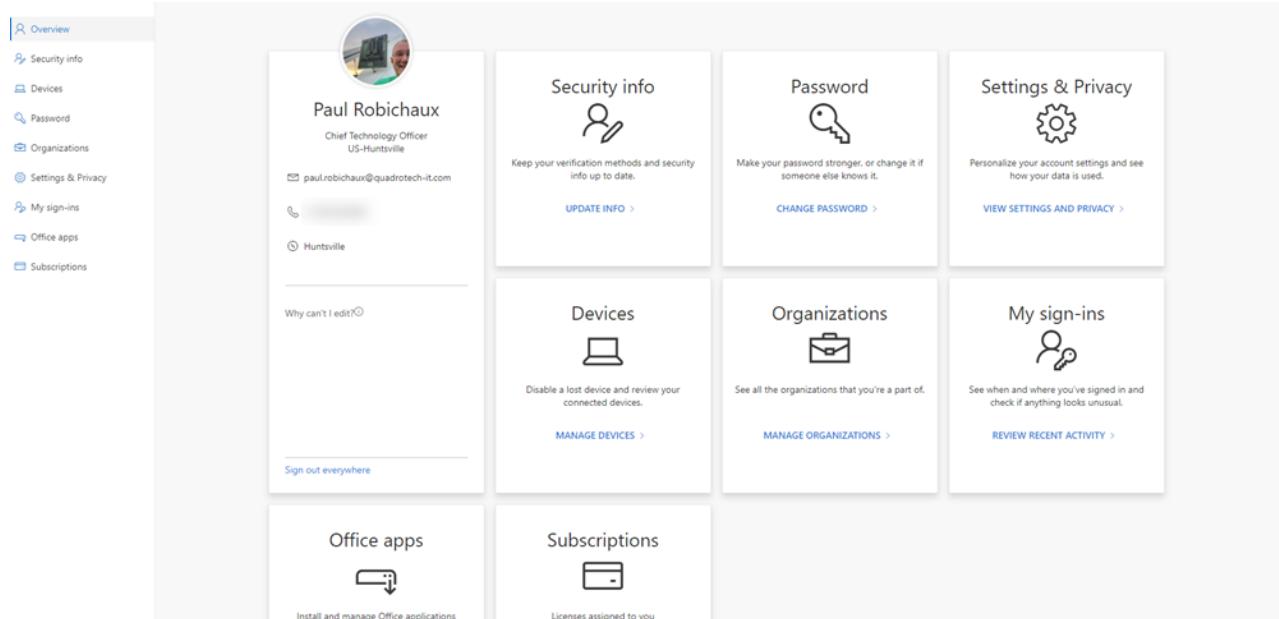


Figure 4-2: The integrated account view is available to all users

When a user logs in and clicks on their profile icon in the upper-right corner, then chooses the [View account link](#), they'll see a view similar to Figure 4-2, from which they can see and change many of the settings associated with their account. For example, they can see what devices they have installed Microsoft apps on

and what licenses or subscriptions are assigned to them (including ones they've purchased). Since the introduction of the view, Microsoft has added Entra ID sign-in [information](#), and it's reasonable to expect that they will continue to add more self-service data and actions in this view.

Managing User License Assignments

doesn't charge for (e.g., the free trial-version licenses formerly available for Stream, Teams, and Power BI), access to any workload requires users to have an appropriate license. Normally accounts receive licenses when they are added to Microsoft 365. You can assign licenses manually through the admin center, via a custom provisioning script, as part of a migration, or using third-party products. By the same token, when a user leaves, you may wish to reclaim the license, bearing in mind the limitations covered later.

Starting in mid-September 2024, accounts with the User or License administrator roles can assign or remove licenses for user accounts. Microsoft says that "*this change drives consistency with other Microsoft Entra portals in which these roles can assign licenses*," but it's a notable change and you may need to reassign role permissions to certain users in your tenant as a result.

Group-Based License Management

Managing licenses for a large user population has been a challenge for many customers. Automation is essential, as manual methods are far too time-consuming for any environment with a high rate of change.

In the past, some organizations invested time to script solutions based on AD group membership. These scripts typically require that the user be added to a group whose members should receive an Enterprise E5 license, and the custom script runs the necessary PowerShell commands to assign that license. This approach becomes challenging with more complex licensing scenarios such as sub-SKU features and assigning multiple products to an individual user (e.g., Enterprise E5 plus Project and Visio).

To solve these challenges Microsoft offers group-based license management. This feature was originally present in the Entra admin center and required a paid or trial subscription for Entra ID P1 or greater. Entra ID P1 can be purchased on its own, but it's included with Microsoft 365 Enterprise E3 or A3 and higher. The Office 365 enterprise plans can natively use group-based licensing, so you probably won't have to buy anything.

Microsoft has moved the controls for group-based licensing to the Microsoft 365 admin center, although at present you can still see group-based assignments in the Entra portal. The official way to manage group-based licensing is thus to go to the **Licenses** section in the Microsoft 365 admin center, select the license you want to assign, and use the **Groups** pivot to assign that specific license to the groups you want.

The groups that you can assign licenses to can either be created in Entra ID or synchronized from on-premises Active Directory. The license assignments can either be static (i.e., to the members of a group) or dynamic (e.g., based on user attributes such as *ExtensionCustomAttribute1*). For some organizations, a department-based model will be the preferred approach, with licenses assigned to groups representing the different departments within the organization. For others, a product-based approach will be more appropriate, with each type of license being assigned to a single group, and the users being added to that group regardless of which department they are in. If you're using static groups instead of dynamic groups then you will need to directly add the user accounts to the group, as nested groups will not be supported for group-based licensing until the new licensing platform is delivered.

Transitioning from direct license management to group-based license management is simple. Once you put the group-based license assignments in place, users can have both a direct and group license assignment listed for their account for the same type of license. However, they will only consume a single paid license, allowing you to remove the direct license assignments slowly to ensure there are no unexpected results.

License assignments will fail if there are no available licenses to assign. The solution is to purchase more licenses, then force the group-based license assignment to reprocess.

As Microsoft rolls out new features to your tenant they will usually be enabled by default. This will apply to group-based license assignments as well, with new sub-SKU features being enabled by default. As new features arrive you should review your group-based licenses to ensure that any new sub-SKU features are enabled or disabled to meet your organization's requirements.

To configure group-based licensing assignments, go to the **Licenses** page in the Microsoft 365 admin center. On the **Subscriptions** tab, you'll see a list of the licenses in your tenant. Clicking any one of these items will bring up a summary page for that product with two tabs. The **Users** tab allows you to directly assign that product to users, and the **Groups** tab lets you select groups for assignment. To assign licenses to a group, switch to the **Groups** tab, click **Assign licenses**, and select the group you want to use. Under the **Turn apps and services on and off** accordion control, you can select the sub-features (service plans) for the license that you've chosen to assign to the group. In the example shown in Figure 4-3, all the Copilot features are enabled for the newly licensed users.

Assign licenses to groups

The screenshot shows the 'Assign licenses to groups' section of the Microsoft 365 Admin Center. At the top, there is a search bar with placeholder text: 'Search for groups to assign Copilot for Microsoft 365 licenses to. You can assign to a maximum of 20 groups at a time.' Below the search bar is a list box containing a single item: 'cu Copilot Users'. Underneath the list box is a heading 'Turn apps and services on or off' with a small upward arrow icon to its right. A note below the heading says: 'To make sure Copilot works correctly, don't turn off any apps or services. [Learn how to assign licenses to users](#)'.

Below the note is a list of service plans, each preceded by a checked checkbox:

- Copilot Studio in Copilot for M365
- Graph Connectors in Microsoft 365 Copilot
- Intelligent Search
- Microsoft 365 Copilot for SharePoint
- Microsoft 365 Copilot in Microsoft Teams
- Microsoft 365 Copilot in Productivity Apps
- Microsoft Copilot with Graph-grounded chat
- Power Platform Connectors in Microsoft 365 Copilot

Figure 4-3: Configuring service plans for a license assignment

Click **Assign** when you're happy with your selections to create the license assignment. You'll see a modal confirmation dialog that points out that license assignments "might take a moment," although they are usually updated almost instantaneously. For on-premises Active Directory groups, you should expect the normal directory synchronization delay before group membership changes flow through to license assignment changes.

To reduce the risk of licenses being accidentally removed from users, if a user is removed from a group that is managing their license assignments the associated Microsoft 365 services will initially go into a suspended state instead of a deleted state. The user will not be able to access and use those licensed services, but their data will be safe while their IT administrators correct the licensing mistake. If the license removal was intentional, the suspended services will eventually age out to a disabled state and will begin their normal deletion and final purge processes.

User accounts can be members of multiple groups for license assignment. For example, if a user is a member of groups that assign Office 365 E3 SKU and a group that assigns the Enterprise Mobility and Security E3 license, the cumulative effect is that both licenses are assigned to their account. This allows you to approach group-based licensing in a modular fashion, instead of needing to create separate groups for all possible combinations of license assignments in your organization.

[This article](#) describes how to use PowerShell to control the assignment of group-based licensing, including how to generate a report showing licenses assigned to user accounts through both direct and group assignments.

Note: Groups used for group-based licensing assignments must be security-enabled. If you want to use a Microsoft 365 group for license assignment, make sure that its *SecurityEnabled* property is set to True. Groups created using the Entra admin center are security-enabled, but other administrative interfaces might not set the property. To update a group, run the *Update-MgGroup* cmdlet:

```
$Group = (Get-MgGroup -Filter "DisplayName eq 'HR Working Group'")  
Update-MgGroup -GroupId $Group.Id -SecurityEnabled:$True
```

License Stacking

Some Microsoft 365 workloads support “license stacking.” This means that administrators can assign multiple licenses for the workload to an account. When this happens, the workload selects the license that allows maximum (or superior) functionality and applies that license when assessing if the account can use a license-controlled feature. For instance, an account can hold a license for Teams granted through the Teams exploratory SKU and Office 365 E3 license. In this case, Teams will use the “full” license granted through Office 365 E3.

In Exchange Online, license stacking is important because the mailbox belonging to an account can go into a soft-deleted state very quickly after an administrator removes a license from the account and a delay occurs before they assign a new license. For instance, when replacing Office 365 E3 with Office 365 E5, removing the E3 license may cause the mailbox to go into soft-deleted status before an administrator assigns the E5 license. Group-based licensing may also trigger similar behavior when accounts might be present in multiple groups. With license stacking in place, the issue should not happen, and mailboxes will remain online.

Allowing Users to Buy Licenses

Microsoft benefits by selling as many licenses as possible for Microsoft 365 services. In January 2020, Microsoft introduced a self-service purchase mechanism to allow people with a valid user account in a tenant to effectively bypass their IT departments and buy licenses for the Power Platform products (Power Automate, Power Apps, and Power BI). They have since added other parts of Microsoft 365 (for example, Visio, Project, Power BI Premium, and Power Automate), as well as Windows 365 Enterprise and Windows 365 Business. MC 899941, released in late September 2024, announces the impending rollout of Microsoft 365 Copilot self-service purchasing but it wouldn’t be surprising to see the rollout delayed based on the negative feedback I expect Microsoft to get for this change.

Users were originally able to sign up for 30-day trials of Project and Visio using the self-service mechanism by supplying their own payment information. Microsoft changed the Visio trial mechanism so that users can enable it for a free trial, or request a license for purchase by the organization, without supplying any payment information.

Managing Self-Service Purchases

Over the years, Microsoft has gradually expanded the products available for user self-purchase. The set now includes:

- Clipchamp Premium.
- Dynamics 365 Marketing Additional Application.
- Dynamics 365 Marketing Additional Non-Prod Application.
- Dynamics 365 Marketing Attach.
- Dynamics 365 Marketing.

- Microsoft 365 F3.
- Microsoft 365 Copilot.
- Microsoft Purview Discovery.
- Power Apps per user.
- Power Automate Per User with Attended RPA Plan.
- Power Automate per user.
- Power Automate RPA.
- Power BI Premium (standalone).
- Power BI Pro.
- Project (Plan 1 and Plan 3).
- Teams Exploratory.
- Teams Premium.
- Visio (Plan 1 and Plan 2).
- Viva Goals.
- Windows 365 (Enterprise, Business, or Business with Hybrid).

The default is that Microsoft allows users to purchase licenses. Many administrators don't want users to buy licenses outside of the normal IT controls. In particular, the idea that users should buy their own Purview licenses is frankly madness.

Note: Microsoft is adding controls in the Microsoft 365 Admin center so that administrators can manage user self-service license purchases. This is a welcome change given the decrepitude of the MSCommerce module; as this update rolls out, we'll update the text of this section. If you see an item in **Settings > Org settings > Self-service trials and purchases**, that means Microsoft's rollout has reached your tenant.

Thankfully, you can prevent users from doing so with PowerShell. If you want to [globally block all users from adding self-service licenses](#), you can do so with the *Update-MgPolicyAuthorizationPolicy* cmdlet:

```
Update-MgPolicyAuthorizationPolicy -AllowedToSignUpEmailBasedSubscriptions $false
```

Instead of disabling self-service purchase for the organization, you can use the [MSCommerce](#) PowerShell module to grant or allow this ability for individual users. To make changes, download the module from [the PowerShell gallery](#). Version 2.3 is the current version; Microsoft disabled all earlier versions because they contained a security vulnerability. You can only use the module with an account that has the Global admin or Billing admin roles. Note that this module only supports PowerShell version 5 and earlier, so you may not be able to easily install it.

```
Install-Module -Name MSCommerce
Import-Module MSCommerce
Connect-MSCommerce
```

Run the *Get-MSCommerceProductPolicies* cmdlet to see what products are available for self-purchase. If the *PolicyValue* setting is Disabled, users cannot self-purchase. If Enabled, they can.

```
Get-MSCommerceProductPolicies -PolicyId AllowSelfServicePurchase
```

ProductName	ProductId	PolicyId	PolicyValue
Project Plan 3	CFQ7TTC0KXNC	AllowSelfServicePurchase	Disabled
Visio Plan 1	CFQ7TTC0KXN9	AllowSelfServicePurchase	Disabled
Project Plan 1	CFQ7TTC0KXND	AllowSelfServicePurchase	Disabled
Power Apps	CFQ7TTC0KPOP	AllowSelfServicePurchase	Disabled
Power BI Pro	CFQ7TTC0L3PB	AllowSelfServicePurchase	Disabled
Power Automate	CFQ7TTC0KPON	AllowSelfServicePurchase	Disabled
Visio Plan 2	CFQ7TTC0KXN8	AllowSelfServicePurchase	Disabled
Microsoft 365 F3	CFQ7TTC0LH05	AllowSelfServicePurchase	Enabled

You can disable self-service on a product-by-product basis by running the *Update-MSCommerceProductPolicy* cmdlet, or, as in this example, disable self-service purchases for all products:

```
Get-MSCommerceProductPolicies -PolicyId AllowSelfServicePurchase | Where-Object {$_.PolicyValue -eq "Enabled"} | ForEach {Update-MSCommerceProductPolicy -PolicyId AllowSelfServicePurchase -ProductId $_.ProductId -Enabled $False}
```

Starting in July 2024, Microsoft will post [notifications in the admin center](#) when users make a self-service purchase. Accounts with the Global admin or Billing admin roles will see these notifications in the notifications area of the admin center. You can ignore the notifications, or you can use them to identify the purchases and then either take over the license or cancel the self-service purchase—but, as previously noted, you can pre-emptively solve the problem by disabling self-service purchases at the tenant level.

Self-Service Trial Licenses

Some services allow users to get trial licenses. For example, users can [request trial licenses for Viva Goals](#) or Power BI Pro themselves. When they do, the licenses are automatically assigned and granted, and they appear alongside paid licenses in the Microsoft admin center. However, these trial licenses will expire at the end of their trial period, and users can't convert them to a paid license on their own; an admin must do so.

Administrators receive notifications when users in their tenant start a new trial.

In addition to user-driven self-service trials, administrators can request trials for various Microsoft products through the admin center; for example, you can sign up for a trial of Entra ID P1 or P2 licenses, or for various Defender features. As with user-initiated trials, these licenses show up in the **Licenses** and **Billing** pages of the admin center and can be assigned and managed just like paid licenses.

Canceling or Taking Over User-Initiated Licenses

If a user has bought a license, or started a trial, as the admin you have the option to cancel their purchase or trial through the **Billing > Your Products** page. From this page, when you select the **Self-service** filter, you'll see all users who have purchased licenses or started trials on their own, and you can cancel their purchase or trial. In that case, users lose access to the service associated with the license. You can also [take over their self-initiated license](#) by moving them to a managed subscription; in that case, they keep access but the license is accounted for as part of your normal subscription.

Allowing Users to Request Licenses

In an ideal world, we'd always have a big enough budget to buy enough of the right licenses to assign every user exactly what she needs. In practice, this doesn't happen much, so sometimes users don't have the licenses they need. Besides permanent assignments, it is sometimes the case that a user needs a license for a specific assignment or task. To help solve this problem, in the same way that you might check out a book from the library, Microsoft allows users to request licenses on their own, but only if you block self-service purchases first. The way this currently works is a little weird: users click the "buy now" link from the product page on Microsoft.com, then enter their email address. If the domain matches a domain that's enrolled in the service, the user logs in with her credentials, then is presented with a form. The contents of the form may vary depending on what you've done. Let's say that Alice wants to buy Power Apps licenses for herself, Bob, and Carlos:

- If the organization enables self-service purchases, Alice goes to the Microsoft.com page for Visio, supplies her payment information (which must be a valid credit card), logs in to the tenant, and specifies the email addresses for Bob and Carlos. The purchase proceeds and the licenses are assigned to those users.

- If you want to force Alice to use your organization's existing license process, you can go to the **Billing > Licenses** section of the admin center and click on the **Requests** pivot, then click the **Use your existing request process instead** link. This page allows you to set a message that users see when they try to buy a self-service license (e.g. "To request a product, file a service ticket at <https://help.internal>"). Alice will see this message but isn't prompted for anything else; her request won't appear in the admin center.
- If the organization doesn't have a specific process, then when Alice tries to make a self-service purchase, she'll see the same form as described earlier, asking for payment details and so on, but when she submits the request, it will appear on the **Requests** pivot. You can approve or reject individual requests, and for requests you approve, you can choose which users in the request are approved (e.g., you can accept the requests for Alice and Carlos but reject Bob). Remember that accepting the request allows it to be completed for the original purchaser, just as if you had enabled self-service purchases directly. The purchased licenses aren't considered as part of your tenant subscriptions.

Assigning Licenses with an Auto-Claim License Policy

In addition to having a license assigned automatically through group membership, manually by admin action, or manually by the user herself, you can control license assignments through an *auto-claim policy*. This policy allows a user to automatically receive a license when they try to use a workload for which they are currently unlicensed—think of it as a just-in-time automated license assignment. The auto-claim policy is triggered the first time an unlicensed user signs into the workload, and the resulting license stays assigned to the user until you do something to remove it.

Auto-claim policies are very broad in scope: they apply to all users in the tenant, including new users that you create after the policy is enabled. They don't require any premium licensing though, and they don't assign a license to a user until the user tries to launch the app.

Each tenant can have a single auto-claim license policy, configured in the **Auto-claim policy** pivot of **Billing > Licenses** in the Microsoft 365 admin center. Some tenants have auto-claim enabled by default, while others do not. If your tenant has this setting disabled, you'll see a **Turn on setting** button the first time you visit the pivot.

The auto-claim policy specifies:

- Which apps the policy assigns.
- What license to assign when an unlicensed user signs into the specified apps for the first time. Obviously, the plan should license the use of the app.
- One or more backup licenses to assign should no available licenses exist for the primary assignment. The backup licenses are in priority order and the claim is made for the first available license in that order.

Currently you can assign Teams, Power Apps per-user, and Power Automate (both premium and per-user licenses) through the auto-claim mechanism. However, you can only create a policy when you have licenses for the corresponding product, so you may not see every supported product when creating a policy if you don't have licenses for some of them.

You can see an auto-claim activity report that shows license assignments made for the preceding 90 days. Note that once a user has been assigned a license through auto-claim, they keep that license unless you manually remove it; turning the auto-claim policy off (or disabling auto-claim in **Settings > Org settings**) doesn't remove previous license assignments.

For more information, read [this article](#).

Managing User Role Assignments

Microsoft 365 (and some of its key workloads, notably Exchange Online and Entra ID) offers customers a variety of administrative roles that you can assign to users who need to perform management tasks. Much like on-premises environments, there is no single “admin” level permission that someone needs to perform some management tasks for your tenant should have. Instead, a set of pre-configured administrative roles and groups is available to allow the assignment of limited but necessary permissions to administrators to do their job. This model is called role-based access control (RBAC). Keep in mind that the service and workload-specific roles are different from the Azure roles that you may wish to assign; for more information on Entra ID role management, see [Microsoft’s documentation](#).

Assigning Administrative Roles to Users

There are several ways to assign a privileged role to a user. The easiest way is probably to select and edit their account in the Microsoft 365 admin center. You can then assign an administrative role to the user by clicking the **Manage Roles** link on the user settings page. You can also use the Roles section in the Entra admin center to assign some roles, or even break out the [Microsoft Graph PowerShell](#) module and do it from the command line.

By default, only the first account created when you sign up a new tenant receives any level of admin access. That initial account, which is homed in the cloud, is assigned the **Global admin** role. It will remain permanently available unless you delete it. You should keep at least one cloud-based Global admin account available so that you can log in even if AD FS or Azure AD Connect is broken for your tenant.

Global admin holders get complete administrative access to all features within Microsoft 365, including individual services such as Exchange Online and Teams. Naturally, every organization will have at least one Global admin. While having too many of these accounts is a security problem, it’s a good idea to keep multiple accounts to give you redundancy in case the one person with administrator permissions isn’t available when you need them.

Assigning Roles through Groups

If your tenant has Entra ID P1 or P2 licenses, you can [assign Entra ID roles to groups](#). This is a little more complex than the way that you’d accomplish the same task with on-premises AD. You must create the group in Entra ID, then select the **Microsoft Entra roles can be assigned to the group** option (which changes the *isAssignableToRole* property on the group object). Then you can assign roles to the group, then add users to the group. *isAssignableToRole* is an immutable property, so you cannot role-enable existing groups, and you cannot disable role assignment from a group once you’ve set this flag.

By default, only Global Administrators and Privileged Role Administrators can create groups with this flag set or manage the membership of such groups. Although you can delegate this ability, you should be careful when doing so to prevent accidentally giving people excess privileges. For the same reason, you cannot use dynamic groups with role assignments; all assignments to role-enabled groups must be done manually. These groups can be managed through the Microsoft Graph, provided that the caller has the *RoleManagement.ReadWrite.All* permission; the ordinary *Groups.ReadWrite.All* permission won’t work.

Assigning Roles Directly to Users

In the user management interface, you can assign a user to the **Global Administrator** role or assign them to one or more customized administrator roles (Figure 4-4). When you assign a user to one of these roles you must give an alternative email address for them to use when they need to recover a lost password for their admin account.

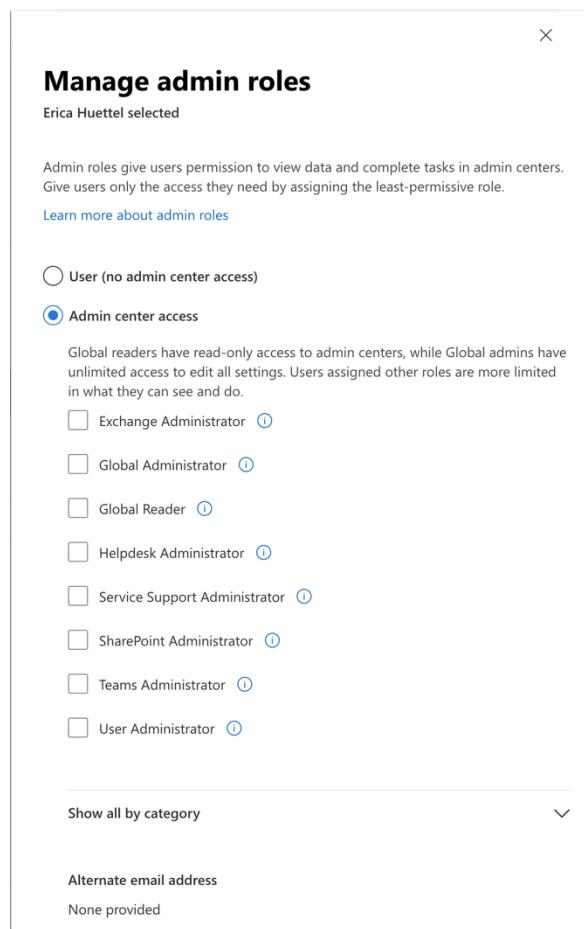


Figure 4-4: Assigning administrative roles to a user account

Understanding the Built-In Roles

The familiar security principle of “least privilege” dictates that you should only grant users whatever limited admin access is necessary for them to do their job. With more than 80 roles scattered throughout the Microsoft Entra and Microsoft 365 admin centers, it can be difficult to track which roles do what, or even what all the roles *are*. Microsoft groups these roles into two basic groups: the first group (labeled with “Admin center access”) grants access to specific admin centers in the Microsoft 365 ecosystem:

- **Global Administrator:** you already know what this is—the all-powerful master administrator account that can do anything, anywhere, within the tenant.
- **Exchange Administrator:** Users with this role use the Exchange Online admin center to manage mailboxes, groups, anti-spam policies, and access activity reports in the Microsoft 365 admin center. An Exchange Admin becomes an Organization Management role group member in Exchange Online, which is a high privilege role group. Exchange Online has a more granular permissions model known as Role-Based Access Control (RBAC), which you can use to assign least privilege permissions instead. RBAC is discussed later.
- **Global reader:** this is like the old “Exchange view-only administrator” role in on-premises Exchange; users who hold this role can read, but not change, most non-security-related settings in both Entra ID and Microsoft 365. The Global reader role works with Microsoft 365 admin center, Exchange admin center, Teams admin center, Defender portal, Compliance portal, Entra admin center, and the Device Management admin center. You may find that it doesn’t completely work with all workloads.
- **Helpdesk administrator:** Delegating responsibility for password resets can relieve some of the support burden from IT teams. Many processes created to reset user passwords involve the need for an authorized person to check the identity of the user before any change is made to their password,

for example by having them walk up to their desk and show a company identification badge. Once the user is recognized, the authorized person sends the request to the help desk. Giving that authorized person the right to reset the password themselves can save time. However, there is no granularity when it comes to assigning this admin role through the Microsoft 365 admin center. Helpdesk admins can reset any other user or helpdesk administrator's password, but not other types of admin users. They could reset the password for someone in a completely different location, or someone whose identity is unverified. As such it is important to be careful to only assign this role to trusted individuals.

- **Service support administrator:** Formerly known as the Service admin role, this role grants the ability to manage service requests and to access the Service Health Dashboard. You should assign this role to users who are members of the Exchange administrator, Teams administrator, or SharePoint administrator groups to allow them to raise support tickets for those services. The role also gives the holder read-only access to information about groups, users, and licenses, which means that it is a good role to assign to people who want to know about license usage within a tenant. Interestingly, Microsoft changed the name of this role to match the role name in the Microsoft Graph API, rather than leaving the UI alone and changing the role name in the API definition.
- **SharePoint Administrator:** This role grants the ability to manage SharePoint Online, which also affects OneDrive for Business, as well as creating and managing sites, and managing user profiles. SharePoint admins can assign other users with administrative permissions within SharePoint Online for sites and term stores. They can also access activity reports in the Microsoft 365 admin portal.
- **Teams Administrator:** Users with this role can manage all aspects of Teams (including policies and calling) but cannot assign or remove user licenses. They can also manage Microsoft 365 Groups, which makes sense given how Teams uses them.
- **User Administrator:** This role can manage users, groups, passwords, service requests, and see the Service Health Dashboard. This admin role is ideal for a help desk or low-level support person. Although a User admin role holder can remove other user accounts, they cannot remove the account belonging to a Global admin nor can they reset passwords for Billing admins, Global admins, User experience success managers, or Service admins.

Other admin roles are grouped according to service category (e.g., "Collaboration", "Devices," and "Identity"). Microsoft is continually moving and adding roles as they expand the set of supported role features. There are currently more than 80 individual roles, the details of which you can find [documented here](#).

Creating Custom Roles

In addition to the built-in roles, you can create your own custom roles in Entra ID. These custom roles draw from the same set of permissions as the built-in roles—think of the built-in permissions as a deck of cards from which you can draw the specific cards you want to. You can't make up a new "13 of diamonds" card, and you can't make up your own new permission, but you can combine permissions into custom roles that grant exactly the access you want to grant to role holders. To create custom roles, you must have Entra ID P1 or P2 licenses. The mechanics of setting up custom roles will be familiar to anyone who's used custom roles in Exchange on-premises or Exchange Online: first you create a new role, then you add permissions to the role, then you assign the role to users. You can create these roles using the Entra admin center, PowerShell via the `New-MgDirectoryRole` cmdlet, or through Microsoft Graph. All 3 approaches are [documented here](#).

Using the Roles Section of the Admin center

The Roles section in the Microsoft 365 admin center may be easier to use for assigning roles, because it gives you a single list of all the supported roles and allows you to filter, search, and sort them. You can export a CSV file showing which users have been granted roles in the tenant, or you can see and change

assignments for any individual role. Clicking on a role will give you a short list of capabilities the role has, plus tabs for viewing and changing user assignments and viewing a comprehensive list of the role's permissions (which, sadly, you cannot change).

The Roles page uses multiple pivots (or tabs) at the page top. All the Entra ID roles are on the Entra ID pivot, while Exchange roles are on the Exchange pivot. Microsoft will occasionally add or remove pivots here as they make changes to the admin centers.

Listing Who Holds Administrative Roles

The list of roles above may not be exhaustive because Microsoft adds new roles over time. To find the full set of currently known roles active in your tenant, and the people who hold these roles, you can run this PowerShell code:

```
[array]$Roles = Get-MgDirectoryRole | Sort-Object displayName
ForEach ($Role in $Roles) {
    [array]$RoleMembers = Get-MgDirectoryRoleMember -DirectoryRoleId $Role.Id
    If ($RoleMembers) {
        Write-Host ("Members of the {0} directory role" -f $Role.displayName)
        $RoleMembers.additionalProperties.displayName
    }
}
```

You can assign administrative roles to licensed or unlicensed users. An unlicensed user does not have access to any licensed feature, such as an Exchange Online mailbox or being able to install the Microsoft 365 apps for enterprise on their computer. However, they can log in to admin portals and use PowerShell to perform management tasks. Administrators who perform content searches and want to preview search results need an Exchange Online mailbox to be able to see the results. In general, third-party services and tools that require the use of privileged or service accounts are likely to send mail to those accounts, so be sure you're paying attention to their mailboxes.

Note: Microsoft 365 uses the alternative email address for account recovery if the password for the account is lost. In some cases, the alternative email address is needed when the administrator is unable to access their account or mailbox at all. Therefore, it is best to use an email address that is independent of the tenant. This raises some obvious security concerns; someone could use the alternative email address to reset the password for the administrator account. You should ensure that the alternative email address is well protected by a strong password and multi-factor authentication. Services such as Outlook.com or Gmail can offer the necessary level of security.

Exchange Online Administrative Roles

Exchange Online has its own administrative roles or management role groups, some of which link to Microsoft 365 admin roles and others that are independent. You can see the Exchange Online admin roles by logging in to the Exchange admin center and navigating to the **Roles > Admin roles** section.

Global admins automatically have Organization Management rights in Exchange Online. Users assigned the Global admin role join an Exchange Online role group called **TenantAdmins_xxxxx**, where the last five characters in the group name are unique to your tenant. The TenantAdmins group is nested in the Organization Management role group and is displayed as **Company Administrators**. Organization Management is a powerful admin role that has access to manage all the features of Exchange Online, so you can see why the Global admin role should only be assigned to selected administrators in your organization.

Users who get the Exchange administrator role also automatically have Organization Management rights in Exchange Online. From an Exchange Online perspective, this is the same level of admin rights that a Global

admin receives, but an Exchange service administrator is not granted any other admin rights within Microsoft 365 itself, such as managing billing, subscriptions, or domain names.

Helpdesk Administrator holders are automatically granted View-Only Organization Management rights in Exchange Online. Users assigned the Password admin role join an Exchange Online role group called **HelpdeskAdmins_xxxxx**. The HelpdeskAdmins group is nested in the View-Only Organization Management role group and is displayed as **Helpdesk Administrator**. This role group can view the configuration and recipient details within Exchange Online but can't make any modifications, other than resetting user passwords.

Note: You might notice in the Exchange admin center that a View-Only Organization Management role group member can create distribution lists and manage distribution lists that they have created. This is due to the default role assignment policy for users in Exchange Online which permits anyone to create and manage their distribution lists.

Aside from the Exchange Online admin roles inherited from admin roles, several other Exchange Online role groups also exist for granularly assigning rights to different users within your organization:

- **Compliance Management** – members of this role group can manage Data Loss Prevention, Information Rights Management, and Retention. In addition, members of this role group can view audit logs as well as all configuration and recipient attributes in the organization. Managing features such as DLP and IRM is often part of a more general security and information compliance role in an organization, not necessarily a duty performed solely by Exchange administrators, and this role group allows those users to be assigned the admin rights they need without having broader Exchange admin rights. Note that a separate set of roles govern access to the Purview compliance portal, discussed later.
- **Discovery Management** - members of this role group can configure legal hold on mailboxes. Microsoft has deprecated the eDiscovery experience in EAC (and it isn't even present in the modern EAC) in favor of using the Purview toolset, so you may not run into this role much in the future.
- **Help Desk** – members of this role group can view and manage the same individual recipient attributes that the users can view and manage for themselves. For example, users can log in to OWA and change personal details such as their phone number and street address or update their password. Help Desk role group members can therefore also change the user's phone number, street address, or reset their password. This role group is suitable for low-level support staff, or for service accounts that automatically synchronize attributes such as phone numbers and street addresses from other systems such as an HR database.
- **Hygiene Management** – members of this role group have view-only access to Exchange configuration and recipients, and they have permission to manage some aspects of the transport system, mostly settings for anti-spam and anti-malware filtering, which are actually now in the Defender portal. You'll normally assign this role to people who manage your anti-malware appliances or services, and perhaps to select members of your organization's security team.
- **Organization Management** – members of this role group have access to manage all features of Exchange Online, except for the rights that the Discovery Management role group allows. As discussed earlier, Global admins and Exchange service administrators are automatically made members of this role group. You can also assign membership of this directly in Exchange Online, but you may find it better to assign the Exchange service administrator role instead as this will force the addition of an alternative email address for lost password recovery.
- **Recipient Management** – members of this role group have access to manage recipient objects in Exchange Online. Recipient objects include user mailboxes, shared mailboxes, group mailboxes, resource mailboxes, distribution lists, contacts, and other mail-enabled objects. Recipient Management members can also perform mailbox migrations, message traces, and reset passwords.

This role group is ideal for day-to-day tenant administration and is often assigned to first and second-level support teams. However, it is also suitable for general use by higher-level administrators who want to separate their admin accounts into low and high privilege use. For example, a Global admin or Exchange service administrator may have a separate admin account that is only granted Recipient Management rights. They can use the low privilege account for general administrative tasks, running report scripts, and so on, and only log on to the higher privilege account for the less frequent tasks that require those higher admin rights.

- **Records Management** – members of this role group are granted rights to perform compliance-related tasks such as configuring or viewing audit logs, configuring journaling, performing message traces, managing retention policies, and configuring transport rules.
- **Security Administrator, Compliance Management, Global Reader, Security Operator, and Security Reader** – although you will see these role groups in the Exchange admin center, they only appear here because the role groups are used across multiple Microsoft products (including Information Protection and the Purview portal). The Security Reader role group grants read-only access to Entra ID, Entra Identity Protection, Entra Privileged Identity Management, and all audit logs and sign-in reports. The Security Administrator role group grants the same access as Security Reader, plus the ability to configure security services. In particular, the Security Admin role can be used to block Copilot for Security from ingesting settings and audit data from Microsoft 365 services if you should want to do so. You won't manage membership in these role groups yourself; instead, you'll assign access to the services, and when you do, the role group membership will be automatically updated.
- **Investigators, Analysts, and Readers** – several of the Defender, Purview, Entra, and Priva products add roles for their own specific coverages, where the suffix designates how much privilege is granted to the defined role. For example, the Insider Risk Management Admins role goes with the [Purview Insider Risk Management](#) license, as does Insider Risk Management Analyst. The difference between the two is that the Analyst role can't see or change most of the related settings for the feature.
- **View-Only Organization Management** – this role group gives read-only access to all recipient properties and configuration settings for the organization. This role group is ideal for anyone who needs broad visibility of the organization without the right to make changes. One scenario where this level of access is useful is for reporting scripts and tools that need to be able to read a wide range of information about the organization.

As you can see, a wide range of pre-configured administrative roles exists in Exchange Online to suit different requirements. Keep in mind that sometimes these roles don't align well across services, and you may need to carefully check to ensure that roles you assign in Entra ID deliver the right level of access for individual applications that may piggyback on those role definitions.

Assigning Security- and Compliance-Related Roles

The security and compliance features in Microsoft 365 support a set of permissions defined in RBAC role groups that allow the separation of responsibilities across different sets of users. The role groups are like those used by Exchange Online, except that these role groups only apply to the functionality available through the Defender and Purview portals and have no connection to the role groups used by Exchange Online, even though some of them share the same name.

To see the definitive version of the available roles and to assign or remove roles to users, go to the appropriate section of the Microsoft Purview portal (gear icon in the top nav bar, then **Roles and scopes**) or the Microsoft 365 Defender portal (see the tenant administration chapter if you need a refresher on the difference between these two). Each of these admin centers has its own set of roles, and if you're using the [Defender-centric RBAC model](#) you'll notice some significant differences. There are also some roles associated

with Entra ID that will be displayed in these admin centers but must be managed through the Entra admin center. Microsoft also maintains [documentation listing all the roles and their capabilities](#).

Here's a partial list of the roles you can assign to users:

- **Reviewer** - members of this role group can view the list of e-discovery cases that currently exist. Case managers can assign specific documents in an eDiscovery case for a reviewer to analyze or use a limited set of the analysis features in Microsoft Purview. Members of this group can see only the documents that are assigned to them.
- **Records Management** – members of this role group can manage retention and compliance features related to how long user data is stored and what policies are applied and enforced to archive or expire it.
- **Security Operator** – members of this role group can manage security alerts, view security reports, and view security settings.
- **Insider Risk Management** – members of this role group can manage and control the insider risk policies applied to users in a tenant.
- **Compliance Data Administrator** – members of this role group are typically IT administrators who are responsible for configuring security and compliance settings and policies, such as mobile device management, DLP, and preservation. Compliance administrators can also manage settings for reports in the Compliance portal.
- **Security Administrator** - membership of this role group is not intended to be managed by you directly through the security or compliance portals (although you can do so). Instead, Microsoft intends you to grant users access through the Security Administrators role. This role group may include Microsoft Support or external partners.
- **Security Operator** - this allows holders to read security reports, manage alerts, manage the tenant allow/block list, and view all security settings, but they can't change most of them.
- **Compliance Administrator** – identical to the Compliance Data Administrator role, except that holders cannot manage data loss prevention settings.
- **Security Reader** - like the Security Administrator role, this role group is not intended to be managed by you. It gives read-only access to security and compliance features.
- **Supervisory Review** - members of this role group can create supervisory review policies for the organization, which determine the type of content that will be subject to supervisory review, and who will be performing the reviews.
- **Organization Management** - members of this role group can perform the same tasks as Compliance Administrators. They can also configure permissions for the Compliance portal and configure audit logging for the organization. Global admins are automatically added to this role group.
- **Mailflow Administrator** - this role group grants its members access to the mail flow dashboard. Users who are members of the Global admin or Exchange admin role groups will already have access to this dashboard, but if you grant membership in Mailflow Administrator to users they will only have access to the dashboard, not to other Exchange or Microsoft 365 management features.
- **eDiscovery Manager** - members of this role group can perform searches across workloads, and apply holds to Exchange Online mailboxes, SharePoint Online sites, and OneDrive for Business libraries. An eDiscovery Manager has access to specific eDiscovery cases. When you grant a user the eDiscovery Manager permission, you can also grant them eDiscovery Administrator privileges, which allows the user to view and edit all eDiscovery cases for the organization.
- **Data Investigator** – a new role group whose holders can perform mailbox, SharePoint, and OneDrive searches using the new investigation features in the Compliance portal.
- **Global Reader** – this role group allows the holder to read all reports, alerts, and settings for security and compliance features, similar in concept to how Exchange View-Only Administrator works.

- **Quarantine Administrator** - This role allows holders to manage mail quarantine settings and items in the Compliance portal.

You can create custom role groups. The **Create** button on the Permissions page allows you to create a new role group by specifying the base roles you want to use for the new role group, then assigning it to a set of users. It's important to know that your custom role group will get all the privileges assigned to the base roles you pick—there's no way to remove a specific privilege from the roles you create.

Like any other role assignment, the tenant administrator should review what accounts hold which roles regularly to ensure that users do not retain privileged access for longer than required. The eDiscovery Manager role group is particularly powerful because of the two sub-roles that it contains. eDiscovery Managers have access to all their assigned cases. eDiscovery Administrators have access to all cases and can assign themselves to a case. Although dependent on the volume of eDiscovery workload within the tenant, the usual situation is to have only a few eDiscovery Administrators and more eDiscovery Managers. However, in a small tenant, the same people might comprise the two groups.

Administrative Units

Administrative units (AUs) are containers for objects, like organizational units on-premises. AUs allow you to group your users into logical units, then scope management tasks to the AU instead of the entire organization. For example, you could create an AU for all the users in the Sales department, or all users working in Slovakia; then you could grant permission for an ordinary user (let's call her Dagny) to perform user management tasks only on the users in a specific AU.

Like on-premises OUs, the real power of AUs is the ability to give Dagny permission to perform various tasks against *only those users* who are in the scope of an AU. This is very important for large organizations. The limited-scope admin roles (such as Exchange administrator) that exist control *what* their holders can do, but they don't restrict *which users* those role holders can manage.

The simplest way to create AUs is to use the Entra admin center, as [described here](#). One nice optimization to this process is that you can create role assignments scoped to the group at the time you create the group itself. Of course, you can also create those role assignments separately by editing the properties of the AU in the Entra admin center.

After you've created the group, you need to [add members](#) (which can be users or device objects).

Finally, you need to add role assignments that are scoped to the AU. The result is that Dagny, or whoever else has been granted permissions on the AU, can exercise the privileges of the assigned role, but only on users who are in the targeted administrative unit. The Microsoft 365 Admin center will filter out any users who aren't in the selected AUs, so Dagny won't even see them. If Dagny uses PowerShell instead, she will see users who are out of scope for her AU permissions, but she can't modify them; role scoping only applies to write operations.

If you prefer to manage your AUs with PowerShell, you can; the documentation linked above has examples for each of the cmdlets you'll need to use.

Managing Privileged Accounts

Best practice in the Windows community is to perform administrative actions with dedicated administrator accounts rather than assigning the necessary permissions to user accounts. This is done to restrict permissions to a limited set of accounts rather than allowing for user accounts to gather a proliferation of permissions, sometimes for doubtful reasons. It also ensures that you do not have to perform regular reviews of highly permissioned accounts to remove permissions from accounts that do not need them.

Inside the Microsoft data centers, very few administrators have elevated permissions, and great care is taken to ensure that permissions are only granted when needed and for a minimum period and that they are only used from privileged access workstations (PAWs), dedicated computers specifically configured for high security.

You can certainly bring the practice of using dedicated accounts for administrative tasks forward into Microsoft 365. However, given that the service is a very different environment that hosts many different workloads and the need for permissioned access is reduced because there are fewer administrative tasks to perform (no server management, for instance), perhaps this is a good time to consider whether a better approach could be taken.

Privileged Identity Management

Microsoft offers two features to manage privileged access to user information. The first is [Entra ID Privileged Identity Management \(PIM\)](#), a framework for the management of privileged access to applications that depend on Entra ID, such as Microsoft 365. Using PIM, you can manage temporary or permanent elevation of user accounts to grant administrative privileges, such as Global Administrator. A user can be permanently eligible to elevate their permissions, or you can require the user to request approval each time they require elevated permissions. PIM will elevate the user's permissions for the time needed, then revoke the permissions afterward. Added controls such as enforcing multi-factor authentication (MFA) are also available in PIM, as well as an audit trail and activity report. PIM is available for customers who have Entra ID P2 licenses, whether bundled with the Enterprise Mobility + Security E5 license or purchased separately, or customers who purchase the separate Entra ID Governance license.

Privileged Access Management

The second feature is Purview [Privileged Access Management](#) (PAM), which is generally available for Exchange Online. Other workloads will be added over time. Microsoft considers PAM to be a compliance feature now, so each user who requests or responds to a PAM request must have either an E5-equivalent (the Office 365 or Microsoft 365 E5, A5, G5, etc. SKUs) or an E3 license plus the Microsoft 365 E5 Compliance or Microsoft 365 E5 Insider Risk Management licenses.

PAM works on the basis that administrators create requests for authorization when they want to perform privileged tasks. Policies controlling individual cmdlets or RBAC roles or role groups state whether requests receive automatic approval or need manual review. These requests are routed to a set of approvers (a mail-enabled security group). Anyone in the group can approve a request through the Microsoft 365 Admin Center or with PowerShell. Once approved, the requester can execute the task for as long as the approval still is valid (the default is four hours).

In addition to considering who has permissions, you should also take steps to check the use of permissions through auditing. The audit log collects a vast array of events for administrative and user actions. You can use the audit log search in the Compliance portal to examine these events and export them for later analysis should the need arise.

Managing Exchange Online Mailboxes

Early email systems only supported user mailboxes. Today's email systems are a lot more sophisticated and support many different mail-enabled objects designed for different purposes. Exchange Online supports the following recipient types:

- User mailboxes.
- Shared mailboxes.

- Room and resource mailboxes.
- Distribution lists.
- Public folders and public folder mailboxes.
- Mail contacts and mail users.
- Group mailboxes (used by Groups and Teams).
- Scheduling mailbox (for internal use only).

Exchange Online uses but does not allow tenant administrators access to system mailboxes. These mailboxes include arbitration mailboxes, such as that used to generate the Offline Address Book, the health mailboxes used by Managed Availability probes, and mailboxes created for system test purposes. On the other hand, the Exchange Online mailboxes you can manage have some unique characteristics not found on-premises, many of which we will meet here.

The Link Between EXODS and Entra ID

Mail-enabled objects, including user mailboxes and groups, exist in both the Exchange Online directory service (EXODS) and Entra ID. This arrangement allows Exchange to control some extra properties for mail-enabled objects over and above the set available in Entra ID, but it also creates the necessity to process many attribute changes in two places—once to each copy. Background processes synchronize EXODS and Entra ID. These processes use an identifier called *ExternalDirectoryObjectId* stamped on EXODS objects to link to Entra ID. The identifier does not feature in on-premises Exchange, but its importance is high enough for Exchange Online to display it as a default property when you run the *Get-ExoMailbox* cmdlet:

```
Get-ExoMailbox -Identity Tony.Redmond

ExternalDirectoryObjectId : eff4cd58-1bb8-4899-94de-795f656b4a18
UserPrincipalName       : Tony.Redmond@office365itpros.com
Alias                  : Tony.Redmond
DisplayName            : Tony Redmond
```

Exchange cmdlets accept the *ExternalDirectoryObjectId* as a valid identity. In other words, this works:

```
Get-ExoMailbox -Identity eff4cd58-1bb8-4899-94de-795f656b4a18
```

Because the property holds the Entra ID object identifier, PowerShell cmdlets from other modules can use the *ExternalDirectoryObjectId*. For example, this snippet retrieves the *ExternalDirectoryObjectId* for a mailbox and uses it to fetch information about the Entra ID user account to which the mailbox belongs.

```
$ObjectId = (Get-ExoMailbox -Identity Kim.Akers).ExternalDirectoryObjectId
Get-MgUser -UserId $ObjectId
```

The same technique works for Groups. In this example, we use the *ExternalDirectoryObjectId* to list the members of a group.

```
$ObjectId = (Get-UnifiedGroup -Identity ExchangeGoms).ExternalDirectoryObjectId
[array]$Members = Get-MgGroupMember -GroupId $ObjectId
ForEach ($Member in $Members) {Get-MgUser -UserId $Member.Id | Select -ExpandProperty DisplayName}
```

When an *ExternalDirectoryObjectId* is unavailable for an Exchange object, it means that the object is specific to Exchange and doesn't exist in Entra ID. Dynamic distribution lists are the best example of such an object.

User Mailboxes

An on-premises Exchange administrator who begins working with Exchange Online mailboxes won't notice much difference between cloud mailboxes and their on-premises counterparts. You can't manage databases or move mailboxes around because Microsoft takes care of these activities, but the essentials of managing

mailbox properties are similar. Many of the techniques used to work with mailboxes through the EAC or PowerShell are the same on both platforms.

Some features available on-premises are not in Exchange Online. The cmdlet extension agent is an example. This agent often runs in on-premises deployments to automate the population of mailbox properties during the creation of a new mailbox. For instance, you might set the time zone and language for a mailbox so that its owner has a seamless introduction to OWA the first time they access their mailbox.

Because Microsoft 365 is a massive multi-tenant infrastructure, it is logical that Microsoft imposes some throttles and controls over the resources that an individual user can consume, the size of mailboxes, and the volume and type of messages that the system handles. These limits exist to protect the integrity and performance of Exchange Online and are [documented online](#). Microsoft reviews the limits regularly and updates them in line with experience and user demand. You should acquaint yourself with these limits as they might influence the details of your deployment.

Data Caching: Exchange Online is a very different environment to an Exchange on-premises deployment, so it would be unreasonable to expect that everything will work the same. Caching is an example. Sometimes a change that you make to an object takes a few seconds – or even a few minutes – to be effective throughout Exchange Online. It might even take some time for a new object to appear because of the need for synchronization across different parts of Microsoft 365. This is quite normal and is a side-effect of the caching of data to improve performance and responsiveness within the service. The change or new object will appear eventually. Just have faith!

Creating a New Mailbox

Because cloud mailboxes must have a Microsoft 365 account, the EAC does not include the ability to create a new mailbox. You can:

- Create a new account through the Microsoft 365 admin center and assign it an Exchange Online license. The mailbox is available a few moments after you create the account.
- Create mailboxes on-premises and synchronize them with Entra ID using a tool like AADConnect (hybrid mailboxes).
- Create a new account and mailbox through PowerShell.

Apart from instructing Exchange to create a mailbox for an account, the Exchange Online license assigned to an account controls some mailbox settings, such as its storage quota and access to other products such as SharePoint Online. [More information](#) is available online about the consequences of assigning or removing licenses to or from accounts. If you create accounts with PowerShell, you must make sure that the new accounts are fully provisioned and licensed. Accounts created without a license will not be able to access any applications until they become licensed.

Once created, you can change the settings for Exchange Online mailboxes through the Microsoft 365 admin center, EAC, or PowerShell. Management of the settings for hybrid mailboxes always happens through the on-premises environment. One major difference between on-premises and cloud mailboxes is that Exchange Online does not apply naming policies to new objects. In practical terms, this means that you cannot control the format of display names. If your company organizes address lists using the last name, and first name convention, you must input the display name according to that policy or run a fix-up script afterward to ensure that all mailboxes follow the same naming convention.

Display Names: There are many places where Microsoft 365 applications display user photos if available in the user account. If not, initials taken from the display name serve as a fallback. For instance, the user photo for the user Paul Robichaux will display PR. However, if you use the last name and first name

convention for display names, the user photo displays RP. The apparently “wrong” choice of initials can be hard for users to understand.

Editing a Cloud Mailbox

Many of the properties of Exchange Online mailboxes, including permissions, forwarding settings, and visibility in the GAL, can be set through the Microsoft 365 admin center. If you need access to the full set of mailbox properties, click the **Edit Exchange properties** link in the properties dialog to open the EAC mailbox properties page. At this point in the evolution of Exchange Online, you might rarely if ever go to the EAC for anything, as most of the things you might commonly manage are available elsewhere.

A note on mailbox names: Microsoft’s help suggests that *“The user’s alias is the portion of the email address on the left side of the @ symbol. It must be unique in your organization.”* While aliases were required to be unique, the *Name* parameter of the object could sometimes be identical between different objects because in some cases Microsoft would just copy the alias for the object into the *Name* field. Microsoft [announced that this behavior was changing](#) so that the *Name* field would always contain a globally unique ID. After delaying the change, they completed it for the worldwide and 21Vianet clouds as of April 2023; it remains paused for all other clouds as of September 2024.

Creating a Mailbox with PowerShell

PowerShell is often used to script the creation of new user accounts and mailboxes because it allows companies to tie the creation of an account into other processes, such as the creation of a new HR record and access records, the printing of an employee badge, and so on. On-premises administrators are familiar with the concept of creating and updating mailboxes with PowerShell because the *New-Mailbox* cmdlet has been used for this purpose for well over ten years. The *New-Mailbox* cmdlet exists in Exchange Online but the environment in which it functions is very different, largely because of the multi-tenant nature of Microsoft 365 and the need to license users before they can access functionality. Exchange Online strictly enforces the need for mailboxes to be licensed and will remove unlicensed mailboxes if they don’t get a license within 30 days of creation. Thus, you cannot take scripts used to create mailboxes on-premises and expect to be able to use them with Exchange Online. Invariably, some adjustment is necessary, if only to assign a license to a new mailbox immediately after its creation.

One point of difference you need to be aware of is the difference between a mailbox and a remote mailbox. You know what a mailbox is: it’s homed either in the cloud or on-premises, in the same location as its associated account object. A remote mailbox is a cloud mailbox associated with a mail user object that’s stored in an on-premises Active Directory. You’ll create remote mailboxes when you want your users anchored in on-premises AD but their mailboxes in Exchange Online. Most likely, this will already have been done for you as part of your migration to Exchange Online.

It is not the intention to discuss how to use PowerShell to create Exchange Online mailboxes or how to write a bulk mailbox creation process (the Microsoft 365 admin center includes [an option for bulk account creation](#)). A scan of the Internet will provide many examples of code that you can examine and repurpose to suit your needs, including some from Microsoft (for instance, [a script to create multiple mailboxes](#) is available as is one to [assign licenses to multiple mailboxes](#)). Instead, this walkthrough will help you understand the differences that exist between Exchange on-premises and Exchange Online.

Creating a Cloud Mailbox for an On-Premises User

Remember that if you run a hybrid deployment, the on-premises environment is always the master, and Entra ID is the replica. Mailboxes and user accounts are created on-premises and then synchronized to Entra ID. However, even if you run a hybrid deployment and will never create cloud-based mailboxes, it’s good to

understand what happens when creating a new cloud mailbox from scratch. The basic steps in the process are as follows:

1. Make sure that your PowerShell session loads the necessary modules. You need to load both the ExchangeOnlineManagement and Microsoft Graph PowerShell SDK modules to create mailboxes and manipulate the underlying Entra ID objects. See the PowerShell book if you need more background on this.
2. Run the *Enable-RemoteMailbox* cmdlet to create a new user account and its Exchange Online mailbox.
3. Run the *Set-User* cmdlet to update the on-premises directory with the organizational and personal settings for the user object.
4. Run the *Update-MgUser* cmdlet to set the correct country code (location) for the new mailbox in the cloud. You assign a country to a user account to ensure that Microsoft 365 makes the services designated for that country available to the user. For example:

```
Update-MgUser -UserId Kim.Akers@Office365itpros.com -PreferredDataLocation DE
```

5. Assign a license to the user.

Creating a new mailbox with the *New-Mailbox* cmdlet on an on-premises Exchange server usually completes in a matter of seconds. The same is not true for Exchange Online. Although the cmdlet and syntax are the same, the creation of the new object across EXODS and Entra ID takes some time to synchronize across the directories.

Creating a Cloud-Only Mailbox

You may want to create an Exchange Online mailbox for a user account that's stored in Entra ID. This is easy to do in the Microsoft 365 admin center, but if you want to do it with PowerShell, it is easily accomplished with the *New-Mailbox* cmdlet and the accompanying *-MicrosoftOnlineServicesId* parameter. For example:

```
New-Mailbox -alias paulr -MicrosoftOnlineServicesId paulr@Office365itpros.com
```

Updating Mailbox Attributes

Some of the attributes commonly populated for mailboxes are not set with the *New-Mailbox* or *Set-Mailbox* cmdlets. These are attributes controlled by Entra ID and are common to all Exchange recipient objects, whether they have a mailbox, and are updated with the *Set-User* cmdlet. As it happens, many of these attributes are useful when creating filters to create dynamic distribution lists or address lists, so it is important to give some attention to making sure that they hold the correct values. For example, the code shown below updates the user object for the mailbox that we just created with the organizational and personal information that you might expect to find in the corporate directory. The example shown here updates several properties, including the *Manager* property with a value that points to the name of the new user's direct manager. The update will fail if Entra ID cannot find the manager.

```
Set-User -Identity "Kim Akers" -City "Dublin" -CountryOrRegion "Ireland" -Department "Marketing Operations" -Title "VP Marketing (New Products)" -Manager "Paul.Robichaux" -Office "Dublin HQ" -Company "Popular Books"
```

Once the new mailbox exists, you can update its settings with *Set-Mailbox* and other cmdlets. For instance, here is how to enable an archive mailbox with the *Enable-Mailbox* cmdlet.

```
Enable-Mailbox -Identity "Kim Akers" -Archive
```

Add User Photos to Mailboxes

Given the graphic nature of Microsoft 365 applications, it's a good idea to update a new mailbox with a suitable photo after it's created. The photo then shows up in the GAL, the people card, and apps like Teams

that display user profile pictures. In the past, the Exchange *Get/Set/Remove-UserPhoto* cmdlets were the best way to manage photos for users and Microsoft 365 groups, but Microsoft deprecated those in 2023. The currently supported method uses the Microsoft Graph PowerShell SDK cmdlets described below to manage user photo information stored in Entra ID. Switching cmdlets doesn't affect controls that applications place over user ability to update photos. For instance, the *SetPhotoEnabled* setting in OWA mailbox policies (see below) continues to control if users can update their photos through OWA.

These cmdlets from the Microsoft Graph PowerShell SDK manage photos for user accounts:

- *Set-MgUserPhotoContent*. Update the photo data for a user account.
- *Get-MgUserPhoto*. Retrieve the photo data for a user account.
- *Remove-MgUserPhoto*. Remove the photo data for a user account.

You cannot update photos for other mail-enabled objects, like distribution lists or mail contacts. For example:

```
# Check if account has a photo
Get-MgUserPhoto -UserId Jim.Smith@Office365itpros.com
# Update account with photo
Set-MgUserPhotoContent -UserId Jane.Doe@office365itpros.com -Infile "c:\temp\JaneDoe.jpeg"
```

These cmdlets manage photos for Microsoft 365 groups:

- *Set-MgGroupPhotoContent*.
- *Get-MgGroupPhoto*.
- *Remove-MgGroupPhoto*.

Alternatively, the Teams *Set-TeamPicture* cmdlet updates the photo data for a team. This is analogous to running *Set-MgGroupPhotoContent* to update the photo for a group mailbox.

Image files for user photos can be in JPEG or PNG format and should be less than 4 MB. Behind the scenes, Entra ID stores the highest possible resolution image. Workloads access Entra ID to fetch photos in whatever format they need. For instance, to display thumbnails of users when showing group membership or fetch a high-resolution for use in a Teams meeting.

An example of how to scan user mailboxes to [find and update mailboxes without photos can be downloaded from GitHub](#).

Allow Users to Update Their Photos

Exchange Online, Teams, and other workloads allow users to update their photos. This capability is controlled by the *SetPhotoEnabled* setting in the OWA mailbox policy assigned to the user's mailbox. The use of OWA mailbox policies means that organizations can decide to allow some users to manage their photos while barring others from doing so. In the latter case, the organization takes responsibility for updating user photos by:

- Building a connection to a system holding suitable photos, like an HR system.
- Building a special app to manage user photos (although Microsoft is deprecating the relevant Exchange Web Services APIs).
- Using commercial or freeware software, like [CodeTwo User Photos for Office 365](#) (freeware).

By default, the *SetPhotoEnabled* setting is *\$true*, meaning that users can upload a photo from apps. If this setting is off (as it may be in a legacy tenant) users will see a message such as "*picture options are disabled by policy*" if they try to change their photo. To allow users to upload and update their photos, either:

- Update the OWA mailbox policies so that *SetPhotoEnabled* is *\$True* in all policies, or:

- Create or update an OWA mailbox policy with `SetPhotoEnabled` set to `$True` and assign this policy to the mailboxes of accounts you want to allow to upload photos.

For example, to update an OWA mailbox policy, run the `Set-OWAMailboxPolicy` cmdlet:

```
Set-OWAMailboxPolicy -Identity OWAFullAccess -SetPhotoEnabled $True
```

To assign an OWA mailbox policy to a mailbox, use the `Set-CASMailbox` cmdlet:

```
Set-CASMailbox -Identity Chris.Bishop -OWAMailboxPolicy OWAFullAccess
```

Changes to an OWA mailbox policy take up to 30 minutes before they are effective.

Mailbox Plans

When you create a new Exchange Online mailbox, the new mailbox inherits many of its settings from a mailbox plan. Four mailbox plans are available within a tenant to accommodate the different Exchange Online plans included in Microsoft 365 and Office 365 products. To see the set of mailbox plans, run the `Get-MailboxPlan` cmdlet:

```
Get-MailboxPlan | Format-Table DisplayName, IsDefault, Name
```

DisplayName	IsDefault	Name
ExchangeOnlineEnterprise	True	ExchangeOnlineEnterprise-8fc1c029-5e32-485e-9810-179fb4701447
ExchangeOnlineDeskless	False	ExchangeOnlineDeskless-bc1e76cc-4c0b-491c-a518-3a0a43cbf78e
ExchangeOnline	False	ExchangeOnline-12c139bc-eafa-4a43-b4d2-e285f83e075d
ExchangeOnlineEssentials	False	ExchangeOnlineEssentials-1a1bf516-90d5-4c4b-a047-5b3544ad9826

The role of the mailbox plan is to be a template holding settings for mailbox properties. When you create a new mailbox, the new mailbox inherits settings from the mailbox plan chosen by Exchange Online. Most mailboxes are created along with new accounts via the Microsoft 365 admin center. When this happens, Exchange Online uses the license assigned to the account to select the mailbox plan to apply to the new mailbox. Table 4-1 lists the Office 365 and Microsoft products and the associated mailbox plans.

Products	Mailbox Plan
Exchange Online Kiosk, Microsoft 365 F3, Office 365 F3	<i>ExchangeOnlineDeskless</i>
Exchange Online Plan 1, Microsoft 365 E1, Office 365 E1	<i>ExchangeOnline</i>
Exchange Online Plan 2, Microsoft 365 E3/E5, Office 365 E3/E5	<i>ExchangeOnlineEnterprise</i>
Microsoft 365 Business Basic	<i>ExchangeOnlineEssentials</i>

Table 4-1: Licenses and Mailbox plans

In the output for the `Get-MailboxPlan` cmdlet shown above, the Exchange Online Enterprise plan is marked as the default. If you create a user mailbox without a license, Exchange Online uses the default plan to populate its settings. Mailboxes that don't need licenses, like shared and resource mailboxes, use the Exchange Online mailbox plan. An administrator can specify the mailbox plan to use when creating a new mailbox with the `New-Mailbox` cmdlet.

To report the number of mailboxes assigned to each mailbox plan, check the plan registered for each mailbox. Note that the filter used to find mailboxes requires the distinguished name for the mailbox plan.

```
$Report = [System.Collections.Generic.List[Object]]::new()
$MbxPlans = Get-MailboxPlan
ForEach ($Plan in $MbxPlans) {
    $Dn = (Get-MailboxPlan -Identity $Plan.Name).DistinguishedName
```

```
[Array]$Mbx = Get-ExoMailbox -Filter "MailboxPlan -eq '$Dn'" -Properties MailboxPlan -ResultSize Unlimited # Find mailboxes with the plan
If ($Mbx) {
    ForEach ($M in $Mbx) {
        $ReportLine = [PSCustomObject][Ordered]@{
            Name      = $M.DisplayName
            UPN       = $M.UserPrincipalName
            Plan      = $Plan.DisplayName }
        $Report.Add($ReportLine) }
}
} #End ForEach
$Report | Group Plan | Format-Table Name, Count

Name          Count
----          -----
ExchangeOnlineEnterprise 43
ExchangeOnline   17
```

The *Set-MailboxPlan* cmdlet configures settings in mailbox plans while the *Get-MailboxPlan* cmdlet reports the settings. Because the idea behind mailbox plans is to configure basic mailbox settings, not every property configurable with the *Set-Mailbox* cmdlet is available in a mailbox plan. The settings cover:

- Mailbox quotas and warning thresholds.
- Message send and receive size.
- Deleted items retention period.
- Mailbox retention policy.
- User role assignment policy.

In this example, we use *Set-MailboxPlan* to update the Exchange Online enterprise plan to update the largest supported message size for send and receive to 125 MB, change the deleted item retention period from 14 to 30 days, and assign a new default mailbox retention policy.

```
Set-MailboxPlan -Identity ExchangeOnlineEnterprise -MaxSendSize 125MB -MaxReceiveSize 125MB
-RetainDeletedItemsFor 30.00:00:00 -RetentionPolicy "General Mailbox Retention Policy"
```

Somewhat frustratingly, although *Get-MailboxPlan* returns a large set of mailbox properties and values, *Set-MailboxPlan* is unable to update most settings. If you want to update a mailbox property outside the set supported by mailbox plans, you must run *Set-Mailbox* after creating the mailbox. For instance, you might want to write a value into one of the custom attributes.

Modifying the settings of a mailbox plan does not affect existing mailboxes. If you want to change settings for existing mailboxes, you'll need to run the *Set-Mailbox* or *Set-CASMailbox* cmdlets. However, if the license assigned to a user mailbox changes, Exchange Online applies the settings for the relevant plan to the mailbox (this doesn't happen immediately as it takes some time for Exchange to detect and react to the license change).

Each mailbox plan has a corresponding CAS mailbox plan. This mimics the relationship between *Set-Mailbox* and *Set-CASMailbox* where the first cmdlet updates essential mailbox settings while the second deals with connectivity. In this instance, the *Set-CASMailboxPlan* cmdlet allows administrators to control the following settings.

- Enabling Exchange ActiveSync.
- Enabling IMAP4 and POP3.
- Which OWA mailbox policy is applied.

Recipient Limits

The default recipient limit for an Exchange Online mailbox is 500. This means that the mailbox owner can send messages addressed to up to 500 recipients. The limit exists to ensure that Exchange Online mailboxes

do not consume large quantities of resources by sending messages to large numbers of recipients. You can update the recipient limit for a mailbox to anything from between 1 to 1,000 through the EAC or with PowerShell. For example, this command sets the limit to 900 for the chosen mailbox:

```
Set-Mailbox -Identity James.Ryan -RecipientLimits 900
```

To set a new recipient limit for every user mailbox in the tenant, use a command like this:

```
Get-ExoMailbox -RecipientTypeDetails UserMailbox -ResultSize Unlimited | Set-Mailbox -RecipientLimits 900
```

Although the usual request is to increase the recipient limit to deal with situations such as the distribution of internal newsletters, a use case exists to reduce the limit to restrict the ability of specific users to communicate with large numbers of recipients.

If you want a new default recipient limit to apply for new mailboxes, you can update the setting in the appropriate mailbox plans. For example, this command updates the value for enterprise mailboxes:

```
Set-MailboxPlan -Identity ExchangeOnlineEnterprise-8fc1c029-5e32-485e-9810-179fb4701447 -RecipientLimits 750
```

Multi-Geo Mailboxes

When Exchange Online is configured for multi-geo operation, a tenant can distribute mailboxes across the home region (for example, the United States) and one or more satellite geo locations (for example, the United Kingdom, France, and Norway), depending on where users are and the need to satisfy local data sovereignty. In multi-geo tenants, Entra ID user accounts have a *PreferredDataLocation* property to record the data center region where a user's data should be stored. Exchange Online synchronizes the value of *PreferredDataLocation* into the *MailboxRegion* property for mailbox objects stored in EXODS. This property is blank for mailboxes in single-geo tenants. Exchange Online uses *MailboxRegion* to know where user mailboxes and archive mailboxes are stored (both primary and archive mailboxes must be in the same region). If the *PreferredDataLocation* field for a mailbox changes, the service will automatically move it to the new region.

Configuring a Mailbox-Enabled Account

Creating a new mailbox with the *New-Mailbox* cmdlet also creates a new user object in Entra ID. Creating a new mailbox doesn't assign a license and until the account is assigned a license for Exchange Online, the user won't be able to sign into the mailbox. To allow sign-on, we must update the account with a Microsoft 365 location code for the country where the account is located and assign a license. A license must be assigned to a new account within 30 days to avoid it being blocked and placed into Microsoft 365's automatic deletion routine.

The Microsoft 365 admin center shows the country to which a user is assigned. You can use the same country names with PowerShell, but the country code can also be passed – FR for France, DE for Germany, IE for Ireland, and so on. A tenant can accommodate users in multiple countries, and you can update a user's location as many times as you like, and the multi-geo capability available to large tenants allow them to distribute mailboxes across multiple data center regions. You can't update a tenant's location after it is created because the location determines factors such as billing and the data centers used to hold user data.

Two country properties exist for user accounts. The *Country* property is used for display and sort purposes. You can assign anything you like to the *Country* property for an account because the *Update-MgUser* cmdlet does not validate the input to ensure that the country exists. However, because the *Country* property is used

for sort and display purposes, including the filters used for objects like dynamic groups, these values must be accurate and consistent.

The *UsageLocation* property, which uses the 2-character [ISO 3166 code for a country](#), is much more important because it controls the services that can be provided to the account. For this reason, *Update-MgUser* checks input to ensure that a valid country code is assigned to an account. Instances exist where certain functionality is unavailable in a specific country, as in the case of a voice calling plan. It is therefore essential to be accurate when you set the *UsageLocation* value for an account. Here's an example of setting the two country properties:

```
Update-MgUser -ObjectId Kim.Akers@Office365ITPros.com -Country "Ireland" -UsageLocation IE
```

As explained previously, it can take some time before updates to the new account synchronize across all workloads. You need to take this factor into account if you plan to script the creation of new mailboxes. After we update the user object with a valid location code, we can assign it a license. We do this by running the *Set-MgUserLicense* cmdlet. See the PowerShell book for information about how to manipulate licenses through PowerShell, including how to perform this task using the Microsoft Graph PowerShell SDK cmdlets.

After you assign a license, we should have a licensed user with a functioning mailbox. You can confirm the assignment of the license to the user by examining their account through the Microsoft 365 admin center. It is easy to assign licenses to accounts through the Microsoft 365 admin center, especially when dealing with the finer points of turning on or off different services licensed by a plan. However, it is often more efficient to use PowerShell when you want to check the licenses that are already assigned to accounts or to reallocate licenses to accounts, as might be the case if you choose to upgrade a plan for selected users.

Email Primary and Proxy Addresses

Mail-enabled objects have one or more addresses that allow the Exchange transport service to route messages to them. Exchange Online mailboxes usually have several SMTP proxy addresses (also known as email aliases), any of which can be used to send email to the mailbox. A mailbox always has an address for the onmicrosoft.com service domain used by the tenant. Administrators can assign other addresses to mailboxes for any of the domains owned by the tenant. The set of addresses is stored in the *EmailAddresses* attribute for mail-enabled objects. For instance, here's a typical set for a mailbox:

```
Get-ExoMailbox Jane.Sixsmith | Select-Object -ExpandProperty EmailAddresses
smtp:Jane.Sixsmith+Amazon@office365itpros.com
SMTP:Janey@office365itpros.com
smtp:Jane.Sixsmith@office365itpros.com
SPO:SPO_edc2687c-5939-41d1-9ab1-24a7dc43ac6e@SPO_b662313f-14fc-43a2-9a7a-d2e27f4f3478
SIP:Jane.Sixsmith@office365itpros.com
smtp:Jane.Sixsmith@office365itpros.onmicrosoft.com
```

Each address is of a certain type. In this case, there are SMTP addresses, an address used by SPO (SharePoint Online) to synchronize information about documents created by the mailbox's owner with the Microsoft 365 substrate. You should not remove this address as internal Microsoft processes manage its creation and removal. The SIP address is used for SIP messaging communications, such as Teams calls.

One of the four SMTP addresses has a capitalized prefix. This is the primary address, which means that it is the one Exchange inserts as the reply address for outbound messages so that recipients use the address when they reply to messages. It is best practice to use the same value for both the User Principal Name and primary SMTP address for a Microsoft 365 account. For example, to set the primary SMTP address for a mailbox with PowerShell, run the *Set-Mailbox* cmdlet to set the *WindowsEmailAddress* attribute.

```
Set-Mailbox -Identity Jimmy.Jones -WindowsEmailAddress Jimmy@office365itpros.com
```

If the address selected as the primary is not already present in the mailbox properties, Exchange will add the address and make it the primary.

Except for plus addresses (see below), only administrators can assign multiple email proxy addresses to mailboxes, distribution groups, shared mailboxes, group mailboxes, mail contacts, and mail users using tools including the Microsoft 365 admin center, EAC, and PowerShell.

Sending Email Using Proxy Addresses

Exchange Online supports the ability for users to send email using any of the secondary SMTP proxy addresses (otherwise known as email aliases) assigned to their mailbox. This is especially useful when a tenant supports multiple domains, as in the case of a corporate merger, and users need to send messages using proxy addresses for different domains. To allow users to send email using proxy addresses, update the Exchange organization configuration using PowerShell (below) or through the Mail flow settings in the EAC:

```
Set-OrganizationConfig -SendFromAliasEnabled $True
```

After updating the configuration, it can take several hours for all the mailbox servers used by the tenant to receive the change. Once this process completes, users can use the From field in the message compose form to select and use a proxy address. OWA users must select the proxy addresses they wish to use through the Compose and Reply section of OWA settings to make addresses available for use. Outlook desktop and Outlook mobile users can insert proxy addresses in the From field for new messages. After sending, the proxy address appears for recipients in place of the sender's primary SMTP address.

Plus Addressing

An SMTP address is composed of a local part and a domain. The domain tells mail servers how to route messages to the server identified in the domain's MX record in DNS. The local part is the user address used to identify the eventual recipient. Exchange Online supports plus addressing, meaning that users can add a suffix (an arbitrary tag chosen by them) to the local part of their SMTP address. A plus sign divides the suffix from the local part. For example:

Kim.Akers@Office365itpros.com is a "normal" SMTP address.

Kim.Akers+SomeValue@Office365itpros.com is an SMTP address with a plus suffix.

When the transport service processes an inbound email with a plus address, it removes the plus sign and suffix and uses the remainder to deliver the message.

The idea behind plus addresses is that you can use them to find out if companies are sharing (or selling) your email address for marketing (or spamming) purposes. For instance, if a website asks for an email address before granting access to some content, you can create a plus address and use the name of the website as the suffix. If you later find that spam or other unwanted email arrives using that plus address, you know that the site shared your address. You can then use inbox rules to filter or block messages from that address.

Consumer mail systems like Outlook.com and Gmail support plus addressing. You can use plus addressing in two ways:

- **Administrator controlled:** The tenant assigns plus addresses as SMTP proxy addresses to mailboxes. These addresses are persistent like any other SMTP proxy address, which means that they can be used with features like sending using a proxy address described above. Administrators can assign plus addresses to mailboxes and groups through the EAC or PowerShell, but not through the Microsoft 365 admin center. Mail-enabled objects like shared mailboxes and distribution lists support plus addressing, but as these objects aren't owned by a user, an administrator must assign the plus address. For example:

```
Set-DistributionGroup -Identity TigerTeam -EmailAddresses  
@{Add='Tiger.Team+0365@office365itpros.com'}
```

- **User-initiated:** Users can create their own plus addresses as needed by adding the plus sign followed by whatever text they want to use as a suffix to their regular email address when they give email addresses to other organizations. For instance, if doing business with Contoso, you could tell Contoso to send you an email at *First.Last+Contoso@tenant.com*.

Currently, the *AllowPlusAddressInRecipients* setting in the Exchange organization configuration controls how Exchange Online processes plus signs found in email addresses. The value can be:

- **\$True:** The Exchange transport service uses the plus sign to indicate that it can remove the tag after a plus sign and deliver the message using the remaining address. For example, Exchange will take the address *Tony.Redmond+eCommerce@office365itpros.com* and deliver the message to *Tony.Redmond@office365itpros.com*. This is the default for any new tenant.
- **\$False:** This is the default for older tenants where the possibility exists that valid email addresses exist containing the plus sign. This setting means that Exchange treats the plus sign as a literal character that's part of the email address and will only deliver messages if it can find a match in the proxy addresses assigned to a recipient. For example, if an administrator assigns *Tony.Redmond+eCommerce@office365itpros.com* as a proxy SMTP address to a mailbox, Exchange can deliver the message to that mailbox. It will not strip the "+eCommerce" portion off and attempt to deliver to Tony.Redmond@office365itpros.com.

The *AllowPlusAddressInRecipients* organization setting must be set to True to allow users to create their own plus addresses as described above. You can update the setting through the Mail flow settings in the EAC or by running the *Set-OrganizationConfig* cmdlet:

```
Set-OrganizationConfig -AllowPlusAddressInRecipients $True
```

When plus addressing is active, any intermediate gateway which processes inbound email must focus on the domain for routing. If the gateway attempts to do directory lookups to check recipient addresses and cannot handle plus addresses, the lookups might fail and cause the rejection of messages.

Plus addressing is available by default. Any proxy addresses containing plus characters that are still present for mail-enabled objects will not work as before because Exchange Online will no longer attempt to match the complete address (including the plus sign and tag) on inbound messages against its directory. This could lead to the non-delivery of email. If your organization wishes to opt out of plus addressing, run the command:

```
Set-OrganizationConfig -DisablePlusAddressInRecipients $True
```

See [this article](#) for details of PowerShell code to locate and remove plus addresses from mail-enabled recipients.

Administrator Access to User Mailbox Settings

Occasionally, users need help from an administrator to update mailbox settings. Two methods are available:

1. Select the **View another mailbox** from the menu revealed by selecting the user photo at the top right-hand corner of the EAC. After selecting the mailbox to manage, EAC displays the settings for the mailbox in a separate browser window. A banner showing the target mailbox and the name of the user updating the settings. Apart from needing to be a member of at least the Recipient Management role group, no special access rights must be held by the administrator to allow them to update user settings.

2. Through PowerShell, Exchange Online supports a set of cmdlets to allow administrators to manipulate different personal mailbox settings, or options usually selected by users. You can use these cmdlets to configure a mailbox on behalf of a user or to check that certain settings are in place. An account that performs maintenance on user accounts through PowerShell should be assigned the Recipient Management role. If the need exists to view the data in the mailbox, the account needs *Full Access* permission.

Using a browser to change user settings is easiest when you only have one or two mailboxes to update. PowerShell is the preferred method when changes need to be applied to multiple mailboxes, or when you want to update mailbox settings in a script that creates a new mailbox.

Administrators with the RBAC User Options role can manage settings for any user mailbox. For example, an admin who holds that role can do the following to grant Tony Redmond full rights over the mailbox owned by Kim Akers.

```
Add-MailboxPermission -Identity 'Kim Akers' -User 'Tony Redmond' -AccessRights FullAccess  
-AutoMapping $False
```

Note the use of the *AutoMapping* parameter. If omitted, Exchange tags the mailbox as an alternate, meaning that the user has full access to all folders and content. Autodiscover then includes the mailbox in the resources it publishes to Outlook when the client polls Autodiscover for information about available services. After learning about the mailbox from Autodiscover, Outlook adds the mailbox to the set it opens and it will automatically be visible in the Outlook client. When *AutoMapping* is *\$False*, Autodiscover ignores the mailbox when it builds the list of resources available to Outlook. The user can edit their mailbox settings to open any extra mailboxes that they have access rights to at any time. For more information, see the section on *AutoMapping* in the Exchange Online chapter.

Securing the Data of Ex-employees

Over time, some employees will leave the organization. Many departures are expected and planned for, some are amicable, and some will be immediate and potentially traumatic. For legal reasons, you might need to preserve the employee's mailbox in the latter case. In an on-premises environment, you can preserve mailboxes by disabling the user account. If needed, you can reenable the account to restore a mailbox to full running order. The same is true for in the cloud, but you probably do not want to pay the monthly license for an unused account only kept in case the organization needs some of the information in its mailbox in the future. Removing the need for licenses is why inactive mailboxes are so valuable.

When you delete a user account through the Microsoft 365 admin center, the following points in the removal workflow need consideration:

- **License:** Remove the license held by the deleted account or keep it for later reassignment to another account.
- **Mailbox:** Exchange Online removes all the proxy email addresses (primary address and any secondary addresses). In addition, Exchange removes all delegate permissions from the mailbox, but you can grant permission to allow another user to access the mailbox content and retrieve information. As shown in Figure 4-5, the reassignment cannot happen until after the removal of any holds on the mailbox. Alternatively, if the account has an E3 or E5 license, you can place a hold on the mailbox before deleting the account. Exchange Online will then make the mailbox inactive (see the Exchange chapter) and retain it in that state until the hold lapses.
- **OneDrive for Business:** To review and retrieve important information held in the user's OneDrive for Business account, you can grant access to another user. Apart from documents, the account might hold information created by applications, like Teams meeting recordings. By default, access lasts for

30 days after which OneDrive for Business permanently removes the information, so the person granted access must review and retrieve information in that period. A tenant can increase the retention period for deleted OneDrive for Business accounts by updating the setting in the SharePoint admin center from 30 (the default) up to 3650 days (ten years).

The Microsoft 365 admin center can remove only cloud accounts. On-premises accounts are only manageable with an on-premises administration tool. In addition, the workflow does not address access to information in other workloads. For instance, if the user you want to delete is the sole owner of some Groups or Teams, the deletion process does not make sure that the groups/teams remain with at least one owner. The same is true for traditional SharePoint sites where the deleted user might be the sole administrator. In other words, treat the user removal workflow as something that deals with the user's data held in cloud mailboxes and OneDrive for Business accounts while ignoring the user's activity in other workloads. We'll come back to this topic shortly.

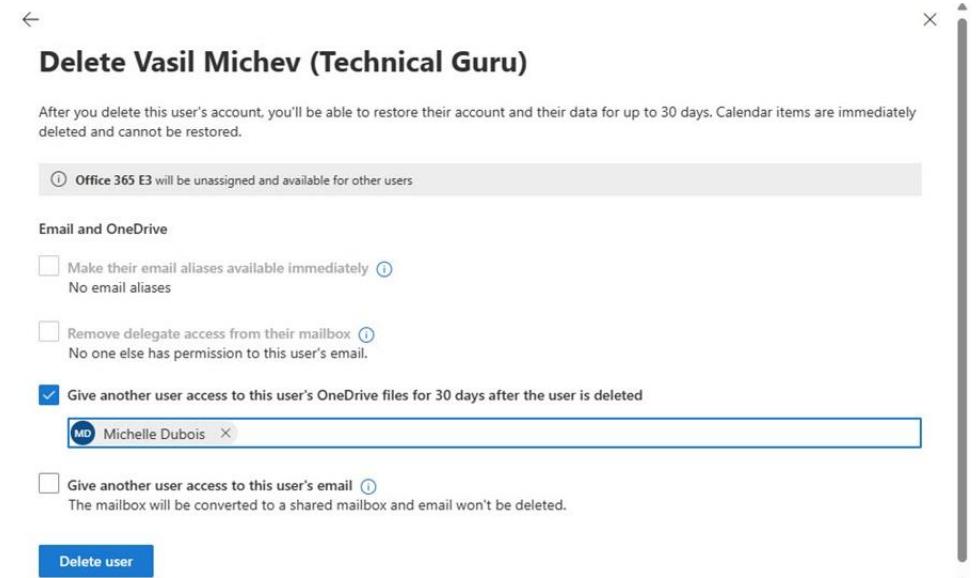


Figure 4-5: Steps to delete a user account when removed through the Microsoft 365 admin center

Remember that it might be a good idea to create an autoreply to let senders know that the person is no longer with the organization. This is a separate action that the Microsoft 365 admin center does not perform when removing an account.

Microsoft's account removal process is reasonable and suits the needs of many organizations. Sometimes you might want to use a different process, especially if some element of discord is present when someone leaves. For this reason, we should discuss the different steps you can take to preserve all the data that a person might have access to when the time comes for them to leave the organization.

Revoking Access to a User Account

The first and most essential action is to secure access to the user's account to prevent any unauthorized deletion of data. We can then put their mailbox and other data into a suitable status for long-term preservation. Normally, when a user authenticates to the service, they create a session with the application they're using. The session receives both an access token and a refresh token from Entra ID. Usually, an access token is valid for an hour. When that period elapses, an automatic reauthentication process kicks in to get a new access token to allow the session to continue. This interaction happens if the refresh token is still valid, and the account credentials are the same. The refresh token has a defined lifetime. This architecture leads to the occasional result that a user with a blocked or deleted account still has a valid refresh token and can still access some workloads. Because each session has a separate refresh token, you might have sometimes

noticed that a user might be able to still sign in on one device after a password change or account blockage while other devices disallowed sign-in.

Continuous access evaluation (CAE), as described in the Identities chapter, means that individual services can receive notifications that tell them when critical directory events happen, such as blocking an account or a password change. Because clients may still present an unexpired, valid-looking token even after critical events, workloads that support CAE like Exchange Online and SharePoint Online reject the token after receiving notification of a critical event. Microsoft began adding CAE support to the Microsoft 365 admin center in September 2024, a welcome change; you should note that, as of September 2024, changing role assignments for a user is not considered as a critical event and will not trigger CAE.

When the Microsoft 365 admin center blocks an account, it resets the account's *RefreshTokensValidFromDateTime* property to the current date and time (this is the same as the forced sign-out option for an account available in the Microsoft 365 admin center). Forcing apps to sign out means that Entra ID invalidates any existing refresh tokens issued to apps. Because the forced sign-out invalidates the refresh tokens, the next time an app attempts to use its refresh token to renew its access, it discovers that the token has expired and so forces the user to reauthenticate. As a block exists for the account, the user cannot reauthenticate. In addition, the CAE mechanism will almost immediately revoke the refresh and access tokens.

You can [strictly enforce location policies using CAE](#). When this setting is enabled, tokens are checked against the location policies defined for conditional access, so that replaying a valid token captured from a different location will fail.

You can manually block sign-ins, initiate forced sign-outs, and reset account passwords from the Microsoft 365 admin center. Any of these actions will flag the account for CAE, meaning that in nearly real-time the workloads that support CAE will reject any previously issued tokens for that account. To block an account, select the account from the list of active users, edit its settings, and select **Block this user** from the set of icons under the user's name.

Revoking Access with PowerShell

Blocking an account from signing in through the Microsoft 365 admin center is the right approach when you manage the departure of a single employee. Using PowerShell commands is better when you need to secure a set of accounts quickly or you want to automate the process to secure an account for a departing employee. To revoke access for an account with PowerShell, do the following:

- Run *Update-MgUser* to disable the account. Disabling the account triggers a CAE event to force the user to reauthenticate. They cannot authenticate because of the account's blocked status, so you could stop here if you like.
- Create and set a new password for the account to allow administrator access once the time comes to recover information from apps. Naturally, the new password only works after unblocking the account. Password changes also trigger CAE events. The commands below update an account with a simple password. The PowerShell chapter contains an example of how to generate a random password that is more secure than an administrator-defined string. Entra ID prompts the user to reset their password after signing in. If you are happy for the user to continue using the assigned password, change the *ForceChangePasswordNextSignIn* setting in the [password profile](#) to *\$False*. When using delegated access to reset an account password, the signed-in account must hold the delegated *Directory.AccessAsUser.All* permission and the account must hold at least the User Administrator role. To change passwords with an app, the app must have consent to use the *User.ReadWrite.All* permission.

- Force an immediate sign-out from apps by revoking signed-in sessions with the `Revoke-MgUserSignInSession` cmdlet. This action also triggers a CAE event.
- Disable any devices registered to the user to prevent them signing in from those devices. Revoking access to a device [requires the signed in account to hold the Cloud Device administrator](#) or Global administrator role.

```
Connect-MgGraph -Scopes Directory.AccessAsUser.All -NoWelcome
$Account = Read-Host "Enter the User Principal Name of the account to block"
$user = (Get-MgUser -UserId $Account -ErrorAction SilentlyContinue)
If (!$User) { Write-Host ("Can't find an account for {0}" -f $Account); break }
Write-Host ("Revoking access and changing password for account {0}" -f $User.DisplayName)
# Disable the account
Update-MgUser -UserId $User.Id -AccountEnabled:$False
# Create a password profile with details of a new password
$password = @{}
$password["Password"] = "!NewYorkCity2022"
$password["ForceChangePasswordNextSignIn"] = $True
Update-MgUser -UserId $User.Id -PasswordProfile $password
# Revoke signed in sessions and refresh tokens
$revokeStatus = Revoke-MgUserSignInSession -UserId $User.Id
If ($revokeStatus.Value -eq $true) {
    Write-Host ("User access revoked for {0}!" -f $User.displayName)
}
# Disable registered devices
[array]$userDevices = Get-MgUserRegisteredDevice -UserId $User.Id
If ($userDevices) {
    Foreach ($device in $userDevices) {
        Update-MgDevice -DeviceId $device.Id -AccountEnabled:$False
    }
}
```

Incident response revocation: If you're disabling an on-premises user account because you suspect that it's been compromised in some way, you should reset the password *twice*. [Microsoft's documentation suggests](#) this approach to ensure that an attacker who's captured a password hash can't use a pass-the-hash attack.

When employees depart, having their account lose access to some teams might not be important. If it is, or in situations where it's necessary to preserve the account in full working order, an alternative to disabling an account is to change its password and revoke access. The account remains active but is inaccessible unless those attempting to sign-in know the new password.

Permanently Removing User Accounts and Mailboxes

When you delete a user account, it remains in the Entra ID recycle bin for 30 days. You can remove the account permanently (hard deletion) beforehand by:

- Selecting the account in the Deleted users section of the Entra admin center and deleting it there.
- Running the `Remove-MgDirectoryObject` cmdlet.

Permanent removal means that *no recovery is possible*. Entra ID synchronizes the removal to workload-specific directories, such as EXODS, to ensure the removal of any workload-specific objects such as the user's mailbox. Microsoft cannot recover user objects after permanent removal and cannot recover any workload-related data either. Remember, Microsoft does not take backups of Entra ID or Exchange Online. It is therefore clear that deciding to make a user account irrecoverable should only happen when you are certain that it's safe to remove the object and its data.

Putting a User Mailbox on Litigation Hold

After blocking the user account, you should place its mailbox on litigation hold to ensure that no one can remove information from the mailbox. Litigation hold retains everything in the mailbox (including system

data) until an administrator releases the hold. By comparison, retention policies or retention tags apply more precise holds. However, the catch-call nature of litigation holds make them valuable when the need exists to preserve everything.

This example shows how to place a mailbox on litigation hold. The *Set-Mailbox* command updates the *RetentionComment* property with details of who applied the hold and the date of its application. The litigation hold will remain in effect until an administrator sets *LitigationHoldEnabled* to *\$false*.

```
$RetentionComment = ("Employee Terminated on {0} by {1}" -f (Get-Date), $Administrator)
Set-Mailbox -Identity 'Bad Employee' -LitigationHoldEnabled $True -RetentionComment
$RetentionComment
```

You can create a core eDiscovery case whose only purpose is to manage a hold on mailboxes for ex-employees. Create a hold within the eDiscovery case and add the mailboxes that you want to keep to the hold. You can also add the OneDrive for Business sites belonging to ex-employees to the hold if you want to preserve their contents.

Risk always exists that a soon-to-be-terminated employee might hear of their impending fate in advance and not react well to the news. They might then decide to remove information from their mailbox and other data repositories (shared mailboxes, group mailboxes, Teams conversations, SharePoint Online document libraries, their OneDrive for Business personal site, and so on) before management makes the formal announcement. This is a tricky situation because of the lack of backups for cloud applications, but it is somewhat mitigated by the ability to assign retention policies to SharePoint Online sites to stop people from removing information.

Placing the mailboxes of affected employees on hold as soon as possible after management decides that the employees are leaving will preserve the mailbox contents no matter what steps their owners take to remove information, but it does create the possibility that employees will learn about their impending departure when HR asks IT to place mailboxes on hold. One way to fix this issue is to create a special RBAC role that allows HR representatives to place mailboxes on hold. This will not stop a maliciously-minded individual from erasing data from SharePoint Online or their OneDrive for Business account, but you can ask Microsoft support to help recover information removed from SharePoint using the backups that they take.

Long-term Mailbox Preservation

Two choices exist as to how to preserve the mailbox for the long term. You can convert it into a shared mailbox or make it an inactive mailbox.

- **Convert to a shared mailbox:** An EAC option exists for this purpose. Converting to a shared mailbox removes the need for a license (unless the new shared mailbox has an archive mailbox, a hold exists on the mailbox, or the mailbox has a larger quota than the default 50 GB assigned to shared mailboxes) and keeps the mailbox contents online so that whoever needs to access the mailbox can open it. Note that this option does *not* guarantee data preservation or immutability, as anyone with permission to access the shared mailbox can modify it unless you have applied a hold. You should check that full delegate auditing is enabled for the mailbox (see the report and auditing chapter) so that Exchange records whatever actions the delegates take with items in the mailbox. Because the purpose of the shared mailbox is to preserve information, you should prevent people from sending messages to the mailbox by changing its SMTP address and hiding it from the GAL. You also need to remove the mailbox from the membership of any distribution lists and Groups to which it belongs and revoke its access to other SharePoint Online sites. Converting the mailbox of a departed employee to a shared mailbox is a simple and effective way to preserve mailbox contents that is preferable if you think that someone will need to access the information in the mailbox in the

short term. If you have the necessary licenses, you should put the mailbox on hold if you need to retain its contents for compliance purposes.

- **Convert to an inactive mailbox:** If no need exists for short-term access to the mailbox contents, you might prefer to “warehouse” the mailbox by making it inactive. As explained earlier, two prerequisites exist: first, the mailbox must be on hold before the account is removed. Second, the account must have a license that supports retention policies to allow the mailbox to be put on hold. Once the mailbox is on hold, it is safe to remove the user account because Exchange Online will keep the mailbox until the hold lapses, or the tenant removes all holds which apply to the mailbox. No one will be able to log into the mailbox and no need exists for a license. When a mailbox is made inactive, Exchange removes it from address lists and distribution lists. A mailbox can stay in the inactive state for a sustained period, but you can recover or restore an inactive mailbox if needed. Information held in the mailbox remains available for eDiscovery searches.

Exchange Online Plan 2 (included in Office 365 E3 and E5) or the Exchange Online Archiving add-on license are needed for retention policies. Because of this, mailboxes belonging to accounts with lower-cost licenses like frontline workers can’t be made inactive and therefore their mailboxes must be converted into shared mailboxes if the need exists to retain these mailboxes for compliance purposes.

As noted earlier, you can run the *Remove-MgUser* cmdlet to remove a user account. Removing a user account releases the licenses assigned to the account. You can either reassign the licenses to other accounts or reduce the number of licenses that you pay for each month.

The steps needed to disable and preserve an employee’s account in a hybrid deployment are different. Remember that in this scenario, the on-premises Active Directory is the master and all changes to accounts and mailboxes must happen on-premises and then synchronize to Entra ID, which usually creates a delay before a guaranteed block exists for an account.

Dealing with OneDrive for Business

Because their OneDrive for Business account stores personal information belonging to the removed user, its contents are out of sight to administrators unless you take steps to recover data after the removal of a user account. Originally, OneDrive for Business was all about documents. Now, it stores many other items of interest that the organization might wish to retain including recordings of Teams meetings, whiteboards, OneNote notebooks, Loop components, personal Lists, and Stream and Clipchamp videos. By default, unless the site is on hold, after the removal of a user’s account, a background timer job removes their OneDrive for Business account 30 days after the deletion of the user account (the My Sites Clean Up timer job). Microsoft 365 sends a message to the user’s manager to warn about the clean-up and sends a second reminder 3 days before removal of the data. If the Entra ID user account properties do not hold details of the user’s manager, Microsoft 365 obviously cannot send the notification. If 30 days is too short a retention period, you can increase it to anything up to 3,650 days. For instance, this command sets the retention period for OneDrive for Business Accounts to one thousand days.

```
Set-SPOTenant -OrphanedPersonalSitesRetentionPeriod 1000
```

You can ensure continued access to the OneDrive accounts owned by ex-employees by configuring the SharePoint Online settings to automatically assign a secondary owner to OneDrive for Business sites. Go to the More features page of the SharePoint admin center, open the User Profiles item, click Setup My Sites under My Site Settings, verify that the Enable access delegation box is checked, and then select a user account to be the secondary owner. If Entra ID does not hold details of a manager for the removed user, SharePoint sends the reminders to preserve data to the secondary owner, who can then arrange for a review of the data and the capture of anything that needs preservation to another location (for example, another user’s OneDrive for Business site or a SharePoint Online team site). You can also create a link to a user’s

OneDrive account through the Microsoft 365 admin center. Select the user, open their properties, and select the OneDrive tab. The Create link to files option creates a link that allows the administrator to work with the files in the user's OneDrive account. For instance, they can select files and move them to another account or SharePoint site.

Dealing with Other Workloads

Of course, because information exists in many other places in Microsoft 365 workloads than the user's mailbox, administrators need to do some added work to look for and recover anything considered valuable. These include:

- Equipment issued to the employee. PSTs and documents might be on the hard drive of the user's PC and hold information invisible to administrators unless they can gain physical access to the drive. In terms of the potential for information leakage, PSTs are especially vulnerable as users can remove them from the organization on easily portable USB thumb drives along with copies of documents downloaded from SharePoint and OneDrive for Business accounts. You can scan the audit log to figure out whether the ex-employee downloaded an excessive number of files during their last weeks of employment, but it is impossible to know whether they copied messages from Outlook to a PST and took that PST with them. Copies of documents and messages protected with sensitivity labels cannot be accessed when someone leaves the organization because the ex-employee needs to authenticate using a valid account before they can open the content. This is a good reason to use sensitivity labels to protect confidential information.
- Given the widespread use of mobile devices, a terminated employee probably used a personal mobile device to access their mailbox. Because of caching, it might be possible to use cached credentials to connect to the mailbox with a mobile device even after the employee leaves. Given that a user might have multiple mobile devices, it is best to issue a remote wipe for all ActiveSync devices registered with the mailbox. Any future attempt to access the mailbox will wipe the device that issues the connection request. Depending on how the mobile device vendor has implemented the ActiveSync protocol within the email client, the wipe might affect some or all personal data. To wipe all the ActiveSync devices connected to a user account, run the following PowerShell command:

```
Get-MobileDevice -Mailbox 'Bad Employee' | Clear-MobileDevice
```

- Microsoft Endpoint Manager has more selective wipe capabilities for its managed devices than ActiveSync has. See [this page](#) for information about how to perform a full or selective wipe of a mobile device with Microsoft Endpoint Manager.
- SharePoint Online sites managed by the user. Other users who have access to these sites can continue to work with the information held in the libraries and lists and an administrator can grant ownership for these sites to a different user.
- Loop workspaces owned by the deleted user are in SharePoint Embedded storage. When someone leaves the organization, [these objects can become ownerless](#). Make sure that Loop workspaces are transferred to another user before deleting the account.
- Groups and Teams. If the user is the sole owner of a group or team, you should assign that role to another user. If you want to capture information about the conversations that an employee has participated in, you can run a content search against the group mailboxes for the teams they belong to and their mailbox for items. Once the search is complete, you can then export the results to a PST or ZIP file. Don't forget to check for Exchange Online distribution lists and dynamic distribution lists owned by the deleted users.
- Teams chat messages sent by a deleted account remain online while at least one chat participant remains in the tenant. When the accounts for all chat participants are removed, Teams removes the

chat from its Cosmos DB message database. If you want to preserve the chats for a deleted account, use a content search to recover all items with a keyword `type:microsoftteams` and export the search results to a PST.

- Teams meetings organized by an ex-employee still function. However, the meetings cannot be transferred to allow another user to become the meeting organizer. If having all meetings organized by a current employee is important to the organization, you will have to remove the old meetings and reschedule replacements.
- If the account has a number assigned for use with the Teams Phone system, it should be removed.
- You can recover Microsoft Forms created by an ex-employee and transfer them to another user. See [this page](#) for information.
- Entra ID app registrations owned by the deleted users should either be reassigned to another user or removed.
- If the ex-employee owns some Power Automate workflows, these flows will stop working after the account is removed. Depending on what the workflows do, this might or might not have a bad effect and it's worth checking out.
- Copilot pages created by the user follow the same deletion schedule as their OneDrive account. After the OneDrive deletion period expires, the pages move into the recycle bin and are eventually removed. During this period, a SharePoint administrator can recover content from a page, but they cannot assign ownership of the page to another user.

It is sensible to review the list of data sources annually as the potential places where users can store valuable corporate data might grow as the feature set available within Microsoft 365 expands.

Removing Calendar Events: When someone leaves the organization, their mailbox may be the organizer of events that exist in other peoples' calendars. In many cases, you might want to remove those events from calendars to allow someone else to reschedule replacement events (or not, as the case might be). The `Remove-CalendarEvents` cmdlet cancels future events organized by a specific mailbox and sends out cancellation notices. For example, this command cancels all meetings organized by Nancy Anderson from today's date, which is probably what you would do for an employee leaving the organization. Remember to run the cmdlet before you remove the mailbox.

`Remove-CalendarEvents -Identity "Jim.Doe@Office365itpros.com" -CancelOrganizedMeetings`

On the other hand, if the user is going away for an extended period and will eventually return, you can run the cmdlet to cancel events for a date range. See [this page](#) for more information about the cmdlet.

Handling Inbound Email for Ex-Employees

When you convert a user mailbox to a shared mailbox, the mailbox keeps all the assigned email addresses and can continue to receive emails sent to the mailbox. Someone will need to process messages that arrive in the mailbox to let the senders know that the intended recipient no longer works at the company.

Alternatively, you can change the assigned email addresses so that Exchange will "bounce" (send a non-delivery notification) any new messages sent to the mailbox.

You can let people who try to contact the now-departed employee receive the normal non-delivery notification or you can create a better experience by telling them why the person they tried to contact is no longer available. This PowerShell code sets up internal and external autoreply messages for the mailbox and adds a MailTip that is visible to internal users. We also hide the mailbox from all address lists and enable mailbox auditing to track any access that occurs to the mailbox.

```
Set-MailboxAutoReplyConfiguration -Identity "Terminated Employee" -InternalMessage "The person you  
are emailing no longer works for us. Please refer communications to Mr. Manager"  
-ExternalMessage "Mr. Terminated Employee is no longer an employee of this company."  
-AutoReplyState Enabled
```

```
Set-Mailbox -Identity "Terminated Employee" -MailTip "Terminated Employee has left the company.  
Please do not send any more mail to their mailbox" -HiddenFromAddressListsEnabled $True
```

Auto-replies and MailTips inform users about people that are no longer with the company if the mailbox still exists in an active state. However, we might want to remove the mailbox completely after harvesting any useful data in it. Exchange Online does not have a way to inform correspondents that a mailbox is no longer in use, but we can do this by creating a shared mailbox to hold the email addresses previously assigned to removed mailboxes or the old addresses of user mailboxes that have been converted to shared mailboxes. In effect, you use the shared mailbox (which does not need a license) to redirect inbound messages so that the senders will receive some information to inform them that their correspondent is no longer available.

Although Exchange Online limits the number of SMTP proxy addresses that you can assign to a mail-enabled object, a shared mailbox can easily hold 400 email addresses. If you need to keep a higher number of addresses for departed employees, you can spread the addresses over several mailboxes. One technique is to create a shared mailbox for each department so that external senders can receive an autoreply giving them details of a new contact within the department.

Of course, the shared mailbox will act as a black hole if you simply add the email addresses of departed employees to it. To complete the process, you should create an autoreply for the shared mailbox so that Exchange Online will respond to the senders after it delivers inbound messages for the addresses assigned to the shared mailbox. Ideally, the autoreply will tell the sender that they should not use the address in the future.

Although there might be some value gained by receiving email in the shared mailbox, often companies do not want to accumulate messages from people who have left. It can be an onerous task, not to mention a potential breach of personal privacy, if someone accesses the shared mailbox to process and respond to the messages found there, so the best solution is often to institute an automatic bounce mechanism to suppress inbound messages. This can be achieved with the combination of a distribution list and a transport rule.

Here's how:

- Create a normal distribution list and add the shared mailbox (or mailboxes if necessary) to its membership. Make sure that the group owner (by default, the administrator who creates the group) is not added to the membership as they will not be able to receive new mail once the transport rule created in the next step implements a block for group members.
- Now create a transport rule to intercept messages sent to the members of the distribution list and return a rejection notice to the senders. We provide suitable text to explain why the rule rejects messages.

```
New-TransportRule "Block Email to Disabled Mailboxes" -SentToMemberOf "Disabled Mailboxes" -  
RejectMessageReasonText "Unfortunately the person with whom you attempted to communicate is no  
longer with our company." -Enabled $True
```

Once enabled, the rule will reject any message sent to one of the SMTP addresses assigned to the shared mailboxes in the distribution list. It is a simple but effective way to provide a better user experience.

When Someone Dies

All of us will die someday. In large organizations, statistics show that the likelihood exists that one or more employees will die per 10,000 annually, depending on the average age of employees. Given the era we live in, when we do pass on, we will leave behind many digital assets, among which might be a corporate mailbox. It's a good idea to have a procedure to preserve the mailboxes and other information belonging to dead employees. The steps that you might take are like those that you use to preserve content in mailboxes for terminated employees and include:

- Disabling or blocking the account.
- Deciding if the mailbox should become an inactive mailbox or remain online. Alternatively, if you run a hybrid deployment, you could move the mailbox back to an on-premises database that is reserved for this purpose. The purpose of keeping the mailbox is to allow for the retrieval of any valuable information from the mailbox within a retention period decided by HR and/or the legal department and in compliance with applicable regulations such as GDPR. Some arrangements should be put in place to extract personal information from the mailbox and give it to the employee's family. For instance, some people store passwords and other valuable information in their mailboxes that might be needed by their family following their death. Personal and corporate data might also need to be recovered from the user's OneDrive for Business site. After retrieving whatever information is considered valuable from the mailbox, you might move it into an inactive state and keep the mailbox for a further period.
- Removing the mailbox from any distribution lists and the Groups/Teams to which it belongs. You can discover what groups a mailbox belongs to by looking at the mailbox properties via EAC or by running some PowerShell code (an example is in the Groups chapter). If you make a mailbox inactive, its membership in distribution lists and groups is automatically canceled.
- If the mailbox remains online, remove the mailbox's access to any shared mailboxes. You can consider adding the mailbox to a special "Departed Employees" distribution list, which is hidden from the GAL. Some companies like to use a transport rule that blocks any incoming messages sent to the members of the "Departed Employees" group. The rule might also generate a customized NDR back to senders to inform them of the sad demise of the intended recipient. As described above, you can use the *RejectMessageReasonText* parameter for the *New-TransportRule* cmdlet to create a thoughtful response to messages sent to a deceased employee. An alternative is to set an auto-reply message on the user's mailbox by either logging onto the mailbox or using the *Set-MailboxAutoReplyConfiguration* cmdlet (explained in the Exchange Online chapter).

Eventually, the retention period for policies applying to the mailbox or retention labels assigned to mailbox items will elapse, and you will either remove the user's account or cancel the hold that keeps their mailbox inactive.

Remember that a user is likely to have responsibility for documents and other information in other places across the service and that some effort is necessary to track down this information and transfer it to the safekeeping of another user.

Humane effectiveness: Although it is good to have a well-documented process to handle what happens when users die, it is also good if an organization can show some humanity. Some large businesses delegate the authority to manage the process of securing the digital assets of deceased employees to joint HR/IT teams who can flex and alter the process as necessary to meet the needs of any specific circumstances that might arise. The IT members of the team ensure that the technical processes are followed while HR ensures that everything is done humanely and thoughtfully. It is a good approach to follow.

Compromised Accounts

A compromised account is one where someone outside the tenant (an attacker or hacker) manages to gain access to the account resources. Usually, this is because the attacker obtains the credentials necessary to sign in to the account, perhaps because their account credentials are compromised through a breach of another site.

Signs of unusual activity such as missing data, new rules or a forwarding address appearing in the mailbox that the user can't remember setting up, or strange emails from the mailbox might be indications of a

compromised account. The steps necessary to secure the account and prevent further unauthorized access are:

- Block the account.
- For on-premises accounts, reset the account password twice
- Enforce multi-factor authentication on the account if you have not already done so.
- Check all the mailbox settings to ensure that inbox rules, sweep rules, and forwarding addresses are valid (if a forwarding address exists outside the organization, ask if a business purpose exists for forwarding email to that address).
- If the account has administrative access, check what data might have been compromised through this access, validate that the access is needed, and remove it if not.
- The audit log can help you find what data the account has accessed recently. You should check any documents the account uploaded to SharePoint or OneDrive for Business to ensure that they don't contain malware.
- When the account is completely checked out, unblock it and give the new password to the user.

Microsoft's advice on the topic is in [this support article](#).

Managing User Pronouns

Microsoft 365 supports the display of pronouns on the user profile card. The option to enable pronouns is available in the Security & Privacy tab under Org settings in the Microsoft 365 admin center. Once enabled, users can select their preferred pronouns (like *He/Him* or *She/Her*) through an option on the profile card in applications like Teams and OWA. Although Microsoft 365 suggests some commonly-used forms of pronouns, users can input any text they like up to the 30-character limit.

Pronouns are visible to everyone in the organization. There's no way to suppress pronouns for some users and display for others. For more information, read [this article](#).

Managing User Settings for Viva Insights

As with many other parts of Microsoft 365, Viva Insights settings can be applied at two different levels: the tenant and the individual user. The tenant-level defaults for Viva Insights allow you to control whether Viva Insights runs at all and, if so, which specific features are enabled by default. You can always override the defaults for individual users, but setting defaults for the tenant is useful because the default settings will be applied when new users are added.

The [Get-DefaultTenantMyAnalyticsFeatureConfig](#) and [Set-DefaultTenantMyAnalyticsFeatureConfig](#) cmdlets allow you to view and set the defaults you want to use. The most important default is probably the *PrivacyMode* setting, which can be set to *Opt-in* (in which case users must choose to receive Viva Insights data) or *Opt-Out* (in which case users must manually turn off Viva Insights themselves). Which of these settings you prefer will of course depend on your users, where they work, and your organizational culture. This cmdlet allows you to control whether various Viva Insights features are enabled for those users who have access to them. For instance, you might decide to give users access only to the Viva Insights digest email, and to enable it by default, which you'd do like this:

```
Set-DefaultTenantMyAnalyticsFeatureConfig -PrivacyMode Opt-Out -Feature all -IsEnabled $false  
Set-DefaultTenantMyAnalyticsFeatureConfig -Feature Digest-email -IsEnabled $true
```

You can also manage user-level settings with PowerShell but the story here is a bit messier. The [Set-VivaInsightsSettings cmdlet](#) lets you control whether the user has access to the [Viva Insights Headspace](#) feature, but for now that's all it can do. You can use the [Set-MyAnalyticsFeatureConfig](#) cmdlet to enable or

disable the Viva Insights dashboard, Outlook add-in, and digest email features. Expect Microsoft to rationalize this situation in the future by moving more settings to *Set-VivaInsightsSettings*.

Somewhat oddly, these cmdlets are all included in the Exchange Online PowerShell module.

Managing User Access to Microsoft Bookings

As described in the tenant management chapter, global access to Bookings is managed through the **Org settings** section of the admin center. You can control user-level access to Bookings on multiple levels.

First, you can control whether individual users have access to the shared bookings feature. You can either do that by removing the Bookings service plan from the set of plans licensed to the user in the user's account details in the admin center, or by using PowerShell, as described in the PowerShell book. The example below shows how to remove the Microsoft Bookings service plan from the user *Terry.Hegarty*. First, we create a license option using the SKU of the Office 365 E3 license (6fd2c87f-b296-42f0-b197-1e91e994b900) and add the individual plan we want to disable—in this case, Bookings. Then we use the *Set-MgUserLicense* cmdlet to apply the change:

```
$LicenseOptions = @{Skuid = "6fd2c87f-b296-42f0-b197-1e91e994b900"; DisabledPlans = @("199a5c09-e0ca-4e37-8f7c-b05d533e1ea2")}

Set-MgUserLicense -UserID Terry.Hegarty@Office365itpros.com -AddLicenses @($LicenseOptions) - RemoveLicenses @()
```

Second, if you want to prevent a user or set of users from creating new shared bookings pages, you do that by creating and assigning an OWA mailbox policy (as described elsewhere in this chapter). When a user creates a new bookings page, that user becomes its administrator; after the page has been created, the user can define the services available, their cost, and the set of users assigned to handle booking requests.

The *BookingsMailboxCreationEnabled* flag on the policy controls whether or not that specific user may create new shared booking pages, so create (or modify) an OWA mailbox policy with the appropriate value and assign it to the users whose shared bookings access you wish to control.

Third, you may want to regulate who can use the Personal Bookings feature. You can control this feature at the user or tenant level. At the tenant level, you will need to use *Set-OrganizationConfig -EwsApplicationAccessPolicy* to either block or allow the **MicrosoftOWSPersonalBookings application**. For individual users, you can block or allow that application using *Set-CASMailbox*. Both of these cases are [described in Microsoft's documentation](#).

Chapter 5: Managing Exchange Online

Michel de Rooij

This chapter reviews Exchange Online. We'll discuss how to manage Exchange Online using the Exchange Admin Center (EAC) and PowerShell. User accounts must hold the Global administrator or Exchange administrator role to manage Exchange Online.

Exchange Online

For many companies, email is the first workload that they move into the cloud. Given the popularity of Exchange since its introduction in 1996, it was therefore unsurprising that many of the early organizations that moved to the cloud migrated mailboxes from on-premises Exchange servers.

Exchange Online is the cloud-based version of Exchange. Or is it? Both products share common roots and common functionality, but the version of Exchange that runs inside the cloud is very different from its on-premises counterpart. As we will see, the difference is somewhat inevitable given that Exchange Online must function inside a massive multi-tenant infrastructure while Exchange Server is designed to deliver an email service for many on-premises customers, each of whom might adopt a different method to deploy and manage Exchange.

Exchange Online reach

Footprint

300K physical servers
~175 datacenters
26 countries
210 network POPs

Storage

1.4 EB of data (logical)
42 trillion Items
7.3 B mailboxes

Daily Processing

9.2 billion messages
2.4 billion spam messages blocked
660 billion requests
1.9 trillion item read/opened

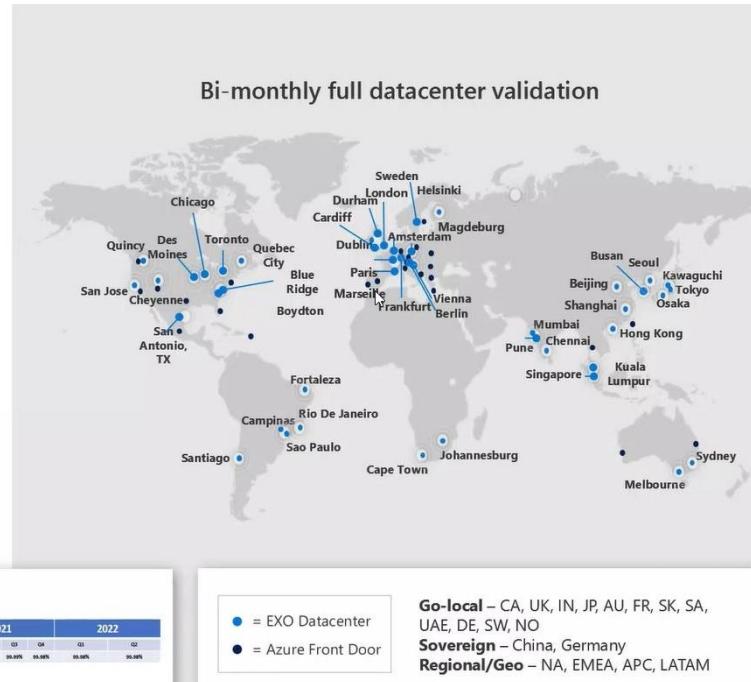


Figure 5-1: The scale of Exchange Online (source: Microsoft – MEC 2022 conference)

The number of Exchange Online servers grows in line with the number of Microsoft 365 accounts. At the Ignite conference in October 2018, Microsoft said that Exchange Online used 175,000 physical servers. Four years later, at the MEC 2022 conference, Microsoft reported that the number of Exchange Online servers had increased to over 300K (all physical servers), the number of data centers supporting Exchange Online had

grown to 175, and 210 network point of presence (POPs) existed to carry client traffic to Microsoft's data center network (Figure 5-1). The email infrastructure spanned 7.3 billion mailboxes and delivered 9.2 billion messages and blocked 2.4 billion spam messages daily. Exchange Online databases hold 42 trillion items in 1.4 exabytes of data, with each mailbox replicated four times by the Database Availability Groups running on the mailbox servers.

So Many Mailboxes

Microsoft's claim for Exchange Online to span 7.3 billion mailboxes seems enormous in the context of 345 million paid Office 365 subscriptions, but the figure includes Outlook.com users ([400 million switched over to use the Exchange Online infrastructure in 2017](#)), shared mailboxes, archive mailboxes, group mailboxes, resource mailboxes, and special cloud-only and system mailboxes managed by the Microsoft 365 substrate for compliance and other purposes. Although you can't report the mailboxes used by the substrate, some insight into the diversity of accounts used by Exchange Online is seen by running the *Get-User* cmdlet to report the count of the different user types found in a tenant:

```
Get-User | Group-Object RecipientTypeDetails -NoElement | Sort-Object Count -Descending
```

Count	Name
166	GuestMailUser
131	UserMailbox
23	SharedMailbox
13	RoomMailbox
4	SchedulingMailbox
3	DiscoveryMailbox
3	TeamMailbox
3	User
2	EquipmentMailbox
1	MailUser

Discounting *GuestMailUser* (Entra ID B2B Collaboration guest users), *User* (accounts not licensed to use Exchange Online), and *MailUser* (a mail-enabled user in another organization), the user types reported here are:

- **UserMailbox:** Regular user mailboxes.
- **SharedMailbox:** Shared mailboxes.
- **RoomMailbox:** Room mailboxes (Outlook places).
- **SchedulingMailbox:** Used by the Bookings app to hold appointments.
- **DiscoveryMailbox:** Used to hold the results of Exchange discovery searches. These mailboxes are now largely obsolete. However, they cannot be removed until the associated searches are no longer required.
- **TeamMailbox:** Used by the obsolete site mailboxes feature. Microsoft retired site mailboxes in April 2021. These mailboxes might still exist because they are subject to a retention hold.
- **EquipmentMailbox:** Used for the calendar for room equipment like a TV set. These objects are not in heavy use today.

Notice that group mailboxes, used by Microsoft 365 Groups (Outlook Groups, Teams, and Yammer) do not feature on this list. That's because Exchange Online treats Microsoft 365 Groups like distribution lists rather than mailboxes. Inactive mailboxes are not on this list because they are user mailboxes in an inactive state rather than a certain type of mailbox.

Apart from user mailboxes, people don't sign into the accounts used with these objects. The accounts exist to support permissions, such as the ability to access a shared mailbox. This brief discussion illustrates the point that user mailboxes are not the only mailboxes and accounts used by Exchange Online.

Exchange Online and Outlook.com

Exchange Online and Outlook.com share the same physical infrastructure. Outlook.com users receive service from mailboxes running on Exchange Online servers and connect to their mailboxes using a modified version of OWA. The functionality exposed in the consumer version of OWA is controlled to ensure that consumer accounts do not have the same level of functionality that's available to Exchange Online users; it's also segmented in terms of the functionality available to premium and free accounts. However, functionality developed for one platform does show up in the other. For example, the Sweep feature first appeared in Outlook.com before Microsoft decided to make it available to Exchange Online users. On the other hand, the Encrypt email feature first appeared in Exchange Online before it showed up in Outlook.com. Sharing the same physical infrastructure makes it very easy for Microsoft to switch features between the consumer and business platforms.

Exchange Online Data Center Operations

Unlike the other Microsoft 365 services, Exchange Online still uses physical servers. The servers in the available pool receive updates on a rolling basis. Up to 10% of the servers are offline at any point. An on-premises administrator who paid a visit to a data center and reviewed how Microsoft runs Exchange Online would see some very familiar things, but many operation details are very different. The fundamentals of running a messaging system stay the same – users authenticate against Entra ID to connect to mailboxes to receive and send emails. Messages exist in databases on Exchange mailbox servers and are transported to their destination via transport servers. Connectors link servers together and to the rest of the Internet via SMTP. Database replication hums along in the background to ensure that copies of user mailboxes are in four databases spread across at least two data centers. Apart from the sheer size of the infrastructure to support both Exchange Online and Outlook.com, the structure of mailboxes in databases running in Database Availability Groups spread across mailbox servers is very recognizable.

The Largest Migration? In February 2021, the [UK National Health Service](#) (NHS) completed the migration of 2.1 million mailboxes from on-premises servers to Exchange Online. About 2.3 petabytes of data was moved over six months at rates of up to 83,000 mailboxes daily. The NHS is the largest single Office 365 tenant. As far as we know, this is the largest mailbox migration to Exchange Online performed to date.

Native Data Protection

Many people are struck by the fact that Microsoft does not backup the Exchange Online mailbox databases. Instead, Native Data Protection, a resiliency strategy formed by many different features incorporated into the Database Availability Groups, Information Store service, and transport service, protects data and removes the need for backups.

Database Availability Groups

The Database Availability Group (DAG) is the cornerstone of Exchange Online storage. Mailboxes are stored in mailbox databases deployed in a DAG. Each DAG has sixteen mailbox servers spread across the data centers within a region. For instance, within the EMEA region, DAG member servers are in the Amsterdam, Dublin, Helsinki, and Vienna data centers. Each mailbox database has four copies distributed across servers in the data centers. Email clients access the active database copy while the three other copies, one of which is lagged (kept seven days behind the active copy), synchronize with the active copy using log shipping and replay. Exchange captures transactions in transaction logs. Log shipping copies transaction logs generated by the active database copy to the servers holding passive copies. The target servers check the transaction logs as they arrive, and if the logs are valid, replay their contents to update the passive copy.

Because Microsoft's high-speed data center network connects the DAG member servers, log copy and replay operations are almost instantaneous. If a problem occurs with the active server, Exchange decides which of the passive copies to activate and switches it to service client connections. The previously active server then becomes a host for a passive copy.

Exchange Online servers use the ReFS file system (available in Windows Server 2012 or later) to gain better protection for data and to verify the integrity of data written to disk. The Exchange servers use a mixture of SSD (for the metacache) and JBOD RAID arrays and can automatically swap a replacement disk into an array should one fail.

Database Engine Checks

Apart from log shipping and replay (which include consistency checks), the DAG includes other features to ensure that physical or logical corruption does not creep into databases. These include:

- **Single-bit correction:** The database engine detects and fixes single-bit CRC errors that result from hardware problems. The errors are corrected and flagged so that Microsoft's operations team can investigate.
- **Database consistency checker:** A background process reads and checks database pages for checksum failures. Any failed page is automatically fixed. The scheme used makes sure that every page is checked in a database every seven days.
- **Lost flush detection:** Lost flushes happen when the operating system (or disk) reports that a write happened, but the write operation did not complete (or is written to the wrong place). This represents logical corruption. To prevent this from happening, the database engine checks pages as it writes them to passive database copies. If a problem is found, it is fixed through single page patching.
- **Single page patching:** This is a process to replace bad database pages with good pages from other database copies in the DAG. If the problem is detected in a passive copy, the database engine copies the good page from the active database using the transaction log shipping and replay mechanism. If the problem is in the active database, the good page can come from any passive copy.

These features also exist in the on-premises version of Exchange.

Other Exchange Resiliency Features

In addition to the DAG and database engine features, Exchange builds resilience into the transport service so that messages are always sent, even when failures occur. Shadow Redundancy means that the transport service takes a (shadow) copy of each message it receives. If Exchange ever thinks that a message might not have been processed, it can resubmit the shadow copy. The Safety Net queue captures copies of messages as they pass through the transport pipeline. If a failure occurs in the transport service or with a database, Exchange can replay messages from the Safety Net queue to the active database copy. Any redundant copies discovered during the replay are suppressed and not exposed to users.

Behind the scenes, Exchange Online servers are rebalanced on an ongoing basis to ensure that each takes approximately the same amount of user load. In addition, Microsoft withdraws mailbox servers from service to update their software as the need arises. When this happens, Microsoft moves mailboxes to other databases using the Mailbox Replication Service (MRS). During the moves, MRS checks mailbox contents for problems and if it detects problem items, it attempts to correct the items. If this isn't possible, MRS skips the corrupt items.

Tenant-Controlled Resiliency Features

Tenants can control some mailbox management features that assist in resiliency. These include:

- **Single Item Recovery** (SIR): This feature ensures that Exchange Online retains messages that users purge (hard delete) in the Recoverable Items folder of mailboxes until the deleted item retention period expires. The maximum deleted item retention period is 30 days.
- **In-place and Litigation holds:** Holds make sure that Exchange keeps select items or all items in a mailbox for the set retention period. If a mailbox is deleted when it is subject to a hold, it becomes inactive, meaning that it is retained until the hold elapses. Holds can also be set by retention policies.
- **Large mailbox quotas:** Enterprise Office 365 plans include 100 GB mailbox quotas. In effect, many users do not need to delete messages. If they do, the messages go into the Deleted Items folder and stay there until the user empties the folder. Even then, the deleted items go into the Recoverable Items folder (which can have another 100 GB quota) from where users and administrators can recover items for up to 30 days (the deleted items retention period).
- **Expanding archives:** Mailboxes can be archive-enabled. An archive mailbox stores data for the long-term storage and its basic quota is 100 GB. However, tenants can opt for auto-expanding archives, which means that the archive is composed of 50 GB "chunks" linked into a logical entity.
- **Retention labels and policies:** To keep important information for defined periods, users can apply retention labels to folders and items. Exchange Online does not remove items under retention control until the retention period elapses. See the Compliance chapter for more information about Microsoft 365 retention policies and processing.

The combination of the DAG, database copies, database engine features, transport copies, and tenant-controlled resiliency features are enough for Microsoft to conclude that they do not need backups for Exchange Online mailbox data. Microsoft 365 Backup offers some advantages because it can recover mailbox contents very quickly using data stored online and protected by native data protection. The downside is that Microsoft 365 Backup does not satisfy the requirement set by many organizations to hold a copy of user data in another location. See the discussion in the tenant management chapter for more information.

Your situation might be different, but in many cases, tenants do not need to invest in a backup service either (Microsoft 365 Backup or a third-party alternative). Instead, full consideration should be given to how to maximize the use of out-of-the-box functionality to decide if Native Data Protection meets the perceived need for backups.

Managing Mailboxes

Exchange Online mailboxes hold a mixture of default, system, and user-created folders. The default folders are the set of well-known folders like the Inbox that exist in every mailbox. Some people only ever use a small set of default folders – Inbox, Sent Items, and Deleted Items – while others are dedicated filers and store items away in carefully-selected folders. Colloquially, the two types of users are “pilers” and “filers.” If its limits are respected, Exchange doesn’t care how data are organized in a mailbox. Limits for internal mailbox structures include:

- Maximum number of items per mailbox folder: 1 million
- Maximum number of items in the Recoverable Items folder: 3 million
- Maximum number of subfolders per mailbox folder: 10,000 (including the root folder)
- Maximum folder hierarchy depth: 300

Most mailboxes won’t encounter an internal limit, but many have exceeded their storage quota. The accounts for user mailboxes must have a suitable license to access Exchange Online. Shared mailboxes need licenses if they use more than 50 GB storage or are archive-enabled.

You’ll find that we use PowerShell to manage many mailbox settings. To run these commands, you must connect a session to the [Exchange Online Management](#) endpoint.

Unique Mailbox Identifiers

In early 2022, Microsoft announced a change in the way that Exchange Online generates the Name and Distinguished Name properties for new mailboxes owned by Entra ID accounts. Instead of using the *MailNickname* property from the Entra ID account as the basis for the *Name* and *DistinguishedName* properties, Exchange uses the Entra ID object identifier for the account when it creates new mailboxes. EXODS stores the object identifier (also called EDOID) for Entra ID accounts and groups in the *ExternalDirectoryObjectId* property. Mailboxes belonging to on-premises Active Directory accounts aren't affected by the change, which eventually came into force in early 2023.

The aim is to guarantee uniqueness for the *Name* and *DistinguishedName* properties to avoid issues when account data synchronizes from Entra ID to Exchange Online when accounts are homed on-premises. The problem arises because Active Directory creates objects in multiple organizational units whereas Entra ID creates objects in a single organizational unit named after the tenant. Thus, an Active Directory object with a *Name* property of *John.Smith* will cause a synchronization conflict if a similarly named object exists in a different organizational unit. Because Exchange Online stores the EDOID in the *Name* property for new mailboxes, including those created as remote mailboxes from the on-premises EAC, Entra ID no longer synchronizes the *Name* property with Active Directory.

The example below illustrates the new format for the *Name* and *DistinguishedName* properties:

```
Get-ExoMailbox -Identity b67c8bd7-a8d3-4358-b42f-cd51821f7ba3 -Properties Name  
  
ExternalDirectoryObjectId : b67c8bd7-a8d3-4358-b42f-cd51821f7ba3  
UserPrincipalName : Sue.P.Pickett@office365itpros.com  
Alias : Sue.P.Pickett  
DisplayName : Sue Pickett  
Name : b67c8bd7-a8d3-4358-b42f-cd51821f7ba3  
DistinguishedName : CN=b67c8bd7-a8d3-4358-b42f-cd51821f7ba3,  
OU=Office365itpros.onmicrosoft.com,OU=Microsoft Exchange Hosted  
Organizations,DC=EURPRO4A002,DC=prod,DC=outlook,DC=com
```

Exchange Online did not update the properties of mailboxes created before the change became effective. However, if you want, you can update mailbox properties. For example:

```
$ExternalDirectoryObjectId = Get-ExoMailbox -Identity Kim.Akers@Office365itpros.com | Select -  
ExpandProperty ExternalDirectoryObjectId  
Set-Mailbox -Identity $ExternalDirectoryObjectId -Name $ExternalDirectoryObjectId
```

After updating the *Name* property, Exchange Online updates the Distinguished Name property to match. If you don't like using a GUID in the *Name* property, you can reverse the change by running the *Set-Mailbox* or *Set-User* cmdlets to update the property with another value.

General Mailbox Configuration

The *Get-MailboxMessageConfiguration* and *Set-MailboxMessageConfiguration* cmdlets retrieve and set the general properties of a mailbox. These settings control how OWA behaves. Although some are also respected by Outlook, you'll have to use a Group Policy Object or the [Office cloud policy service](#) to exert any real control over Outlook settings, including the roaming client settings supported by Outlook for Windows which are stored in mailboxes.

An example of how to use the *Set-MailboxMessageConfiguration* cmdlet is to create an autosignature for OWA to apply to new messages. This code defines some basic text for the autosignature and sets the default format for new messages created with OWA to "Plain text" (rather than the default HTML):

```
Set-MailboxMessageConfiguration -Identity "Kim Akers" -AutoAddSignature $True  
-SignatureText "From the desk of Kim Akers" -DefaultFormat PlainText
```

The equivalent command to create an HTML-format signature is shown below. In this instance, some simple HTML code creates the autosignature. The last parameter suppresses autosignatures for replies.

```
Set-MailboxMessageConfiguration -Identity "Kim Akers" -AutoAddSignature $True  
-SignatureHTML "<h3>From the Desk of Kim Akers</h3>" -DefaultFormat HTML -AutoAddSignatureOnReply  
$False
```

This is a simple example of creating a signature for OWA. You can download [a more comprehensive script from GitHub](#) to create a customized signature for every mailbox in the tenant. The signature includes user properties (name, title, etc.), a company logo, a clickable link for the user's email address, and links for Facebook and Twitter. Only OWA uses the signature defined by `Set-MailboxMessageConfiguration`; Outlook or Outlook Mobile use different autosignatures. If you want to stop users changing the signature using OWA options after updating it in their mailboxes, you can do so using the technique [explained in this article](#).

Other common settings that you might consider updating for mailboxes include:

- **AlwaysShowBCC**: Display the *BCC*: control when composing new messages.
- **AlwaysShowFrom**: Display the *From*: control when composing new messages.
- **CheckForMissingAttachments**: If True, OWA checks messages before sending to check for the presence of attachments based on message text.
- **EmailComposeMode**: Set to *Inline* (default) to compose new messages in a pane within the same windows or *SeparateForm* to always launch a separate window for new messages.
- **EmptyDeletedItemsOnLogoff**: Controls whether OWA empties the Deleted Items folder when the user logs out.
- **HideDeletedItems**: Controls whether deleted items appear in conversation views. By default, clients show deleted items, so this property is set to `$False`. Both Outlook and OWA respect this property.
- **IsReplyAllTheDefaultResponse**: Controls whether reply-all is the default response for messages. If `$True`, a response to a message includes all recipients (this is the default value). Set the property to `$False` to force OWA to create responses only addressed to the sender of the original message.
- **ReadReceiptResponse**: Controls how OWA generates read receipts for new messages delivered to the mailbox. The values are *DoNotAutomaticallySend* (prompt), *AlwaysSend*, and *NeverSend*. This setting applies only to OWA. See [this article for an explanation](#) of how read receipts work and how to control the relevant settings for OWA and Outlook.
- **NewItemNotification**: Set to *All* (default) to instruct OWA to signal the arrival of new messages (divided into the categories of email, fax, and voicemail) in every way that it can. Other values include *Sound* (a tone announces the arrival) and *EmailToast* (a pop-up "toast" notification signals the arrival).
- **PreviewMarkAsReadBehavior**: Controls how OWA sets the read status of messages. The default is *OnSelectionChange*, meaning that OWA marks a message as read if the user selects another message. If set to *Delayed*, OWA marks the item as read if the user spends more than the time specified in the **PreviewMarkAsReadDelayTime** property (by default, 5 seconds). You can also set this value to *Never*, meaning that the unread status of a message never changes no matter what the user does in the preview pane.
- **MailSendUndoInterval** sets how long OWA waits before sending a message. The interval allows the sender to stop the message if they've made a mistake or need to add something.

New parameters regularly appear for the `Set-MailboxMessageConfiguration` cmdlet as Microsoft increases the range of OWA options available for clients.

Signature Management: Apart from allowing users to create autosignatures using their client of choice, three methods exist to control autosignatures.

1. Use an Exchange transport rule to insert an autosignature. This method has the advantage that it works for all clients and can use data extracted from Entra ID to populate the autosignature.

2. Use a commercial ISV product to manage autosignatures. Examples of ISVs that provide this service include [CodeTwo Signatures](#), [Exclaimer](#), and [Outlook Signatures](#). ISV products cost, but they are very capable and provide the ability to manage autosignatures much more easily than is possible with either PowerShell or transport rules.
3. Develop tenant-specific code to deploy autosignatures to mailboxes using the `Set-MailboxMessageConfiguration` cmdlet. This approach only works for OWA and the Monarch client.

Mailbox Regional Settings

When you create a new Microsoft 365 account and license the account for Exchange Online, the mailbox does not inherit regional properties from the country or service location defined for the user account. Regional properties define the language used by OWA, the mailbox owner's time zone, and their preferred date format. Collectively, regional settings allow users to choose their preferred language no matter what country they work in. For instance, Belgian users might choose Flemish, French, German, English, or any of the other language options supported by OWA.

New mailboxes do not inherit regional settings from the user account. Instead, the first time the mailbox owner signs in, OWA applies default settings based on the tenant location, including the default mailbox folders. For instance, mailboxes that use the English language have an *Inbox* folder, while the same folder in mailboxes configured for French use *Boîte de réception*.

If you connect to a brand-new mailbox with an Outlook desktop or a mobile client, the mailbox takes the language setting of the client and creates the default folders based on that value. This happens without changing the other regional settings. Mailbox owners can use the Outlook settings option to update regional settings at any time. If they choose a different language, OWA offers the option to update the folder names.

Administrators can run the `Set-MailboxRegionalConfiguration` cmdlet to tweak the regional settings used by OWA. In this example, the selected mailbox language, time zone, and date and time formats match the settings for a Dutch user working in the Netherlands. Notice the use of the `LocalizeDefaultFolderName` parameter, set to `$True` to force Exchange Online to create default folder names in Dutch for the mailbox:

```
Set-MailboxRegionalConfiguration -Identity 'Rob Young' -Language nl-NL -TimeZone 'W. Europe Standard Time' -DateFormat 'd-M-yyyy'-TimeFormat 'HH:mm' -LocalizeDefaultFolderName:$True
```

It's important to have the correct time zone set for an account because it's used by applications. For example, Teams displays the local time for a user in their profile card to help other people to decide if it's an appropriate time for a chat or meeting. The `Get-MailboxRegionalConfiguration` cmdlet displays the default regional settings for a mailbox:

```
Get-MailboxRegionalConfiguration -Identity 'Rob Young'
```

Exchange Online is picky about the date and time formats used when updating mailbox regional configurations. The formats must be valid for the selected language. Sometimes it can be difficult to know what acceptable values are for date and time formats. A practical approach is to use OWA to change the regional settings for a mailbox and then examine the values for the mailbox's regional configuration. You can then reuse those values with other mailboxes. To know the values for the timezone setting, you can run this PowerShell code to report the values stored in the system registry:

```
$TimeZone = Get-ChildItem "HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Time zones" | ForEach {Get-ItemProperty $_.PSPPath}; $TimeZone | Sort-Object Display | Format-Table PSChildname, Display -Auto
```

It's possible to use PowerShell to check the various language settings used by Entra ID and Exchange Online for accounts and mailboxes to detect possible inconsistencies that might exist. Here's some code to generate a report:

```
$Report = [System.Collections.Generic.List[Object]]::new()
[array]$Users = Get-MgUser -Filter "assignedLicenses/$count ne 0 and userType eq 'Member'" -ConsistencyLevel eventual -CountVariable Records -All -PageSize 999
ForEach ($User in $Users) {
    Write-Host ("Processing account {0}" -f $User.DisplayName)
    $RegionalSettings = $Null
    $RegionalSettings = Get-MailboxRegionalConfiguration -Identity $User.UserPrincipalName -ErrorAction SilentlyContinue
    $CountryOrRegion = (Get-User -Identity $User.UserPrincipalName -ErrorAction SilentlyContinue) | Select-Object -ExpandProperty CountryOrRegion
    If ($RegionalSettings) {
        $ReportLine = [PSCustomObject]@{
            User                  = $User.UserPrincipalName
            DisplayName          = $User.DisplayName
            Country              = $User.Country
            "Preferred Language" = $User.PreferredLanguage
            "Usage Location"     = $User.UsageLocation
            "Country or region"  = $CountryOrRegion
            Language              = $RegionalSettings.Language.DisplayName
            DateFormat            = $RegionalSettings.DateFormat
            TimeFormat            = $RegionalSettings.TimeFormat
            TimeZone              = $RegionalSettings.TimeZone }
        $Report.Add($ReportLine)
    }
}
$Report | Sort-Object DisplayName | Out-GridView
```

Auto replies and Out of Office Notifications

Out of Office or OOF ([Out of Facility](#)) are names used for the autoreply feature which allows Exchange to send automatic replies after delivering new messages to user and shared mailboxes. Users receive autoreply messages when they send emails to mailboxes that have an autoreply message configured and enabled. Exchange Online also displays a recipient's autoreply in clients like Outlook desktop when adding the recipient to a message.

The *Get-MailboxAutoReplyConfiguration* and *Set-MailboxAutoReplyConfiguration* cmdlets retrieve and set the autoreply settings for a mailbox, including shared mailboxes. To discover the set of mailboxes with autoreply set and the time the autoreply lapses, use the following command:

```
Get-ExoMailbox -RecipientTypeDetails UserMailbox, SharedMailbox | Get-MailboxAutoReplyConfiguration | Where {$_.AutoReplyState -eq "Scheduled" -or $_.AutoReplyState -eq "Enabled"} | Format-List MailboxOwnerId, StartTime, InternalMessage
```

The first check looks for auto-replies scheduled for a specific period, the second finds mailboxes where the autoreply is enabled without dates. The *InternalMessage* property reveals the HTML-formatted text of the auto-reply message for internal correspondents (*ExternalMessage* holds the text seen by external correspondents).

Setting Autoreply for Mailboxes

You can use the *Set-MailboxAutoReplyConfiguration* cmdlet to create an autoreply for a user who has gone on vacation and forgotten to let anyone know. Another scenario is when public holidays occur, and you want to set the autoreply for customer-facing shared mailboxes to let anyone who sends an email to the company know about the potential for a delayed response. In both cases, you enable autoreply, set a time limit, and create separate auto-reply text for internal and external audiences. You can also instruct Exchange Online that

auto-replies go only to external people who are contacts of the mailbox owner (select *All* instead of *Known* if you want the auto-reply to go to anyone external who sends a message to the mailbox).

If you create an autoreply for a certain period, make sure that you set the *AutoReplyState* parameter to "Scheduled" rather than "Enabled." Failure to schedule the autoreply enables it immediately rather than in the future. Exchange Online servers use universal time (UTC), so if you specify a time (rather than just a date) in the start and end times, make sure that you convert the time into UTC. For example, the command below starts auto-replies at 19:30 UTC and ceases at 17:00 UTC on the respective dates.

```
Set-MailboxAutoReplyConfiguration -Identity "Kim Akers" -StartTime "04-Nov-2019 19:30"
-AutoReplyState "Scheduled" -EndTime "08-Nov-2019 17:00" -InternalMessage "Kim Akers is attending
the Microsoft Ignite event in Orlando and will respond to your message after she returns on November
10" -ExternalMessage "Kim Akers is on vacation" -ExternalAudience 'Known'
```

Note that when you view the autoreply configuration for a mailbox, PowerShell converts the times from UTC into the time zone applied to the local workstation. To turn off autoreply for a user, set the *AutoReplyState* property to "Disabled":

```
Set-MailboxAutoReplyConfiguration -Identity "Kim Akers" -AutoReplyState Disabled
```

Here's another example. In this case, we want to add auto-replies to all shared mailboxes to cover the period of a public holiday so that anyone who sends a message to the mailboxes will receive a reply to tell them that the user's out of the office. Some basic HTML formats the text for the auto-replies. Finally, the command creates an event called "August Holiday" in user calendars.

```
$HolidayStart = "04-Aug-2023 17:00"
$HolidayEnd = "6-Aug-2023 09:00"

$InternalMessage = "Expect delays in answering messages to this mailbox due to the holiday between
<b>" + $HolidayStart + "</b> and <b>" + $HolidayEnd + "</b>"
$ExternalMessage = "Thank you for your email. Your communication is important to us, but please be
aware that some delay will occur in answering messages to this mailbox due to the public holiday
between <b>" + $HolidayStart + "</b> and <b>" + $HolidayEnd + "</b>"

$Mbx = (Get-ExoMailbox -RecipientTypeDetails SharedMailbox | Select DisplayName, Alias,
DistinguishedName)
ForEach ($M in $Mbx) {
    # Set auto reply
    Write-Host "Setting auto-reply for shared mailbox:" $M.DisplayName
    Set-MailboxAutoReplyConfiguration -Identity $M.DistinguishedName -StartTime $HolidayStart
    -AutoReplyState "Scheduled" -EndTime $HolidayEnd -InternalMessage $InternalMessage -ExternalMessage
    $ExternalMessage -ExternalAudience 'All' -CreateOOEvent:$True -OOEventSubject "August Holiday"}
```

Autoreply Settings for Calendar Processing

OWA includes some settings to process incoming calendar requests during periods when autoreply is active for a mailbox. These settings are not yet visible to Outlook, but because they are acted upon by the server, their effect is felt when set by OWA. The options are:

- **Block my calendar for this period:** Other users will see this user's calendar as blocked out if they try to schedule a meeting during the period when autoreply is active. The *CreateOOEvent* switch set by *Set-MailboxAutoReplyConfiguration* determines if Exchange creates a calendar event corresponding to the OOF period.
- **Automatically decline new invitations for events that occur during this period:** If new event invitations arrive, they can be automatically declined. The *AutoDeclineFutureRequestsWhenOOF* property controls this setting.
- **Decline and cancel my meetings during this period:** This option scans the user's calendar for meetings that are in place for the period when the autoreply will apply. Meetings that the user was

invited to attend will be declined while meetings that they set up will be canceled. The *DeclineAllEventsForScheduledOOF* property controls this setting.

The settings can be controlled with PowerShell using the *Set-MailboxAutoReplyConfiguration* cmdlet.

Calendar Configuration

The *Get-MailboxCalendarConfiguration* and *Set-MailboxCalendarConfiguration* cmdlets manage calendar settings. For example, this command configures the calendar to use Greenwich Mean Time (GMT) as the time zone with a starting time for the workday of 8:30 A.M.:

```
Set-MailboxCalendarConfiguration -Identity "Kim Akers" -WorkingHoursTimeZone "GMT Standard Time"
-WorkingHoursStartTime 08:30:00
```

The cmdlet also controls the appearance of a user's calendar when viewed through OWA (Outlook uses different settings based on the time and time zone configured for the PC). For example, this command makes Monday the first working day of the week, starts a new year on the first day of the year, changes the default time increment from 30 minutes to 15 minutes, sets the weather unit to be Celsius, and defines the user's location to be County Dublin, Ireland. Figuring out the right longitude and latitude for a user's location might seem hard, but online tools help (like [this example](#)) or you can experiment by inputting different locations into the Weather section of the OWA Calendar options and noting what values are set.

```
Set-MailboxCalendarConfiguration -Identity "Kim Akers" -WeekStartDay Monday
-FirstWeekOfYear FirstDay -TimeIncrement FifteenMinutes -WeatherUnit Celsius
-WeatherLocations "{LocationId:9480;Name Dublin, County Dublin;Latitude:53.348;Longitude:-6.248}"
```

You can also use *Set-MailboxCalendarConfiguration* to control the scheduling of Teams online meetings by default by Outlook clients. A mailbox setting is available to override the organization setting created using *Set-OrganizationConfig*, but only for OWA and Outlook Mobile clients. Outlook desktop uses a different method to control if online meetings are the default for an individual account. This example sets online meetings as the default for the specified mailbox:

```
Set-MailboxCalendarConfiguration -OnlineMeetingsByDefaultEnabled $True -Identity Kim.Akers
```

Calendar Permissions

While granting delegate access via Outlook or OWA are the normal ways for users to allow other people access to a folder like their calendar, administrators can run the *Add-MailboxFolderPermission* cmdlet to do the same. For example, this command gives delegate access to Michael Harty for the calendar of Kim Akers. The Editor access right is needed to create and edit items in the folder, and the sharing permission flags tell us that the delegate can see private items in the target calendar. In this case, *SendNotificationToUser* is specified to send a sharing notification to the new delegate to tell them that they can now access someone else's calendar. In some cases, you will not want to generate a sharing notification as the potential exists that the recipient might unwittingly refuse the invitation.

```
Add-MailboxFolderPermission -Identity Kim.Akers@office365itpros.com:\Calendar -User
Michael.Harty@office365itpros.com -AccessRights Editor -SharingPermissionFlags Delegate,
CanViewPrivateItems -SendNotificationToUser $True
```

FolderName	User	AccessRights	SharingPermissionFlags
Calendar	Michael Harty	{Editor}	Delegate, CanViewPrivateItems

To remove delegate access from a mailbox, run the *Set-MailboxFolderPermission* cmdlet and set the *SharingPermissionFlags* parameter to None.

Exchange holds details of delegate access in a hidden item in the user mailbox. Sometimes this item can become corrupted, and the user will no longer be able to add or remove delegates. In this case, you should run the *Remove-MailboxFolderPermission* cmdlet with the *ResetDelegateUserCollection* parameter to force Exchange to recreate the hidden item.

```
Remove-MailboxFolderPermission -Identity Kim.Akers@office365itpros.com:\Calendar  
-ResetDelegateUserCollection
```

This action has the side-effect of removing the flags which enable delegate access. To complete the fix, you must recreate the delegate settings with *Set-MailboxFolderPermission*. For example, this command re-establishes Michael Harty as a delegate to manage the calendar in the mailbox of Kim Akers.

```
Set-MailboxFolderPermission -Identity Kim.Akers@office365itpros.com:\Calendar -User  
Michael.Harty@office365itpros.com -AccessRights Editor -SharingPermissionFlags Delegate,  
CanViewPrivateItems
```

Viewing Details of User Availability

By default, Exchange Online makes limited free and busy information for mailboxes available to other tenant users to allow them to see when other people might be able to attend a meeting. The default setting is *AvailabilityOnly*, meaning that a user can see when someone is busy, but can't see any details about the reserved time slot. Many organizations choose to upgrade the setting to allow people to see details of slots reserved in other users' calendars. There's no organization-wide setting to control how the calendar works. Instead, you must update the permission granted to the special Default user for each calendar. The *Set-MailboxFolderPermission* cmdlet can update the permission. For instance, this code looks for mailboxes to update and runs *Set-MailboxFolderPermission* to update the access rights for the calendar folder for the Default user to *LimitedDetails*. The *LimitedDetails* value allows other users to see the title, location, and status (out of office, tentative, etc.) for time slots.

```
# Find mailboxes that we have not yet reset the default sharing view  
[array]$Mbx = Get-ExoMailbox -RecipientTypeDetails UserMailbox, RoomMailbox -ResultSize Unlimited -  
Filter {CustomAttribute13 -ne "Open" -and CustomAttribute13 -ne "Blocked"}  
$CalendarName = "Calendar" # English language calendar folder  
ForEach ($M in $Mbx) {  
    Write-Host "Processing" $M.DisplayName  
    # You can hard-code the calendar name (above) or try and find a local language value.  
    # This is one way to look for local values...  
    # $CalendarName = (Get-ExoMailboxFolderStatistics -Identity $M.UserPrincipalName -FolderScope  
    # Calendar | Where-Object {$_.FolderType -eq "Calendar"}).Name  
    # Either way, you need to end up with a valid calendar folder reference  
    # - like Tony.Redmond@office365itpros.com:\Calendar  
    $CalendarFolder = $M.UserPrincipalName + ":" + $CalendarName  
    Set-MailboxFolderPermission -Identity $CalendarFolder -User Default -AccessRights LimitedDetails  
    Set-Mailbox -Identity $M.ExternalDirectoryObjectId -CustomAttribute13 "Open"  
} # End Foreach
```

Users might not use English-language versions of OWA or Outlook, in which case their Calendar folder might have a different name. The code above handles the situation by using the *Get-ExoMailboxFolderStatistics* cmdlet to look for the calendar folder and fetch its name. This cmdlet is expensive in terms of processing overhead, which is why the call is commented out. However, if you need to deal with multiple languages, you'll need to uncomment the command and take the hit.

After updating the permission, the code uses *Set-Mailbox* to update the *CustomAttribute13* attribute so that the next time it runs, it won't process this mailbox. In addition, the code ignores any mailbox with Blocked in *CustomAttribute13* to handle the situation where you don't want to share calendar details for some confidential mailboxes.

Automatic Meeting Shortening

Meeting shortening means reducing the time assigned to an event by a set amount depending on its desired length. The idea is to allow users to have a buffer between meetings to have an opportunity to recharge before the next event. Outlook and OWA allow individual users to set how long they would like to reduce short (under an hour) and long (over an hour) meetings and whether the buffer should be at the start or end of the period. Tenants can apply default settings by updating the Exchange Online organization configuration with PowerShell. It's critical to understand that once a user selects their settings, the organization defaults do not apply to them.

Three organization-wide settings are available to control event shortening:

- **ShortenEventScopeDefault:** Sets whether event shortening is in effect (0 or none) or applies to ending meetings early (1 or *EndEarly*) or starting later (2 or *StartLate*). This parameter must be set to 1 or 2 before you can amend the periods.
- **DefaultMinutesToReduceShortEventsBy:** The number of minutes to shorten events by if they are scheduled for one hour or less. The default is 5.
- **DefaultMinutesToReduceLongEventsBy:** The number of minutes to shorten events by if they are scheduled for over one hour. The default is 10.

To turn on event shortening for the organization and select to end events early, we run:

```
Set-OrganizationConfig -ShortenEventScopeDefault EndEarly
```

Using *Get-OrganizationConfig* to examine the settings afterward shows the current configuration:

```
Get-OrganizationConfig | fl defaultmin*, short*
DefaultMinutesToReduceShortEventsBy : 5
DefaultMinutesToReduceLongEventsBy : 10
ShortenEventScopeDefault          : EndEarly
```

Like any organization-wide setting, some time is necessary to allow clients and servers to pick up new values. Administrators can update these settings for individual mailboxes using the *Set-MailboxCalendarConfiguration* cmdlet. Individual mailbox settings override tenant-wide settings. This command updates a mailbox to end long events 15 minutes early and short events 10 minutes early.

```
Set-MailboxCalendarConfiguration -Identity Chris.Bishop -ShortenEventScopeDefault "End_Early"
-DefaultMinutesToReduceLongEventsBy 15 -DefaultMinutesToReduceShortEventsBy 10
```

Processing Inbound Calendar Requests for Mailboxes

The *Set-CalendarProcessing* cmdlet controls how the resource booking assistant processes meeting requests sent to user and room mailboxes. For example, this command sets the properties controlling the processing of forwarded meeting notifications and external meeting requests:

```
Set-CalendarProcessing -Identity "Kim Akers" -RemoveForwardedMeetingNotifications $True
-ProcessExternalMeetingMessages $True
```

It's common to have conference rooms reserved for use by specific people. To accomplish the goal, we update the calendar processing configuration to block accepting requests from anyone except members of a distribution list:

```
Set-CalendarProcessing -Identity "Room 101" -BookInPolicy "Senior Leadership Team"
```

Users who attempt to book a room receive email responses to tell them if the calendar assistant has accepted or denied their request or when the request awaits approval by a delegate who manages reservations for the

room. You can update the meeting responses by setting the *AddAdditionalResponse* switch to *\$True* and providing the text to insert into the responses in the *AdditionalResponse* property.

This example shows how to add HTML-formatted text to the response generated for meeting requests, including an emoji fetched from a website along with other settings to exert precise control over how the resource booking assistant handles inbound requests. Some settings can be configured for room mailboxes through the resources section of the Exchange admin center. However, the settings exposed in the Exchange admin center only cover the most basic options (allow repeated meetings, schedule during working hours, duration of events, response text, and booking window). PowerShell is the only way to control in-policy automatic processing and the subjects stored for events in the room calendar:

```
Set-CalendarProcessing -Identity "Room 101" -AutomateProcessing AutoAccept  
-AddAdditionalResponse $True -AdditionalResponse '<h2>Welcome to the Corporate Room Scheduling  
System</h2><p>We have a few basic rules for you to follow.</p><ol><li>Please keep the room tidy and  
remove rubbish at the end of your meeting.</li><li>Please do not change the settings of the AV  
equipment.</li><li>Please clean the whiteboard before you leave.</li><li>Advise Corporate Meetings  
if you have any problems by sending email to: <a href="mailto:corporatemeetings@office365itpros.com">Corporate Meetings.</a></li></ol><p><strong>Room  
101</strong> can hold up to <strong>12</strong> people. Please do not exceed this capacity.</p><p>If  
you need <strong>catering</strong>, please contact Jennifer at (650) 561-4136.</p><p>Thanks for  
meeting with us!</p><p>'`  
-AllowConflicts:$False -ForwardRequestToDelegates:$True  
-AllBookingInPolicy:$False -AllRequestInPolicy:$True  
-AllowRecurringMeetings:$False -BookingWindowInDays 30  
-MaximumDurationInMinutes 30 -ScheduleOnlyDuringWorkHours:$True  
-AddOrganizerToSubject:$False -DeleteSubject:$False
```

In this example, the *AutomateProcessing* parameter for the *Set-CalendarProcessing* cmdlet is set to the default value (*AutoAccept*). This forces the resource booking assistant to accept all meeting requests that comply with policy. For many rooms, this is the right way to proceed because it means that users receive immediate confirmation about room booking requests. If manual control over a room is necessary, set the value to either:

- ***None***: Exchange Online performs no automatic processing for meeting requests for the room. A delegate must process all meeting requests.
- ***AutoUpdate***: The calendar attendant tentatively accepts meeting requests. A delegate must confirm the request before it is final.

If the automatic processing setting for a room mailbox is *AutoAccept*, the *AddOrganizerToSubject* setting is available. If *AddOrganizerToSubject* is true (the default for new room mailboxes), Exchange Online replaces the meeting subject in the calendar of the room mailbox with the organizer's name. The intention of this setting is to preserve the privacy of meeting subjects in room mailboxes shared by many people. It also helps to sort meetings in the room calendar by the different organizers.

You can force Exchange to keep the original meeting subject for events in a room mailbox's calendar by running the *Set-CalendarProcessing* cmdlet to update the *AddOrganizerToSubject* and the *DeleteSubject* settings to false. See [this article](#) for more information.

The other parameters for *Set-CalendarProcessing* do the following:

- ***AllowConflicts***: Set to *\$False* to stop multiple meetings being scheduled at the same time.
- ***AllBookingInPolicy***: Set to *\$False* to stop the acceptance of meeting requests that are in policy (for instance, they are 30 minutes or less).
- ***AllRequestInPolicy***: Set to *\$True* to allow users to submit requests to book the room. A delegate will examine each request and decide whether to accept it.
- ***AllowRecurringMeetings***: Set to *\$False* to prevent users creating recurring meetings for the room.
- ***BookingWindowInDays***: Set to 30 (days) to limit how far in advance a room can be booked.

- **ForwardRequestToDelegates:** Set to `$True` to have the resource booking assistant forward inbound meeting requests to the room delegates for them to decide whether to accept the requests.
- **MaximumDurationInMinutes:** Set to 30 to limit meeting requests to 30 minutes. Requests for longer meetings are rejected.
- **ScheduleOnlyDuringWorkingHours:** Set to `$True` to prevent users from attempting to schedule meetings outside the working hours set for the room mailbox.

When using the `ScheduleOnlyDuringWorkingHours` parameter, it's important to configure the working day for the room mailbox with the `Set-MailboxCalendarConfiguration` cmdlet. This example shows how to configure the working day to be from 9:30am in the morning to 6pm in the evening:

```
Set-MailboxCalendarConfiguration -Identity "Room 101" -WorkingHoursTimeZone "Central Standard Time"  
-WorkingHoursStartTime 09:30:00 -WorkingHoursEndTime 18:00:00
```

Finally, it's a good idea to add a mail tip to any room mailbox subject to review before the acceptance of meetings.

```
Set-Mailbox -Identity "Room 101" -MailTip "Meetings requested for Room 101 are subject to review  
before approval"
```

How Outlook Processes Inbound Meeting Updates

The `VisibleMeetingUpdateProperties` setting in the tenant Exchange Online organization configuration controls how the Outlook (for Windows) client processes meeting updates. In the past, each time a meeting organizer updated any property of a meeting, like its title, location, date, or body (description), email notifications go to all meeting attendees. The attendees then had to process the update. Outlook can auto-process meeting updates, meaning that Outlook automatically applies updates to the event in attendee calendars without the need for any human interaction. Notifications are still emailed but are moved to the Deleted Items folder after Outlook processes the updates.

In general, updating meeting updates without requiring user intervention is welcome. However, some of the updates might contain information that users want to see. For instance, the default configuration is to only show update notifications to users if the meeting location changes or a change is made to any detail of the meeting within 15 minutes of its start. Outlook processes (and hides) any other change, such as an update to the meeting subject or the body of the meeting notice, which is where details such as agendas are often published. Outlook always shows a meeting notification if any of the following conditions are true:

- A change is made to the meeting date, time, or recurrence pattern.
- The notification is for a delegated shared calendar.
- The recipient is @mentioned in the meeting body.
- The recipient has not yet responded to the meeting (in effect, the notification acts as a prompt for them to respond).

You can change how Outlook behaves by running the `Set-OrganizationConfig` cmdlet to update the settings in `VisibleMeetingUpdateProperties`. For example, this command forces Outlook to display updates for any change to the meeting location or body 120 minutes or less before it starts, or a change at any time to the online (Teams or Skype for Business Online) details or meeting subject.

```
Set-OrganizationConfig -VisibleMeetingUpdateProperties Location:120, Body:120, OnlineMeetingLinks,  
Subject
```

The setting applies to all mailboxes in the tenant. You can't change how Outlook works on a per-mailbox basis.

Generating Automatic Calendar Events from Email

When the transport service processes inbound email, a background Exchange agent scans messages to figure out if the messages relate to events generated by airlines, hotels, and other sources like booking agencies. If Exchange Online detects an event, user settings control how it processes the event. The settings to control automatic event detection are in the **Calendar** section of OWA Options. Go to **Events from email** to select how Exchange should process each of the event types. You can choose to:

- **Don't show event summaries in email or on my calendar:** This choice stops processing these events.
- **Only show event summaries in an email:** Exchange delivers event information in an email but won't create a calendar event.
- **Show event summaries in email and on my calendar:** Exchange delivers event information in email and uses that information to create a calendar event based on the information in the email, such as the time and date for a flight together with the airline booking reference, the name of the departure, and destination airports. Exchange includes details of the extracted event in the message sent to the user. If Exchange detects several events (such as flights in a single reservation), it creates a separate calendar event for each event.

Event settings are updatable with PowerShell by running the *Set-EventsFromEmailConfiguration* cmdlet. For example, to set rental car event processing to Email only while making sure that Exchange creates flight reservations in the calendar, run:

```
Set-EventsFromEmailConfiguration -Identity Kim.Akers@Office365itpros.com -FlightReservationProcessingLevel Calendar -RentalCarReservationProcessingLevel Email
```

Unlike other Exchange Online cmdlets, you must identify the target mailbox using one of the SMTP proxy addresses assigned to the mailbox. You cannot pass an alias, display name, distinguished name, or user principal name. This means that regular pipeline processing is not possible. For instance, you can't do this to have flight reservations created as calendar events:

```
Get-ExoMailbox -RecipientTypeDetails UserMailbox | Set-EventsFromEmailConfiguration -FlightReservationProcessingLevel Calendar
```

Instead, you can do this:

```
$Mbx = (Get-ExoMailbox -RecipientTypeDetails UserMailbox)
$Mbx.ForEach( { Set-EventsFromEmailConfiguration -FlightReservationProcessingLevel Calendar -Identity $_.PrimarySmtpAddress } )
```

To disable a setting for an event, set it to *Disabled*. For instance, here's how to disable event creation for all events:

```
Set-EventsFromEmailConfiguration -Identity Kim.Akers@Office365itpros.com -FlightReservationProcessingLevel Disabled -LodgingReservationProcessingLevel Disabled -ParcelDeliveryProcessingLevel Disabled -RentalCarReservationProcessingLevel Disabled
```

As you can see, you must disable each event type separately.

To check the current event processing settings for a mailbox, run the *Get-EventsFromEmailConfiguration* cmdlet:

```
Get-EventsFromEmailConfiguration -Identity Kim.Akers@Office365itpros.com | Select-Object -ExpandProperty EntityTypeProcessorLevelSettings
```

Name	Value
-----	-----
RentalCarReservation	Disabled
FlightReservation	Disabled

LodgingReservation	Disabled
ParcelDelivery	Disabled

You can reset to default values (all events set to email with no automatic calendar events created) as follows:

```
Set-EventsFromEmailConfiguration -Identity Kim.Akers@Office365itpros.com -ResetSettings
```

Before Exchange can process an email to extract event information, Microsoft must recognize the sending organization (like an airline). The full list of recognized senders [is available online](#). Microsoft updates this list on an ongoing basis, with organizations joining when they realize the value of having their email create events in user calendars.

Room Mailboxes, Workspaces, and Room Lists

Room mailboxes are a special form of resource mailbox marked for use as a meeting location. You create new room mailboxes through the Resources section of the EAC or with PowerShell. As described below, the Outlook Places service helps users find rooms for meetings, but it's still a good idea to include some location information in the display name for a room. Here's how to create a new room mailbox with PowerShell:

```
New-Mailbox -Name "SF Executive Meeting Room" -Displayname "San Francisco Executive Meeting Room" -Alias SFExecMeeting -Room
```

A workspace is a form of room mailbox to represent a place like an individual desk, a small meeting room used for calls, or other space where people work. The first step to creating a workspace is to create a room mailbox and set its type to be a workspace:

```
Set-Mailbox -Identity "Floor 1 Desk 17" -Type Workspace
```

A room list is a special form of distribution list composed exclusively of room mailboxes. No other type of recipient (including resource or equipment mailboxes) can be a member of a room list. The idea behind room lists is that they are a convenient way to segregate the different conference or meeting rooms available within an organization so that you have a room list per building or location. Outlook's Room Finder component can use the room lists to present users with options based on their location to select the most appropriate room when scheduling a meeting from Outlook or OWA.

The only way to manage room lists is with PowerShell. Here is an example of how to create a rooms list called "HQ Rooms." Note the use of the *IgnoreNamingPolicy* parameter to override the distribution list naming policy in force for the organization.

```
New-DistributionGroup -Name "HQ Rooms" -Members "Room 101", "Room 102", "Room 103" -RoomList -IgnoreNamingPolicy
```

You can use this command to discover the room lists that already exist within a tenant:

```
Get-DistributionGroup -RecipientTypeDetails RoomList
```

The *Update-DistributionGroupMember*, *Add-DistributionGroupMember*, and *Remove-DistributionGroupMember* cmdlets are available to update the membership of distribution lists. You will see an error if you try to add a recipient that is not a room mailbox to a room list.

The *Remove-DistributionGroup* cmdlet removes a room list.

```
Remove-DistributionGroup -Identity "Old HQ Rooms"
```

Usage Patterns for Room Mailboxes: Organizations often like to understand the usage patterns for room mailboxes. For instance, how many meetings use a room mailbox, who schedules these events, when's the

most popular days for meetings involving room mailboxes, and so on. [This article](#) explains how to use Graph API requests to retrieve meeting data from room mailboxes and generate a report about the events.

Automated Processing for Room Mailboxes

New room mailboxes receive a default value of *AutoAccept* for the *AutoProcessing* calendar property (before the default was *AutoUpdate*). The idea behind the change is to speed acceptance of meeting requests for room mailboxes. If this change doesn't fit with your corporate policies, make sure that you update new room mailboxes after creation. For example:

```
Set-CalendarProcessing -Identity NewRoom -AutomateProcessing AutoUpdate
```

For more information about how to control the processing of booking requests for room mailboxes, see [the online documentation](#).

The Outlook Places Service and Location Metadata for Room Mailboxes

The Outlook Places service helps users find suitable locations when scheduling meetings using the Room Finder feature in OWA and Outlook (both clients use the same component). Outlook Places uses metadata for room mailboxes together with room lists. Each room list represents a building, which the Room Finder collects into sets of rooms based on the *City* property for room mailboxes (Figure 5-2). After the user selects a building, they can choose a room or workspace to schedule. The list of rooms includes room characteristics using icons for capacity, video, audio, display, and wheelchair access (workspaces don't support room characteristics). You can create custom characteristics for a room using the *Tags* parameter for the *Set-Place* cmdlet. For example, you could use *Tags* to show that the room needs a special key to gain entrance.

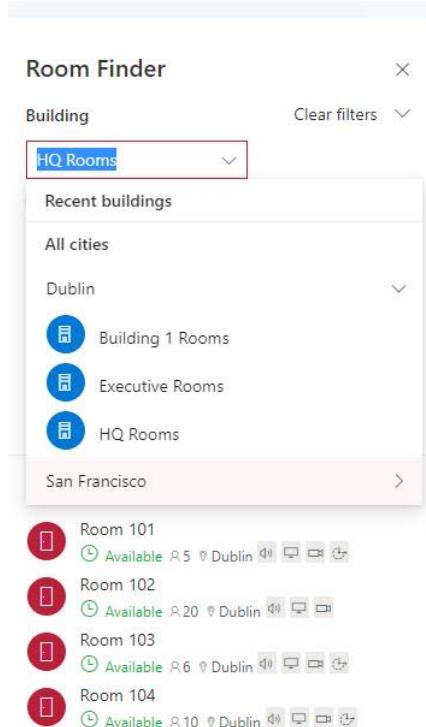


Figure 5-2: Outlook's room finder uses location metadata

The *Set-Place* cmdlet updates the location metadata for a room mailbox. For example, this snippet updates most of the properties available for a location:

```
Set-Place -Identity "SF Room 101" -CountryOrRegion "United States" -City "San Francisco" -Floor 1 -Capacity 54 -Street "10 Sutter Street" -GeoCoordinates "37.790507; -122.400274" -Building "Western
```

```
HQ" -State CA -PostalCode 94104 -Phone "+1 206 177 4151" -Label "Training" -VideoDeviceName
"Crestron Flex UC-M150-T" -Tags "Training room"
```

It can take up to a day before updated metadata is available to clients. The *Get-Place* cmdlet retrieves information about a location. For example:

```
Get-Place -Identity DublinConfRoom@Office365itpros.com | Format-List
```

If the *PlacesEnabled* setting in the OWA mailbox policy assigned to a user mailbox is \$True, OWA displays location information to users in the room card when meetings are scheduled or viewed. If geocoordinates are available for a location, the Directions link calls the Bing Maps Locations API to generate directions to the location. Exchange Online uses a specific format to store geocoordinates for a location that is different from the format used by other applications (for instance, Google Maps uses a comma instead of a semi-colon to separate the latitude and longitude data). Outlook Mobile also consumes geocoordinates (if available) to show a map to a location, but only when scheduling a new meeting.

Rename Scheduling Mailboxes

The Microsoft Booking app uses scheduling mailboxes, which appear in the GAL to allow users to schedule meetings. Some administrators don't like the default display name and title assigned to these mailboxes and suggest that it's a good idea to configure more appropriate names. This PowerShell snippet finds the scheduling mailboxes and updates them with a different display name (to keep all the mailboxes together in one place in the GAL) and job title (to display their purpose). The code also sets a mail tip to help people understand that these aren't real mailboxes.

```
[array]$SchedulingMailboxes = Get-ExoMailbox -RecipientTypeDetails SchedulingMailbox
ForEach ($Mbx in $SchedulingMailboxes) {
    $Mailtip = ("This mailbox is used by the Microsoft Booking app for {0}" -f $Mbx.DisplayName)
    $DisplayName = ("Microsoft Bookings: {0}" -f $Mbx.DisplayName)
    $Status = Set-Mailbox -Identity $Mbx.ExternalDirectoryObjectId -MailTip $Mailtip -DisplayName
$DisplayName -ErrorAction SilentlyContinue
    $Status = Set-User -Identity $Mbx.ExternalDirectoryObjectId -Title "Microsoft Bookings App" -
Confirm:$False -ErrorAction SilentlyContinue}
```

Outlook Roaming Signatures

Microsoft wants to introduce a common framework for Outlook clients that permits signatures to be shared across all clients. The effort to develop the framework started in mid-2020 and focuses on storing user signature data in a hidden folder in the non-IPM part of their mailbox. Microsoft eventually launched roaming signatures (aka cloud signatures) for Outlook for Windows in October 2022 (click-to-run build 2209 or later). Tenants that use the *Set-MailboxMessageConfiguration* cmdlet to maintain user signature information for OWA soon discovered that roaming signatures ignore this data and eliminated their ability to manage custom signatures for user mailboxes.

In October 2023, Microsoft introduced an organization-wide setting to control the use of roaming signatures. By default, the setting is False, meaning that the tenant allows roaming signatures. To postpone the introduction of roaming signatures, set the value of *PostponeRoamingSignaturesUntilLater* to True:

```
Set-OrganizationConfig -PostponeRoamingSignaturesUntilLater $True
```

Postponement means that Microsoft will eventually enable roaming signatures for all Outlook clients. Microsoft has also committed to delivering an API to allow third-party products to manage roaming signatures. That API is not yet available.

Administrator Removal of Meetings from User Calendars

Normally, administrators don't interfere with meeting arrangements. Those who create meetings (the organizers) take care of scheduling and maintaining meeting settings, whether they own the calendar or are a calendar delegate. Reasons why an administrator might intervene include:

- The organizer is unavailable for a sustained period and the need exists to rearrange the meeting.
- The organizer has left the company.
- The organizer is due to leave the company and part of the offboarding process involves cancellation of all their future meetings.

The *Remove-CalendarEvents* cmdlet exists to help in these situations. The cmdlet only works if access is still available to the user's mailbox. Exchange Online must be able to connect to the mailbox to remove events. For this reason, if you plan to cancel a user's meetings when they leave the company, the correct procedure is:

- Revoke access to their account (see the user management chapter).
- Run *Remove-CalendarEvents* to cancel all future meetings (up to 1825 days in the future) in the user's mailbox where they are the meeting organizer, and the meeting has one or more attendees (including resources like meeting rooms). Cancellations cover both normal meetings and online meetings (using Teams or another online provider). Events without attendees (appointments) are left untouched. The mailbox sends meeting cancellations to meeting participants.
- Proceed with the remainder of the account removal process. If holds exist on the mailbox, it becomes inactive. However, you can't cancel meetings from an inactive mailbox. If you forget to cancel meetings, restore the inactive mailbox, cancel the meetings, and then delete the mailbox again.

You can perform a test run beforehand to see what meetings it will remove by including the *PreviewOnly* parameter. For example, this command previews what will happen if the cmdlet removes meetings from the current date up to 365 days in the future:

```
Remove-CalendarEvents -Identity chris.bishop@office365itpros.com -CancelOrganizedMeetings -QueryStartDate (Get-Date) -QueryWindowInDays 365 -PreviewOnly -Confirm:$False
```

```
The meeting with subject "Glastonbury Meeting" and start date "09/06/2023" has been queued for cancellation.  
The meeting with subject "Project X" and start date "09/06/2023" has been queued for cancellation.  
The meeting with subject "Project Mercury" and start date "17/06/2023" has been queued for cancellation.  
The meeting with subject "Project Botha" and start date "21/06/2023" has been queued for cancellation.  
The meeting with subject "Project Botha" and start date "28/06/2023" has been queued for cancellation.
```

When ready to proceed, remove the *PreviewOnly* parameter and run the command again. Exchange Online connects to the mailbox, finds the relevant meetings, and cancels them. Cancellation occurs immediately and meeting participants receive a cancellation notice as normal.

Folder Level Permissions

You can add folder-level permissions to allow a user to access a folder in someone else's mailbox. For instance, you might want someone to check new messages that arrive when you are on vacation. In this example, we permit Marc Vigneau to access the Inbox folder for Kim Akers:

```
Add-MailboxFolderPermission -Identity "Kim Akers:\inbox" -User "Marc Vigneau" -AccessRights Reviewer
```

Automapping is the process Outlook uses to connect to mailboxes automatically that the user has full access to. This does not apply to folder-level permissions. The user who receives the permission must add the other

user's folder as a shared folder. In addition, it can take several hours for Exchange to propagate the new permission and make it effective.

Message Recall

Exchange Online delivered the cloud-based Message Recall agent in April 2023. At the time, Microsoft reported that users attempted to recall messages 800,000 times daily at a success rate of 40%. The agent intended to achieve a 90% successful recall rate, mainly because it went from being Outlook driving the recall process, to a background process in Exchange Online. The process processes message recall requests and removes messages from recipient mailboxes in the same tenant. The agent does not process messages delivered to other Exchange Online organizations or external email addresses. The recall agent also processes messages sent through third-party services, such as mail hygiene and e-mail signature services, which normally would be seen as messages that had left the tenant. Outlook for Windows, OWA and New Outlook clients can initiate message recall requests. Microsoft is working on an API to allow other clients to include the feature.

The agent uses hard deletes to remove recalled messages from recipient mailboxes. It doesn't matter if the message is not in the Inbox because the agent uses the message identifier to find the item. If required by a compliance hold, Exchange Online retains a copy of the deleted message. The deletion becomes effective after clients process the action and remove their copy of the message from local caches. Normally, processing takes just a few moments (if the message exists in thousands of mailboxes, it will obviously take longer: the current limit for message recall 50,000 mailboxes) and when it's complete, the original sender receives a summary message to tell them what happened. Message recall also works for emails sent from shared mailboxes.

By default, Microsoft enables message recall for all Exchange Online organizations. To check the current settings, navigate to **EAC > Settings > Mail Flow**, or use Get-OrganizationConfig:

```
Get-OrganizationConfig | fl *recall*
MessageRecallMaxRecallableAge : 365.00:00:00
RecallReadMessagesEnabled :
MessageRecallEnabled :
MessageRecallAlertRecipientsEnabled : False
MessageRecallAlertRecipientsReadMessagesOnlyEnabled : False
```

The default value for *MessageRecallEnabled* is \$null, which means it is enabled. To disable the feature, or change one of the other message recall related settings, run the *Set-OrganizationConfig* cmdlet:

```
Set-OrganizationConfig -MessageRecallEnabled $False
```

Recall message works against both read and unread messages. Some organizations don't like the ability to recall messages that recipients have already read. If you want to disable this feature, edit the mail flow setting for message recall in the Exchange admin center or run:

```
Set-OrganizationConfig -RecallReadMessagesEnabled $False
```

You can also set the maximum age of messages that can be recalled. The default is 365 days. The setting is a timespan in which the input format is [DDDD.HH:MM:SS], and its property can vary from 5 minutes to 10 years:

```
Set-OrganizationConfig -MessageRecallMaxRecallableAge 7.0:0:0
```

In the first implementation of the cloud-based message recall, messages were silently removed from recipient mailboxes. However, this could create confusion with recipients that read a message only to discover that the message they read was missing after it got recalled by the sender. This behavior can be controlled through

the settings *MessageRecallAlertRecipientsEnabled* for notifying recipients for recalled messages. If you want to notify recipients about recalled read messages, set both *MessageRecallAlertRecipientsReadMessagesOnlyEnabled* and *MessageRecallAlertRecipientsEnabled* to true

```
Set-OrganizationConfig -MessageRecallAlertRecipientsEnabled $True  
MessageRecallAlertRecipientsReadMessagesOnlyEnabled $True
```

These settings affect all mailboxes. It's not currently possible to restrict or enable message recall for selected mailboxes.

MailTips

A MailTip is informational text displayed by Exchange when certain conditions occur, such as adding a recipient to a message. Exchange includes a set of system MailTips, such as those generated when users address messages to moderated recipients or when a recipient's mailbox is full. You can't change the text for system-generated MailTips.

Although Exchange Online includes [protection against email reply-all storms](#), this only works for relatively large tenants. MailTips help users avoid doing something bad like creating a reply-all email storm by inadvertently sending a message to a large distribution list. Several settings in the Exchange Online organization configuration control how MailTips work. To view the settings, run:

```
Get-OrganizationConfig | Format-List mailtip*
```

MailTipsAllTipsEnabled	:	True
MailTipsExternalRecipientsTipsEnabled	:	True
MailTipsGroupMetricsEnabled	:	True
MailTipsLargeAudienceThreshold	:	10
MailTipsMailboxSourcedTipsEnabled	:	True

The settings are:

- **MailTipsAllTipsEnabled**: Set to True to instruct clients to use MailTips.
- **MailTipsExternalRecipientsTipsEnabled**: Set to True to have clients highlight messages addressed to external recipients.
- **MailTipsGroupMetricsEnabled**: Set to True to have Exchange Online count the number of members in distribution lists. Exchange uses this data to know when a message exceeds the large audience threshold. A background process checks distribution lists periodically, so don't expect the numbers used to be 100% accurate.
- **MailTipsLargeAudienceThreshold**: The default is 25. It's lower here as a reminder that there might be a better way to share information with large audiences, such as a post in a Teams channel. Of course, if you don't use Teams, you could increase the threshold right up to the maximum number of recipients an Exchange Online user can address in a message (1,000).
- **MailTipsMailboxSourcedTipsEnabled**: Set to True to have Exchange Online look at mailbox data such as auto-reply messages to generate MailTips.

Custom MailTips

Custom MailTips are text messages of up to 175 characters assigned to any valid mail-enabled recipient type including mailboxes, shared mailboxes, group mailboxes, mail contacts, distribution lists, and dynamic distribution lists. Exchange Online stores MailTips in HTML format.

For example, these commands set custom MailTips for a mailbox, a Microsoft 365 group, and the guest mail user object linked to a guest account:

```
Set-Mailbox -Identity Oisin.Johnston -MailTip "Working 9 to 12 at present. Ping me on Teams if urgent"
```

```
Set-UnifiedGroup -Identity BankingTeam -MailTip "Messages to this Group are delivered to external guest members"
Set-MailUser vasil_michev.org#EXT# -MailTip "Be Careful with Vasil"
```

You can also look for objects with custom MailTips. For instance, here's how to do it for mailboxes:

```
Get-ExoMailbox -ResultSize Unlimited -Properties MailTip | Where-Object {$_._MailTip -ne $Null} | Format-List DisplayName, MailTip

DisplayName : Oisin Johnston
MailTip     : <html>
              <body>
              Working 9 to 12 at present. Ping me on Teams if urgent
              </body>
              </html>
```

Users or the owners of distribution lists or groups cannot set MailTips unless their account holds the Exchange Online administrator role. Like many mailbox settings, it takes a few hours before clients pick up MailTip changes.

Translated MailTips

When you create a custom MailTip, it becomes the default for all languages. To create language-specific translations for a MailTip, you update the multi-valued *MailTipTranslations* property for an object. For example, this command sets up Spanish, French, and German translations for a mailbox. Clients configured in these languages display the language-specific values. If no value exists for the client language, Exchange uses the default MailTip.

```
Set-Mailbox -MailTipTranslations @{Add="ES: Buzón no en uso activo", "FR: Boîte aux lettres non utilisée", "DE: Mailbox nicht aktiv genutzt"} -Identity CServices
```

MailTips for AutoReplies

Exchange generates automatic MailTips for mailboxes that have an autoreply set to inform users of the current mailbox status. You can't control the generation of autoreply tips. Users might continue to see an autoreply MailTip even after the autoreply expires for a mailbox or is explicitly disabled. This is because Exchange Online caches autoreply information to prevent it from having to look up mailbox autoreply data every time a user adds a recipient to a message. The cached data is refreshed every hour. Exchange Online supports MailTips in the same way as on-premises Exchange.

Controlling Email Sent by Delegates

Delegate settings refer to the ability to give a user the right to access another person's mailbox. These rights include the ability to send messages on behalf of the mailbox owner or as the mailbox owner, or the *SendOnBehalfOf* and *SendAs* permissions. By default, when messages are sent by a delegate using these permissions, the outbound messages are stored in the Sent Items folder of the delegate's mailbox. This is because the *MessageCopyForSentAsEnabled* and *MessageCopyForSendOnBehalfEnabled* settings are set to \$False.

Mailbox owners often want to have copies of messages sent to them by a delegate. To force Exchange to create copies of these messages for the mailbox owner, set the properties to \$True. For example:

```
Set-Mailbox -Identity TRedmond -MessageCopyForSendOnBehalfEnabled $True -MessageCopyForSentAsEnabled $True
```

Similar control can be exerted over messages sent by delegates for a shared mailbox.

Configuring Junk Mail Settings

The `Get-MailboxJunkEmailConfiguration` and `Set-MailboxJunkEmailConfiguration` cmdlets manage the junk email configuration for a mailbox. A hidden Inbox rule (called the Outlook Junk E-mail rule) holds the configuration settings. The rule control how Outlook and OWA process messages after Exchange Online delivers them to a mailbox. At this point, mail hygiene processing has already assessed the message to decide if it is spam, contains malware, or exhibits evidence of a phishing attempt. The mailbox's junk mail settings determine if messages remain in the Inbox or move to the Junk Email folder.

As described in the Mail Flow chapter, Exchange Online Protection assesses messages as they pass through the transport system and calculates their spam confidence level. The organization's anti-spam policy then determines what happens next, and this is when the safe senders list in the mailbox's junk email configuration influences what action happens.

- If the policy action is **Move messages to Junk Email folder**, messages received from addresses in the destination mailbox's safe senders list are not moved to Junk Email and are delivered to the Inbox.
- If the action is **Quarantine**, the action depends on the malware verdict. If Exchange Online Protection considers the message to be malware or high confidence phishing, Exchange Online Protection moves the message to quarantine. The same happens if the sender address is in the tenant block list. Exchange Online Protection also quarantines messages deemed to contain spam (without malware or phishing) unless the sender is in the recipient's safe sender list. In this situation, because the recipient considers the sender to be safe, Exchange delivers the message to the Inbox.

When enabled for a mailbox, Exchange Online applies the junk email rule to all inbound messages.

Organizations have the choice to enable the junk mail configuration for mailboxes and allow users to manage their safe sender list or use the [tenant allow or block list](#) instead. From a user perspective, being able to manage their own safe sender list is a nice feature, but it can result in problematic messages being delivered to user inboxes. If a tenant decides to block users from being able to manage safe lists, they should run the `Set-MailboxJunkEmailConfiguration` cmdlet to set the Enabled state to *False*. For instance, this command disables the rule for a selected mailbox:

```
Set-MailboxJunkEmailConfiguration -Identity Lotte.Vetler -Enabled $False
```

To check which mailboxes where Outlook's junk email rule is disabled, run this code (which will be slow):

```
[array]$Mbx = Get-ExoMailbox -RecipientTypeDetails UserMailbox -ResultSize Unlimited
ForEach ($M in $Mbx) {
    If ((Get-MailboxJunkEmailConfiguration -Identity $M.ExternalDirectoryObjectId).Enabled -eq
$False) {
        Write-Host ("'{0}' mailbox has their junk mail configuration disabled" -f $M.DisplayName)
    }
}
```

It would be easy to change the code to look for mailboxes where the Outlook junk email rule is enabled and disable the rule.

New mailboxes get a default Outlook junk email rule, but only after the mailbox is opened in Outlook (in cached mode) or OWA. The most interesting of the rule settings are the trusted senders (the safe sender list) and blocked sender lists. Both are multivalued properties. The following example adds an entry to the blocked senders and domains list (because the mailbox owner does not want to receive messages from this domain), specifies that Exchange Online should always treat the user's contacts as safe senders, and replaces the set of trusted domains.

```
Set-MailboxJunkEmailConfiguration -Identity "Kim Akers"
-BlockedSendersAndDomains @{Add="Badgirls.com"} -ContactsTrusted $True
-TrustedSendersAndDomains "Microsoft.com", "Office365.com", "Outlook.com"
```

The junk email processing rule supports a maximum of 1,024 contacts, but only if the *ContactsTrusted* setting in the mailbox's junk mail rule is set to *\$True*.

Inbox and Sweep Rules

Exchange Online supports both inbox and sweep rules. However, only OWA and the Outlook Monarch client support the creation of sweep rules.

Inbox rules operate on new messages after Exchange delivers them to the inbox. The intention of inbox rules is to filter messages to make them easier for the recipient to deal with. For example, move all email received from another user to a specific folder. Inbox rules process messages immediately.

Sweep rules can operate against any mailbox folder except the Sent Items folder. The purpose of sweep rules is to clean up mailbox contents by "sweeping" unwanted items out of folders to another folder such as Deleted Items. For example, move Viva Briefing messages more than 10 days old from the Inbox and put them in Deleted Items. Exchange Online uses a background assistant to process sweep rules in mailboxes, so processing doesn't happen immediately.

Administrators can create and update both inbox and sweep rules in user mailboxes with PowerShell (using the *New-InboxRule* and *New-SweepRule* cmdlets). In most cases, this isn't necessary as rules processing is a very personal activity.

Controlling Email Forwarding

When an organization assigns an Exchange Online mailbox to a user, they probably want that person to use the mailbox for email and keep messages in the mailbox for compliance purposes. It is possible that some users prefer to use another email system and will forward messages to that system using either a forwarding address created using OWA settings or a rule. No matter what the destination is for forwarding, once messages leave the organization, they are no longer under the control of retention and other data governance policies, which is a bad thing. It's also the case that attackers often plant a mail forwarding rule to capture email from accounts that they wish to learn more about before launching a business email compromise attack. For instance, they might try to insert a mail forwarding rule or set up a forwarding address in the CFO's mailbox to discover information about the trading patterns of a company.

For historical reasons, Exchange Online supports two methods to forward email from a mailbox. The methods use different mailbox attributes, but both instruct the transport service to redirect messages to another SMTP address with the option to also deliver a copy to the original mailbox:

- A user can set the *ForwardingSmtpAddress* through OWA options or an administrator can set email forwarding for a mailbox through the Microsoft 365 admin center. Setting the *ForwardingSmtpAddress* attribute is the preferred approach. Because the mailbox owner can set up email forwarding through OWA, if an administrator creates a forward for a mailbox, its existence is known to the mailbox owner.
- An administrator can set the *ForwardingAddress* attribute through EAC through the **Manage email forwarding** option or by running the *Set-Mailbox* cmdlet. This redirect is invisible to the mailbox owner.

A significant difference between the two attributes is that *ForwardingSmtpAddress* supports any valid SMTP address, including those belonging to external domains. Microsoft recommends that you should use *ForwardingSmtpAddress* whenever possible. *ForwardingAddress* only supports addresses that are known to the tenant, including mail-enabled contacts pointing to external addresses. The properties of a mailbox can have both forwarding attributes set with different SMTP addresses. When this happens, Exchange Online will forward copies of all inbound messages to both addresses.

Here is an example of using the `Set-Mailbox` cmdlet to set a forwarding address for a mailbox. In this instance, the `DeliverToMailboxAndForward` property is set to `$True` to instruct Exchange Online to forward a copy of any inbound messages to the supplied address and keep a copy in the mailbox.

```
Set-Mailbox -Identity "Andy Ruth" -ForwardingSmtpAddress Andy.Ruth@yandex.com
-DeliverToMailboxAndForward $True
```

When you set up email forwarding for a user through the Microsoft 365 admin center, the forwarding address is written into the mailbox's `ForwardingSmtpAddress` attribute, and any value found in the `ForwardingAddress` attribute is cleared. Apart from checking that the input address is formatted properly, no attempt is made to confirm that messages can be redirected to the email address input as the forwarding destination. The administrator is notified that "*the mailbox owner will be able to view and change these forwarding settings*" (because they will be able to see the redirect address through OWA Options). If the need exists to hide forwarding, the administrator should use EAC or PowerShell to set up the redirect through the `ForwardingAddress` attribute.

Both the `Set-Mailbox` cmdlet and the Microsoft 365 admin center flag warnings if redirect addresses are detected in both attributes. `Set-Mailbox` will allow you to write redirect addresses into the two attributes, but the Microsoft 365 admin center insists on removing the redirect contained in the `ForwardingAddress` attribute before it updates the email forwarding settings.

Blocking Email Forwarding

Where organizations once allowed all users to forward messages, it's now more common to find restrictions in place. The easiest way to apply central control over email forwarding is to use the organization's [outbound spam filter policy](#) (see the Mail Flow chapter) to disable forwarding for mailboxes. If you allow some users to forward messages, you should check what email users forward and why and implement further blocks where necessary. Three approaches are available:

1. **Check for and stop users forwarding messages.** The `Get-ExoMailbox` command below lists all mailboxes with a populated forwarding address. We check both `ForwardingSmtpAddress`, which can redirect to an external address and `ForwardingAddress`. The latter only accepts internal recipients.

```
[PS] Get-ExoMailbox -RecipientTypeDetails UserMailbox -Filter {ForwardingAddress -ne $null -or
ForwardingSmtpAddress -ne $Null} -ResultSize Unlimited -Properties ForwardingSmtpAddress,
DeliverToMailboxAndForward, ForwardingAddress | Format-Table DisplayName, ForwardingSmtpAddress,
DeliverToMailboxAndForward -AutoSize
```

DisplayName	ForwardingSmtpAddress	DeliverToMailboxAndForward
Vasil Michev (Technical Guru)	smtp:vasil@contoso.com	True
Ståle Hansen	smtp:stale.hansen@fabrikam.com	True
Eoin Redmond	smtp:Eoin@contoso.com	True

After checking who's forwarding email outside the organization, we can remove the automatic forwarding with a variant of the command:

```
Get-ExoMailbox -RecipientTypeDetails UserMailbox -Filter {ForwardingSmtpAddress -ne $Null} -
ResultSize Unlimited | Set-Mailbox -ForwardingSmtpAddress $Null
```

2. **Remove the ability of users to create rules to forward messages to external domains.** When forwarding is disabled for a domain, Exchange Online detects that this is the case and delivers new inbound messages to the original mailbox. You can block forwarding for all external domains as follows:

```
Get-RemoteDomain | Set-RemoteDomain -AutoForwardEnabled $False
```

Because good business reasons might exist to justify forwarding to certain external domains, a more granular approach can be taken to disable the ability for users to forward messages to selective external domains. This approach is often used to stop users from forwarding messages to consumer email services. For instance, let's assume that you don't want users to be able to forward messages to Yahoo.com accounts. You need to define Yahoo.com as a new external domain and then block forwarding to that domain. Here's how:

```
New-RemoteDomain -DomainName "*.yahoo.com" -Name "Yahoo.com"  
Set-RemoteDomain -Identity "Yahoo.com" -AutoForwardEnabled $False
```

3. **Remove the ability of users to set forwarding through OWA options.** This approach needs you to update the default user role assignment policy because the OWA options are controlled by the policy. You can find a [complete description of the required steps](#) online.

In the past, organizations commonly used transport rules to block forwarded messages to specific domains. The implementation of the block in the outbound spam policy removes the need to use these rules and they should be retired.

Power Automate offers several templates to allow users to forward new messages moved into a folder. These flows can forward messages to external addresses. None of the standard Exchange Online management tools stop Power Automate forwarding messages. However, [a transport rule](#) can block the forwarding of messages using Power Platform (flow).

Naturally, as in the case of any action that removes a facility that some people might be using, it's a good idea to capture the business reasons why a policy exists for email forwarding and to communicate why blocks are being enforced and how the changes might affect users before anything is done.

Reporting Forwarding

If the outbound spam policy for the organization allows some users to forward messages, the Auto forwarded message report available in the Reports section of the EAC gives an insight into forwarding activity. In addition, the Microsoft 365 Defender portal includes a default alert policy called *Creation of forwarding/redirect rule* to flag alerts when users create rules to forward messages outside the tenant. To round things out, it's possible to use PowerShell to check which mailboxes are forwarding messages. The steps required are:

- Creates a collection of user and shared mailboxes.
- Checks if the mailbox has a forwarding address set and reports it if found. We don't check the *ForwardingAddress* property because [it only supports addresses for internal recipients](#), and we are more concerned about mail going outside the tenant.
- Checks if any rules exist in the mailbox. If rules exist, check if any forward messages (including forward as an attachment).
- Check the forwarding addresses to see if the recipient is known to the tenant directory (including guest accounts) and report any forwarding address found.
- Optionally, if the forwarding address is unknown (does not exist in the directory), remove the rule from the mailbox.

You can [download an example script from GitHub](#).

Even if you did not remove the offending rules, you could run the script periodically to discover whether people are attempting to forward emails outside the organization, and if so, what are the target domains.

Licensing for Mailboxes Forwarding Email

If you're in a situation where someone leaves the business and you want to keep their mailbox active and forward new messages to someone else for processing, remember that the mailbox (account) must remain

licensed to allow forwarding to happen. In these scenarios, it might be better to convert the mailbox to a shared mailbox. A shared mailbox requires a license if it is larger than 50 GB or has an archive.

Maximum Message Size

Exchange Online allows mailboxes to send and receive messages up to a maximum of 150 MB. The actual size of messages supported by a mailbox is set by the *MaxSendSize* and *MaxReceiveSize* properties, which can be changed using the *Set-Mailbox* cmdlet or by editing mailbox properties through the EAC (the values are available through the mailbox features page). For example, this command sets the send and receive size to 100 MB for the Kim Akers mailbox:

```
Set-Mailbox -Identity 'Kim Akers' -MaxSendSize 100MB -MaxReceiveSize 100MB
```

Although it is great to be able to send large messages, it is quite another matter to make sure that the recipient will be able to receive them as you probably have zero influence over the connectors and configuration of the email systems involved in the transfer of the message after it leaves Exchange Online. This is especially important in a hybrid situation as it is probable that the on-premises servers support message sizes significantly smaller than the values supported by Exchange Online. It is also important to understand that the message size used for this purpose is the size of the message after it is coded into BASE64/MIME format to allow it to be accepted by other mail systems. This process can add up to a third to the size of a message, so a 60 MB message as seen by the user might become an 80 MB message when presented to the transport system for transmission. In turn, this might end up exceeding the permitted threshold and cause some bewilderment to the user.

Enabling Third-Party Cloud Attachments

Working inside Exchange Online, it's natural to use "cloudy attachments" stored in SharePoint Online or OneDrive for Business document libraries. Your company might use other cloud-based document storage repositories like Dropbox or Google Drive, and you might want to allow users to add attachments to messages from these repositories. The *AdditionalStorageProvidersAvailable* setting in OWA mailbox policies controls access to both first-party and third-party storage providers. By default, this setting is *\$True*. If you block access to third-party storage providers, you must update OWA mailbox policies to ensure that they exert the same control over users. For example:

```
Get-OWAMailboxPolicy | Where-Object {$_._.ThirdPartyFileProvidersEnabled -eq $False} | Set-OWAMailboxPolicy -AdditionalStorageProvidersAvailable $False
```

OWA mailbox policy settings only apply to OWA clients and do not affect Outlook desktop or mobile. After making the change to the policy, wait an hour or so to allow the cached policy to be refreshed.

Mailbox Quotas

The size of the assigned storage quota is a major difference between on-premises mailboxes and their cloud counterparts. Although it is still common for on-premises mailboxes to have relatively small quotas of between 2 and 10 GB, Exchange Online assigns a basic 100 GB quota to mailboxes with enterprise E3 and E5 plans, 50 GB to E1 and education plans, and 2 GB to frontline worker plans. Competitive pressure is one reason why Microsoft offers very large mailbox quotas for Exchange Online. For instance, Google Workspace plans include between 30 GB and "as much as you need" storage. Table 5-1 lists the current quotas assigned to [different types of mailboxes](#).

	Frontline worker (F3)	Enterprise E1 (and Gov/Edu Equiv.)	E3 and E5
Primary mailbox size	2 GB	50 GB	100 GB
Archive mailbox size	N/A	50 GB	Limited to 1.5 TB

Shared mailbox size	50 GB	50 GB	50 GB
Resource mailbox size	50 GB	50 GB	50 GB
Group mailboxes	50 GB	50 GB	50 GB
Public folder mailboxes	N/A	50 GB	100 GB

Table 5-1: Exchange Online mailbox sizes

If a shared mailbox has an Exchange Online Plan 2 license, its quota increases to 100 GB, and it can have an archive. In the past, some unlicensed shared mailboxes had a 100 GB quota. These mailboxes can keep the erroneous quota if their status does not change (for example, administrators do not convert a shared mailbox to a user mailbox and back to become a shared mailbox). New shared mailboxes receive a 50 GB quota.

You do not have to assign the full quota to mailboxes and can restrict users to lower amounts. As you can see in the PowerShell example below, three properties control how Exchange applies a mailbox quota:

- The *IssueWarningQuota* property tells Exchange the point at which nagging messages should be sent to the mailbox owner to tell them that they are approaching the quota limit.
- The *ProhibitSendQuota* property marks the limit at which Exchange will no longer accept new outbound messages from the mailbox.
- The *ProhibitSendReceiveQuota* property tells Exchange when to cut off both outbound and inbound service to the mailbox.

For example, this code sets a warning limit of 23 GB, stops the user from sending messages at 25 GB, and stops the mailbox from receiving messages when the mailbox size reaches 30 GB.

```
Set-Mailbox -Identity TRedmond -ProhibitSendQuota 25GB -ProhibitSendReceiveQuota 30GB
-IssueWarningQuota 23GB
```

You can scan for user mailboxes that have a certain quota and increase their quota with a command like:

```
$Mbx = (Get-ExoMailbox -RecipientTypeDetails UserMailbox -PropertySet Quota -ResultSize Unlimited)
[$double]$QuotaCheck = 75161927680 # bytes - 70 GB in this case
Foreach ($M in $Mbx) {
    [$double]$Quota = $M.ProhibitSendQuota -replace "(.*\O|,[a-z]*\)", "" # value in bytes
    If ($Quota -lt $QuotaCheck)
        { Write-Host "Updating" $M.UserPrincipalName "quota of" $M.ProhibitSendQuota "to 75GB"
         Set-Mailbox -Identity $M.UserPrincipalName -ProhibitSendQuota 74GB -ProhibitSendReceiveQuota
         75GB -IssueWarningQuota 72GB}
}
```

Clients display available quotas in different ways. The mailbox settings section in Outlook's "backstage" (available from the File menu) tells users how much quota they have consumed and how much remains. OWA gives more comprehensive information in the Storage section of its settings. OWA also displays a warning message to users at the bottom of the folder list once they consume 90% of their mailbox quota. The message contains a link to the storage section of settings to allow the user to remove some messages from the mailbox to free quota.

Extra Space Available to Exchange Online Mailboxes

In addition to their basic quota, Exchange Online mailboxes also have a recoverable items quota of 30 GB, automatically increased to 100 GB if the mailbox is on hold. The added quota accommodates the need to keep held items in mailboxes for extended periods. If necessary, it is possible to increase the recoverable items quota past 100 GB, but only by filing a support request with Microsoft. Altogether, the total available storage available per enterprise user mailbox is between 230-300 GB made up of the primary mailbox, primary archive, and recoverable items.

Exchange Online mailboxes also store data created by Exchange, other Office 365 applications, and the Microsoft 365 substrate in hidden folders. This data is inaccessible to users. The amount of system data can

exceed user data, meaning that the overall storage occupied by a mailbox can be much larger than anyone expects. We'll dive into this aspect later.

Moving very large on-premises mailboxes to Exchange Online: The 100 GB mailbox quota assigned to enterprise Exchange Online user mailboxes is more than enough to store email for most people. Some on-premises users might have mailboxes larger than 100 GB, and if this is the case, you'll need to shrink these mailboxes before the Exchange Mailbox Replication Service (MRS) can move them to Exchange Online. Simply because of the amount of data to transfer, large mailboxes take longer to move and are somewhat more problematic than smaller mailboxes. With this in mind, it's a good idea to review the sizes of all large on-premises mailboxes before starting the migration process to make sure that they are at least 10 GB under the 100 GB quota (to allow for some growth) and if not, to reduce their size. It's also important to remove any items larger than 150 MB as items larger than this aren't supported by Exchange Online. If a mailbox is on litigation hold, a large proportion of the mailbox might be occupied by held items, in which case the Recoverable Items folder will be quite big. Users are unlikely to want to prune items out of a massive mailbox and will probably take too long to make a serious dent in the size, so the best approach is to assign a mailbox retention policy to the oversized on-premises mailboxes to have the Exchange Managed Folder Assistant remove older items in the background (for instance, by deleting any message older than 2 years or moving old messages into the archive mailbox). Once the assistant has processed the mailboxes, you should be all set to move them to the cloud.

Folder Associated Information

Administrators sometimes comment that the number of items reported in a folder by a client differs from the server-side data that they see when running a cmdlet like `Get-ExoMailboxFolderStatistics`. The difference is the hidden items (folder associated information or items, known also as FAIs) that Exchange stores in folders for different purposes such as to hold configuration settings (like the town chosen for a weather display in Outlook's calendar), RSS feeds, and retention policies. The FAIs are usually small and do not take up much space in the context of an overall mailbox, but they are very important to Exchange and its clients. The Inbox folder is the location for most FAIs. For instance, Outlook reported 5,564 items for the Inbox folder in Kim Akers's mailbox, but the `Get-ExoMailboxFolderStatistics` cmdlet reported a total of 5,740. The difference is accounted for by the hidden FAIs:

```
Get-ExoMailboxFolderStatistics -Identity Kim.Akers -FolderScope Inbox | Select-Object  
VisibleItemsInFolder, HiddenItemsInFolder, ItemsInFolder
```

VisibleItemsInFolder	HiddenItemsInFolder	ItemsInFolder
5564	176	5740

FAIs account for most of the difference between the numbers reported for the Inbox by Outlook and the cmdlet. You can check this by using the MFCMAPI utility to examine the folder's associated items table.

System Items Stored in Mailboxes

User mailboxes hold items accessible to users through clients together with system items hidden in folders invisible to clients. System folders exist to hold data for application purposes. On-premises mailboxes hold far fewer system folders than cloud mailboxes do because the Microsoft 365 substrate and applications use Exchange Online mailboxes to store a broader range of information. Most system data is in the Non-IPM part of the mailbox, which email clients do not expose. Their focus is on content stored in the IPM (interpersonal messaging) section under a root folder called Top of Information Store. Folders in the IPM part of the mailbox include well-known folders like Inbox, Sent Items, and Calendar. Some applications, like To-Do, store data in IPM folders because other applications share the data (tasks).

A good example of system data is the capture of Teams compliance records in the *TeamsMessagesData* folder in the non-IPM section of group mailboxes (for channel conversations) and user mailboxes (for personal chats). The Microsoft 365 substrate creates compliance records for Teams, Planner, and Viva Engage to support Microsoft Search, machine learning, artificial intelligence, and other centralized services.

Other examples include the folders used to hold data for the machine learning models used by Outlook features like text prediction and suggested replies and the advice highlighted by Viva Insights. Because they rely on cloud-based processing, Microsoft refers to these features as intelligent technology or connected experiences. To process mailbox data in a secure and private manner to derive the information needed by intelligent technology, Microsoft copies the data to specialized AI computers using [Privacy Preserving Machine Learning](#) (PPML). After processing completes, background agents update local mailbox folders with the results, which subsequently becomes the data used by Outlook.

To illustrate just how much invisible data exists in a mailbox, use the *Get-ExoMailboxFolderStatistics* cmdlet to reveal the folders in the *Non-IPM* part.

```
[array]$Folders = Get-ExoMailboxFolderStatistics -Identity Tony.Redmond -FolderScope NonIPMRoot
$Folders.Count
791
$Folders[0] | Select Identity, ItemsInFolderandSubFolders, FolderAndSubFolderSize
-----
Identity      ItemsInFolderAndSubfolders  FolderAndSubfolderSize
-----          -----
Tony.Redmond\                           254922 30.91 GB (33,185,680,155 bytes)
```

In 2020, my mailbox held 304 folders in the non-IPM part. In 2023, that number was 791. The amount of data increased from 20.24 GB to 30.91 GB. By comparison, here's what is in the visible folders in the same mailbox.

```
$Visible = Get-ExoMailboxFolderStatistics -Identity Tony.Redmond -FolderScope All
$Visible.Count
87
$Visible[0] | Select Identity, ItemsInFolderandSubFolders, FolderAndSubFolderSize
-----
Identity      ItemsInFolderAndSubfolders  FolderAndSubfolderSize
-----          -----
Tony.Redmond\Top of Information Store           33518 6.45 GB (6,925,984,347 bytes)
```

So, 85 visible folders against 791 and 33,518 items (6.45 GB) against the whopping 254,922 items (30.91 GB) in the invisible folders. If we look at the data in more detail and review the ten largest folders based on number of items, we gain some insight into the situation (you might find different folders in different mailboxes):

```
$Folders | Sort ItemsInFolder -Descending | Select-Object -First 10 | Format-Table -Property
@{e="Name"; width=30}, @{e="FolderSize"; Width=30}, ItemsInFolder
-----
Name          FolderSize          ItemsInFolder
-----          -----
AllItems       6.45 GB (6,925,768,909 bytes)   33517
NoArchiveTagSearchFolder853... 6.412 GB (6,884,809,716 bytes)   33378
Audits         105.6 MB (110,770,316 bytes)    19553
TeamsMessagesData 1.795 GB (1,927,791,142 bytes)   17545
Deleted Items  2.958 GB (3,175,807,316 bytes)    11397
EdgeSyncEntities 62.79 MB (65,840,745 bytes)     7439
SPOOLS          1.614 GB (1,733,381,462 bytes)    6781
SpoolsSearchFolder 1.614 GB (1,733,381,462 bytes)    6781
ExchangeODatasyncData 40.36 MB (42,323,836 bytes)   5483
BrowsingHistory 24.7 MB (25,902,128 bytes)     5482
```

Microsoft does not document how Exchange or other workloads use hidden folders, so a little guesswork is necessary. Among the folders you might find when looking through the non-IPM part of a mailbox are:

- System folders. For instance, The **Audits** folder holds mailbox audit records (which are also transmitted to the audit log). The **Calendar Logging** folder holds change details for calendar items. Folders are present to store compliance data, such as **TeamsMessagesData** (Teams compliance records). The [Planner integration with the Microsoft 365 message center](#) uses a hidden folder to hold calendar reminders for assigned tasks.
- Data stored by apps: Forms stores forms as PDFs and responses to forms as CSV files in the **c9a559d2-7aab-4f13-a6ed-e7e9c52aec87** folder under the **ApplicationDataRoot** folder. Likewise, Sway uses the **905fcf26-4eb7-48a0-9ff0-8dcc7194b5ba** subfolder to store any files created by the user in HTML format. These are examples of applications storing information in user mailboxes to expose their content to Microsoft Search.
- Search Folders used by different features. MAPI search folders don't store copies of mailbox items, so they don't occupy any storage. Instead, they store links to items found using criteria such as "All PDF attachments." The real items exist elsewhere. Even so, *Get-ExoMailboxFolderStatistics* reports the size as if copies of the items are in the folder. Examples include **GraphFilesAndWorkingSetSearchFolder**, holding attachments and files accessed by a user for the OWA Files feature; the folder starting with **OwaFV15.1AllFocused** holds items in the *Focused* view for the Focused Inbox (another folder starting with **OwaFV15.1AllOther** holds items in the *Other* view).

To discover the set of mailbox folders that consume storage quota, you can use a command like this:

```
Get-ExoMailboxFolderStatistics -Identity James.Ryan -Folderscope NonIPMRoot | Where-Object {($_.TargetQuota -like 'User') -and ($_.FolderSize -like "*GB*" -OR $_.FolderSize -like "*MB*")}| Sort-Object Name | Format-Table Name, FolderSize, ItemsInFolder
```

Because Microsoft takes care of storage provisioning, administrators don't need to worry about the consumption of Exchange mailbox storage in the same way as they do on-premises. This underscores a key point about the cloud: you don't worry about the method used to deliver a service if the service works reliably and meets your needs.

Folder Limit for Cmdlets: By default, the *Get-ExoMailboxFolderStatistics* and *Get-MailboxFolderStatistics* cmdlets both return data for maximum of 1,000 folders. Although it's uncommon to find mailboxes with more than a thousand folders, the storage of data ("digital twins") in mailboxes by the Microsoft 365 substrate on behalf of other applications has increased over time. Users aren't aware of the issue because these are system folders stored in the non-IPM part of the mailbox, but scripts can run into problems if they encounter a mailbox with more than a thousand folders. If you need to retrieve details for more than a thousand folders in a mailbox, run the *Get-MailboxFolderStatistics* cmdlet with the *ResultSize Unlimited* parameter.

User Role Assignment Policies

Exchange Online controls access to features using role-based access control (RBAC), a method of ensuring that people who need to do something have the right to do it. By default, Exchange Online has a single-user role assignment policy to control several aspects of user functionality. Elsewhere in the book, we update a user role assignment policy to control whether users can create distribution lists and add personal retention tags to their mailbox retention policy. For now, all we need to do is introduce the concept that user role assignment policies exist. Each policy divides into roles, each of which controls some aspect of functionality, such as:

- **MyContactInformation:** Enables users to update their contact phone numbers and address.
- **MyProfileInformation:** Enables users to update their name information, such as their display name.
- **MyDistributionGroups:** Controls what actions users can take with distribution lists.
- **MyDistributionGroupMembership:** This allows users to control their membership in the distribution lists they join.

Not every tenant uses all these roles. Some, like text messaging, are remnants of technology that was once more important than it is now. Descriptions of the [full set of user roles](#) are available online.

Autodiscover

Microsoft originally introduced the Autodiscover service in Exchange 2007 to automatically populate Outlook profiles with the details of resources available to a user, such as the server and database hosting their mailbox. Since its introduction, Autodiscover has proven to be extremely valuable. The current set of published services inform clients about resources such as the location of public folders, alternate mailboxes (like shared mailboxes), the OAB, and the Exchange Web Services endpoint. Equipped with this information, clients know how to access the resources when needed. Clients that use Autodiscover (desktop Outlook, Outlook for Mac, and many Exchange ActiveSync clients) connect to Exchange Online to retrieve all the information necessary to configure settings in the user profile. The technical details about where their mailbox is located are invisible to the user. See this post for a description of [how to use Autodiscover in scripts](#).

Autodiscover and Teams: Exchange 2016 CU3 and later on-premises servers run Autodiscover V2. Teams clients need this version to connect to Exchange on-premises servers to retrieve calendar events and other information from mailboxes.

Simplifying the first connection to a mailbox makes it easier to onboard new users. All a user needs to know is their user principal name (usually the same as their SMTP email address) and password. With this information, Autodiscover can connect to Exchange Online, retrieve information about the services provided by Exchange Online, and return the information to the client as an XML-formatted manifest. You can see the contents of the manifest by using Outlook's "Test Email Auto-configuration" function. Do not include the Guessmart and Secure Guessmart Authentication methods as they only work with IMAP4 and POP3 servers. The Autodiscover process is a little more complicated in hybrid deployments because the first connection goes to the on-premises organization and then to Exchange Online.

In November 2022, Microsoft began to remove support for connections made using basic authentication for Autodiscover. This is a consequence of the removal of basic authentication for most email connection protocols.

Recovering Deleted Mailboxes

When you remove an account, a clock starts ticking and the Entra ID object for the user account stays in a soft-deleted state for a 30-day retention period. During this time, you can recover and restore the data belonging to the user, including their mailbox. Once the retention period elapses, Entra ID removes all traces of the user account, and the account becomes irretrievable. You can use the **Deleted users** view in the Microsoft 365 admin center to see the set of deleted users that are still within the 30-day retention period. The list includes any deleted guest accounts. You can select a user from this list and restore their account, including their mailbox, at any time until their retention period expires.

To restore a user account, select their entry to view the details of the account. If you're sure that you want to restore it, click **Restore user** and give details of what the password should be for the restored account (you can assign one, force the user to create one when they first sign in, or have a password auto-generated). Entra ID restores the user account to its pre-deletion state, including the mailbox (if they had one) as well as memberships of any distribution lists, Groups, and Teams to which the account belonged. It takes between 15 minutes and 30 minutes before the system restores an account fully. After the restore operation finishes, the user should be able to log on and use their account as before. See the PowerShell book for information about how to restore deleted accounts with PowerShell.

Restored accounts might not receive licenses automatically and you should check the assigned licenses (and apps enabled or disabled for plans like Office 365 E3) after restoring an account to make sure that the account recovers full functionality. If you don't assign a license to a restored account, Exchange Online removes its mailbox in 30 days. The exception is if the mailbox is subject to a hold, and you delete the user account which owns the mailbox. In this case, it becomes an inactive mailbox.

Mailbox Recovery Troubleshooter: Situations arise when administrators have discovered that they have removed the wrong mailbox and do not know what they should do to execute a recovery. To reduce issues in this area, Microsoft created a [mailbox recovery troubleshooter](#), a walk-through guide as to what an administrator needs to do to recover a mailbox. It is not a wizard and processing a successful recovery needs some skill in PowerShell and knowledge of the various PowerShell modules that are involved, but at least it's a step forward towards automated recovery.

Removing an Unlicensed Mailbox

The usual methods to remove a mailbox from a Microsoft 365 account are to delete the account or take the Exchange Online license away from the account. If you remove the Exchange license from an account, Exchange notices the absence of the license and deprovisions the mailbox, putting the mailbox into a disconnected state. The mailbox remains in this state for 30 days. During this time, you can reconnect the mailbox by restoring the account or adding the license back to the account. After the 30 days elapses, the Managed Folder Assistant permanently deletes the mailbox from its database.

When Exchange Online acknowledges the license removal, it sets the mailbox's *SkuAssigned* property to *\$False*. At this point, you can accelerate the removal process by running the *Disable-Mailbox* cmdlet (the cmdlet won't work for licensed mailboxes). Data in unlicensed mailboxes is not discoverable.

It's usually best to leave disconnected mailboxes for the Managed Folder Assistant to deal with and only use *Disable-Mailbox* when an urgent need exists to purge a mailbox immediately. Given the obvious compliance issues that might arise when purging a mailbox, especially when retention holds are in place, it's wise to document the reasons why this action is necessary and seek management approval before proceeding.

Inactive Mailboxes

The usual course is to remove user accounts once the account holder does not work for the company any longer. However, you might need to keep the information in their mailbox for an extended period for legal or regulatory purposes or because it is a source needed for an eDiscovery case. In the on-premises world, you could disable the user's Active Directory account and leave their mailbox online.

You can also disable the accounts of ex-employees in the cloud. However, if someone leaves the organization and you don't delete their account, you must pay a monthly license fee for that account for as long as the account remains online. Given the number of people who might potentially leave an organization over the course of a year, it's clear that paying licenses for unused accounts could rapidly mount up to a considerable amount.

To address the problem, Microsoft created the concept of inactive mailboxes. Inactive mailboxes are soft-deleted mailboxes that belong to Entra ID user accounts that no longer exist. Inactive mailbox do not need licenses. Their status depends on a hold being applied to some or all of the mailbox contents while the owning account existed. An account must have the Exchange Online Plan 2 service plan or an Exchange Online Archiving license before it supports the application of holds to its mailbox.

Assessing the Inactive State of a Mailbox

When Exchange Online assesses soft-deleted mailboxes, the deciding factor to putting a mailbox into the inactive state is whether any retention policies or holds apply for its owner's account. The [different kinds of holds that force Exchange Online to make a mailbox inactive](#) include:

- Org-wide Microsoft 365 retention policies. The retention policy covers all items in the mailbox.
- Microsoft 365 retention policies with static or adaptive scopes that cover the mailbox. The retention policy covers all items in the mailbox.
- Retention labels applied to items in the mailbox. Retention labels hold items until the retention period defined for the label expires. Users can assign retention labels to mailbox items manually or the assignment can happen using auto-label policies.
- Exchange Online litigation holds. This hold covers everything in the mailbox.
- Holds applied by eDiscovery cases (standard and premium).
- Older in-place holds applied by Exchange Online eDiscovery. Because Exchange Online eDiscovery no longer creates in-place holds, these holds are less common.

The easiest way to ensure that a mailbox will become inactive following the removal of its user account is to put it on litigation hold:

```
Set-Mailbox -Identity "Jill Smith" -LitigationHoldEnabled $True
```

For more information about retention policies, see the chapters covering eDiscovery and Compliance.

Lifecycle of an Inactive Mailbox

When an administrator deletes a user account linked to a mailbox, the following happens:

- A 30-day deleted retention period for the soft-deleted user account commences. The account is in the Entra ID recycle bin and administrators can restore it using PowerShell or the options in the Deleted Users section of the Microsoft 365 admin center or the Entra admin center.
- Exchange Online notes the deletion of the user account (it might take a few minutes before the mailbox state changes). If any holds exist on the mailbox owned by the account, Exchange Online marks the mailbox as inactive and stamps its *WhenSoftDeleted* property with the current date. Its inactive status removes the mailbox from address lists, so it is invisible to users. To allow recovery, the mailbox's *ExternalDirectoryObjectId* property continues to point to the user account.
- After 30 days, the Entra ID deleted account retention period finishes and Entra ID removes the user account permanently. Administrators can accelerate this process by removing the account with:
 - The *Delete permanently* option in the Entra admin center.
 - PowerShell.
 - A Graph API request.

- Exchange Online notes the account's permanent deletion and removes its object identifier from the mailbox.
- If no retention policies or holds apply to the mailbox, Exchange Online treats it as a normal soft-deleted mailbox and uses the deleted mailbox retention period (30 days) to decide for how long to keep the mailbox. When the 30-day period is over, the Managed Folder Assistant permanently removes the mailbox, and it becomes irrecoverable.
 - Inactive mailboxes remain in place until [administrators remove all holds from the mailbox](#). This includes removing the mailbox from the scope of retention policies. Even after removing holds and retention policies, the mailbox might still contain items and folders with retention labels that prevent it leaving the inactive state. The only way to find these items is to recover the inactive mailbox and remove the labels.

- After the clearance of all blocking retention and holds on the mailbox, Exchange Online moves the mailbox out of the inactive state. The mailbox is now in a normal soft-deleted state. Exchange writes the current date into the mailbox's *InactiveMailboxRetireTime* property.
- Soft-deleted mailboxes continue to exist online until they reach their retirement date. Until September 2022, Exchange Online keeps ex-inactive mailboxes for an additional 183 days to allow administrators time to recover data (if necessary) from the mailboxes. During this period, the mailbox content remains available to eDiscovery searches, so it's possible to run a search to find and export the mailbox content. From September 2022, the additional recovery period is 30 days.
- When the Managed Folder Assistant evaluates soft-deleted mailboxes, it calculates when to remove the mailbox by adding the deleted items retention period to the mailbox's *InactiveMailboxRetireTime*. If the calculated date is in the past, the Managed Folder Assistant removes the mailbox permanently.

The approach described above exists to ensure that Exchange Online preserves mailbox data required to meet compliance requirements and avoids any chance of inadvertent data loss. Inactive mailboxes can remain online and available for as long as you want. There is no need to clean up inactive mailboxes or take steps to remove them from the tenant. Microsoft recommends that you leave inactive mailboxes in place and let Exchange Online manage the complex interaction between retention policies, labels, and holds.

You can't sign into an inactive mailbox. If you want to access its contents, you must restore or recover the mailbox. You can also export the data from an inactive mailbox by running a content search and exporting the search results to a PST.

Remember that the personal data belonging to an account usually spans much more than a mailbox. Extra steps are necessary to secure all the information belonging to an account. We'll discuss this point soon.

Inactive Mailboxes and SMTP Addresses: It's possible to have an inactive mailbox with the same SMTP address as an active mailbox. This works because the inactive mailbox is invisible for routing purposes, so the transport service only ever delivers emails sent to the address to the active mailbox. However, it's a horrible idea to allow this situation to occur because it's bound to cause confusion. One way around the problem is to remove all SMTP addresses from a mailbox and to assign it a new SMTP address before deleting its account. Ideally, the new SMTP address should be something that will never be used in production, like *Inactive.Andy.Ruth@Office365itpros.com*. This must be done before the mailbox becomes inactive because once it is inactive, you can't update most of its properties.

Hybrid Inactive Mailboxes

Some problems exist in hybrid configurations where:

- The user account is on-premises.
- Their primary mailbox is on-premises or in the cloud.
- The mailbox is archive-enabled, and the archive is in the cloud.

In this scenario, you cannot make the mailbox inactive by deleting the user account. Microsoft has acknowledged the problem, but no solution is currently available. Two workarounds exist:

Convert the mailbox into a shared mailbox. This approach allows the retention of the archive. The shared mailbox must have at least an Exchange Online Plan 1 license. To make the shared mailbox more like an inactive mailbox, hide it from Exchange address lists and replace the email addresses for the mailbox with something that people are unlikely to guess.

Transfer all the content from the archive back into the primary mailbox. This can be done using Exchange Web Services ([here's a script](#) to show how), but only if the resulting size of the primary mailbox remains under 100 GB. When the transfer is complete, disable the archive and wait for Exchange to process the command (allow an hour or so), and then delete the user account.

Taking everything into consideration, the best solution is to convert the mailbox into a shared mailbox.

Finding Inactive Mailboxes

The `Get-ExoMailbox` cmdlet can list any inactive mailboxes that exist in a tenant. This command retrieves the list of inactive mailboxes. The `WhenSoftDeleted` property tells us how long Exchange has kept the mailbox. Remember, this date commences upon the original deletion. The fact that some inactive mailboxes are present well after 30 days since their deletion tells us that holds remain on these mailboxes.

<code>Get-Mailbox -InactiveMailboxOnly Sort WhenSoftDeleted -Descending Format-Table DisplayName, WhenSoftDeleted</code>	
DisplayName	WhenSoftDeleted
Jack Smith	17/06/2021 15:37:53
Sanjay Patel	26/11/2020 14:10:56
Nancy Anderson	03/10/2021 13:14:05
Boris Johnstone	29/05/2022 09:23:00

If you check for soft-deleted mailboxes, you'll find that inactive mailboxes are in the returned set. This is because inactive mailboxes are technically in a soft-deleted state. The difference between the two sets is that Exchange Online permanently removes soft-deleted mailboxes not under the control of a hold 30 days after they enter the soft-deleted state while inactive mailboxes remain untouched until the removal of the last hold. This command generates a list of soft-deleted mailboxes:

<code>Get-Mailbox -SoftDeletedMailbox Format-Table DisplayName, WhenSoftDeleted, InactiveMailboxRetireTime</code>	
DisplayName	WhenSoftDeleted

Although inactive mailboxes aren't in day-to-day use, they need some management. Most of the time, these tasks amount to responding to an occasional need to recover or restore an inactive mailbox. But it's also a good idea to keep an eye on the set of inactive mailboxes and know why they are in that state. Inactive mailboxes are not visible within EAC (an [inactive mailboxes page](#) in the Data lifecycle management section of the Microsoft Purview Compliance portal lists inactive mailboxes), and it is easy to miss the fact that holds are in place for some deleted (and now inactive) mailboxes. For this reason, it is sensible to update the account properties of inactive mailboxes so that they become more obvious to administrators. For instance, you could update the display name for inactive mailboxes to mark their status. Hopefully, the visual reminder is enough to stop administrators from making embarrassing mistakes.

Removing the Entra ID User Object to Make a Mailbox Inactive

Normally you must wait 30 days for a soft-deleted mailbox to move into the inactive state. During this time, the user account that owns the mailbox remains in the Entra ID recycle bin to allow administrators to recover the account and reconnect the mailbox. You can discover which inactive mailboxes are in this state by running this command to find inactive mailboxes that still have a link to a user account:

<code>Get-ExoMailbox -InactiveMailboxOnly Where-Object {![\$string]::IsNullOrEmpty(\$_.ExternalDirectoryObjectId)} Format-Table DisplayName, ExternalDirectoryObjectId</code>	
DisplayName	ExternalDirectoryObjectId
Imran Khan	b8eef43d-6854-4d77-9e03-745cf2e11e11

If necessary, you can remove the user account by first deleting the account and then removing the deleted object. For example:

<code>\$UserId = (Get-MgUser -ObjectId David.Jacobs@Office365itpros.com).Id Remove-MgUser -UserId \$UserId</code>	
UserId	David.Jacobs@Office365itpros.com

```
$Uri = "https://graph.microsoft.com/beta/directory/deleteditems/" + $UserId
Invoke-MgGraphRequest -Method Delete -Uri $Uri
```

Alternatively, you can remove a soft-deleted account through the Users section of the Entra admin center. Select the Deleted Users view, then select the account you want to remove, and then click the **Delete permanently** button.

Usually, it's best to let nature take its course and let user accounts move through the 30-day account retention process until Entra ID purges the accounts and their mailboxes become inactive, but you never know when you might want to accelerate the process.

Restore or Recover Inactive Mailboxes

In addition to being able to export the contents of inactive mailboxes through eDiscovery searches, you can also [retrieve information by restoring or recovering an inactive mailbox](#). When you restore an inactive mailbox, Exchange Online merges the contents of the mailbox into another mailbox. This might be done when a user needs to work with the information contained in a mailbox that belonged to an ex-employee. Restoring data from an inactive mailbox leaves the inactive mailbox intact and still available for eDiscovery. Recovering an inactive mailbox means that you bring the inactive mailbox back online and link it to a new user account.

Note that you cannot restore or recover an inactive mailbox if that mailbox has an expandable archive. In these circumstances, use a content search to find the information stored in the inactive mailbox, export the data to a PST, and import the PST contents into an active mailbox.

Restoring an Inactive Mailbox

The first step is to run the *Get-Mailbox* cmdlet to return a list of inactive mailboxes and identify which mailbox to restore. Several of the inactive mailboxes might share the same or a similar display name or other attributes, so we need a unique value for the mailbox to pass to Exchange Online to restore the mailbox. The Distinguished Name is best for this purpose, so we'll use that.

```
$InactiveDN = (Get-Mailbox -InactiveMailboxOnly -Identity "Jill Smith").DistinguishedName
```

We can now set up the restore with the *New-MailboxRestoreRequest* cmdlet to ask Exchange Online to fetch the data from the inactive mailbox and move it into a target mailbox. Remember, a restore operation leaves the inactive mailbox intact, so this is in effect a copy operation. The *AllowLegacyDNMismatch* switch allows the *New-MailboxRestoreRequest* cmdlet to process the restore request even though the distinguished names (DN) of the inactive and target mailboxes do not match. Normally, to safeguard against the misdirection of items to a mailbox that they don't belong to, *New-MailboxRestoreRequest* would refuse to copy items into a target mailbox if a DN mismatch existed. We proceed even though we know a mismatch exists, so we override the natural caution of the cmdlet by telling it that it's OK to go ahead and copy the items:

```
New-MailboxRestoreRequest -SourceMailbox $InactiveDN -TargetMailbox Abrus@Office365ITPros.com
-TargetRootFolder "Jill Smith Old Mailbox" -AllowLegacyDNMismatch
```

Name	TargetMailbox	Status
-----	-----	-----
MailboxRestore	Abrus	Queued

The restore operation continues in the background. You can check it by running the *Get-MailboxRestoreRequest* cmdlet. When the status is "Completed," all the data from the inactive mailbox should be in the target mailbox. The target root folder specified in the restore request ("Jill Smith Old Mailbox") is in the target mailbox with all the folders and items that belonged to the inactive mailbox underneath that root.

If the inactive mailbox owns an archive, you can restore items out of the archive and direct them to either the archive of a target mailbox or to the target mailbox itself. *New-MailboxRestoreRequest* supports the

The *SourceIsArchive* switch to control whether to copy items from the primary (the default) or archive mailbox and the *TargetIsArchive* switch to control whether to restore items to the primary mailbox of the target or into its archive. Restoring items to an archive mailbox has the value of creating a clear separation between the restored items and the owner's items in the target mailbox.

Recover an Inactive Mailbox

Recovering an inactive mailbox brings the mailbox back online and connects it to a new user account. This is done by running the *New-Mailbox* cmdlet to create a new mailbox from the inactive mailbox, which is identified through its distinguished name. In this example, we take the inactive mailbox of Jill Smith and use it to create a new mailbox under the control of Joe Healy, a new account. After *New-Mailbox* completes, the old inactive mailbox is gone, and its content is in the Joe Healy mailbox. To complete the process and make the mailbox fully operational, you must assign a license to the new mailbox.

```
# Get the DN for an inactive mailbox and use it to recover.  
$InactiveDN = (Get-Mailbox -InactiveMailboxOnly -Identity "Jill Smith").DistinguishedName  
New-Mailbox -InactiveMailbox $InactiveDN -Name "Joe Healy" -FirstName Joe  
-LastName Healy -DisplayName "Joe Healy" -MicrosoftOnlineServicesID "Joe.Healy@Office365ITPros.com"  
-Password (ConvertTo-SecureString -String "Testing123!" -AsPlainText -Force)  
-ResetPasswordOnNextLogon $True
```

You cannot use the recover method for an inactive mailbox while its user account still exists in Entra ID (for 30 days following the removal of the account). During this period, you can use the standard Recover Deleted Users option to restore the account and reactivate the mailbox, but you can't recover the data to a new mailbox. To test whether the user object still exists for an inactive mailbox, run *Get-Mailbox* as shown below. In this case, Exchange returns a GUID, so you know that the object still exists.

```
Get-Mailbox -InactiveMailboxOnly -Identity 'Jill Smith' | Select ExternalDirectoryObjectID  
  
ExternalDirectoryObjectId  
-----  
636578d1-89fd-42e6-8b1d-237c96635a95
```

If you recover an inactive mailbox, any holds that existed on the mailbox on its original deletion are not active. Instead, Exchange enables single item recovery for the mailbox and applies a special delay hold for 30 days to be sure that the Managed Folder Assist removes nothing from the mailbox during that period.

Removing Org-Wide Holds from Inactive Mailboxes

When a mailbox is inactive, a mixture of org-wide and specific holds might apply to it. The presence of any hold is enough to retain an inactive mailbox. As the tenant creates new org-wide holds, those holds apply to both active and inactive mailboxes (if you use an adaptive scope, it can be set to apply to mailboxes in a specific state, such as inactive). The net effect is that the number of org-wide holds that apply to inactive mailboxes can grow over time, which might then mean that some inactive mailboxes exist for longer than they should because the tenant applied extra org-wide holds after the mailboxes became inactive. This goes against the principle that organizations should be able to control the retention of information.

To solve the problem, the *Set-Mailbox* cmdlet supports the *ExcludeFromOrgHolds* and *ExcludeFromAllOrgHolds* parameters.

- **ExcludeFromOrgHolds:** Takes one or more GUIDs pointing to org-wide holds as input and excludes these holds from the evaluation of whether to keep an active mailbox.
- **ExcludeFromAllOrgHolds:** Excludes all org-wide holds from the evaluation of whether to keep an inactive mailbox.

When you exclude org-wide holds, Exchange will only keep an inactive mailbox if some other hold or retention policy is in place to keep the mailbox. If none exists, Exchange removes the mailbox.

For example, let's assume that you have many inactive mailboxes and want to clean up the set. To remove org-wide holds from the evaluation used by the Managed Folder Assistant to decide if an inactive mailbox is still subject to a hold, we retrieve the identifiers for the holds by running the *Get-OrganizationConfig* cmdlet:

```
Get-OrganizationConfig | Select -ExpandProperty InPlaceHolds
mbx9696959111f74ecda8a40aef97edd2c2:1
grp703105e3b8804a1093bb5cb777638ea8:1
mbx19200b9af08442529be070dae2fd54d3:1
grpfa1654abdba4712a43c354e28a4d56c:1
mbx703105e3b8804a1093bb5cb777638ea8:1
mbxc1e2d6f1785d4bf8a7746a26e58e5f66:1
```

Holds applying to user mailboxes have an "mbx" prefix. We can pass the identifiers in the *ExcludeFromOrgHolds* parameter as a comma-separated list. The example below passes the identifiers for two org-wide holds. The values used for the hold identifiers are in the same format as those reported by *Get-OrganizationConfig*. Notice that the script passes the distinguished name of each inactive mailbox to ensure a unique identity. After processing all mailboxes, we count the number of inactive mailboxes now known to Exchange to discover if removing any holds causes Exchange to age out some inactive mailboxes because no holds now apply to them. When this happens, Exchange removes those mailboxes and the count of inactive mailboxes reduces. Here's the code:

```
[array]$InactiveMbx = (Get-Mailbox -InactiveMailboxOnly -ResultSize Unlimited)
ForEach ($Mbx in $InactiveMbx) {
    Write-Host "Removing Specific Org-Wide holds from" $Mbx.DisplayName
    Set-Mailbox -Identity $Mbx.DistinguishedName -ExcludeFromOrgHolds
"mbx9696959111f74ecda8a40aef97edd2c2:1", "mbx19200b9af08442529be070dae2fd54d3:1" -Confirm:$False
-Force}
Write-Host "Checking inactive mailboxes after processing hold removals"
[array]$InactiveNow = (Get-Mailbox -InactiveMailboxOnly -ResultSize Unlimited)
Write-Host ("{} inactive mailboxes deleted after removing selected org-wide holds" -f
($InactiveMbx.Count - $InactiveNow.Count))
```

In the example below, we exclude all org-wide holds from inactive mailboxes, so there's no need to pass any hold identifiers. Because you're now removing all org-wide holds from the evaluation of inactive mailboxes, it's even more important to make sure that you are happy for Exchange to remove all the inactive mailboxes not covered by a specific hold.

```
[array]$InactiveMbx = (Get-Mailbox -InactiveMailboxOnly -ResultSize Unlimited)
ForEach ($Mbx in $InactiveMbx) {
    Write-Host "Removing Org-Wide holds from" $Mbx.DisplayName
    Set-Mailbox -Identity $Mbx.DistinguishedName -ExcludeFromAllOrgHolds -Confirm:$False -Force}
Write-Host "Checking inactive mailboxes after processing hold removals"
[array]$InactiveNow = (Get-Mailbox -InactiveMailboxOnly -ResultSize Unlimited)
Write-Host ("{} inactive mailboxes deleted after removing selected org-wide holds" -f
($InactiveMbx.Count - $InactiveNow.Count))
```

If you examine the properties of an inactive mailbox after running *Set-Mailbox* to exclude some or all org-wide holds, you'll see that the GUIDs for the excluded holds are present in the mailbox's *InPlaceHolds* property and that Exchange prefixes each hold with a minus sign. This indicates that the Managed Folder Assistant should exclude the hold when evaluating the mailbox. For instance:

```
Get-ExoMailbox -Identity David.Pelton | Select-Object -ExpandProperty InPlaceHolds
-mbxc1e2d6f1785d4bf8a7746a26e58e5f66
-mbx703105e3b8804a1093bb5cb777638ea8
-mbx19200b9af08442529be070dae2fd54d3
-mbx9696959111f74ecda8a40aef97edd2c2
-mbxf6a1654abdba4712a43c354e28a4d56c
UniH26c5d797-0fd3-496d-92ac-4f405700c917
```

The hold that is keeping this inactive mailbox is the last one on the list (it doesn't have a minus sign). This identifier points to hold placed by an eDiscovery case (it has a UniH, or "unified hold" prefix). This mailbox will remain inactive until an administrator removes it from the hold in the eDiscovery case.

Don't exclude org-wide holds from inactive mailboxes without understanding exactly what holds are keeping mailboxes in the inactive state as you cannot retrieve an inactive mailbox after Exchange removes it.

Removing an Inactive Mailbox

If necessary, you can remove an inactive mailbox by running the *Remove-Mailbox* cmdlet. However, before you can remove the mailbox, you must release the mailbox from the holds or retention policies that make it inactive. We've already covered some of the points, but here's a summary of the steps:

- Identify the inactive mailbox to remove.
- Exclude the mailbox from all org-wide holds.
- Remove the delay hold for mailbox content. Two commands are used. The first releases the delay hold on normal mailbox content, the second releases the hold on compliance records stored in the mailbox.
- Remove the mailbox from litigation hold.
- Remove the mailbox from the static or adaptive scopes used for non-org-wide retention policies.
- Remove the mailbox from holds applied by any eDiscovery cases.

The following PowerShell commands do most of the work. The *Get-Mailbox* command returns details of the holds that are in force for the mailbox. You need to see False reported for all the hold types and a minus prefix in front of the hold identifiers. In this instance, one retention policy is still not clear, so an administrator must check the policy settings (it could be a label publishing policy) and exclude the mailbox if necessary.

```
$Mbx = Get-Mailbox -Identity Jack.Jones -SoftDeletedMailbox
Set-Mailbox -Identity $Mbx.DistinguishedName -InactiveMailbox -ExcludeFromAllOrgHolds
Set-Mailbox -Identity $Mbx.DistinguishedName -RemoveDelayHoldApplied -InactiveMailbox
Set-Mailbox -Identity $Mbx.DistinguishedName -RemoveDelayReleaseHoldApplied -InactiveMailbox
Set-Mailbox -Identity $Mbx.DistinguishedName -LitigationHoldEnabled $False -InactiveMailbox

Get-Mailbox -SoftDeletedMailbox -Identity $Mbx.Distinguishedname | Format-List compl*, delay*, InPlaceHolds, LitigationholdEnabled

ComplianceTagHoldApplied : False
DelayHoldApplied        : False
DelayReleaseHoldApplied : False
InPlaceHolds            : {-mbxf6a1654abdba4712a43c354e28a4d56c, -
mbxc1e2d6f1785d4bf8a7746a26e58e5f66, mbx19200b9af08442529be070dae2fd54d3,
mbx85eb38087b2642619b79161788f5b81b}
LitigationHoldEnabled   : False
```

When you're happy to proceed, run the *Remove-Mailbox* cmdlet.

```
Remove-Mailbox -PermanentlyDelete -Identity $Mbx.DistinguishedName
```

The cmdlet must check all applicable holds and retention policies for the mailbox, so it might take several minutes to complete. If the cmdlet finds that it cannot proceed because of a blocking hold, it signals this information in an error message. The administrator then tracks down and releases the blocking hold and retries the removal.

Given the complexity of the processing and the time it can consume to find and remove all blocks, it's easier to leave inactive mailboxes alone and let Exchange Online manage their lifecycle.

Automatic Mailbox Maintenance

Like on-premises Exchange, the Managed Folder Assistant (MFA) runs on a workcycle basis to apply retention policies to mailboxes and clean out deleted items that have exceeded their retention period. At this point it's important to highlight the difference between Exchange MRM and the Microsoft 365 data lifecycle management solution. Both perform retention processing, and the MFA processes the retention tags (labels) managed by the two solutions. The big differences are:

- Data lifecycle management does retention processing for Exchange Online, SharePoint Online, and Teams. Exchange MRM only processes email items in Exchange Online mailboxes.
- Data lifecycle management processes Exchange Online mailboxes as units (locations). It does not distinguish between folders. Exchange MRM can assign default retention tags to default folders like the Inbox and assign personal tags to other folders.
- Data lifecycle management has no knowledge of the Exchange archive and cannot move items to the archive or delete items in the archive. Aside from folder-level retention control, this is the number one reason why Exchange MRM continues to be used within Exchange Online.

The goal for the MFA is for it to process mailboxes at least once weekly, but MFA often processes mailboxes more regularly (here's [a script to report when MFA processing occurs for mailboxes](#)). You can't affect when mailbox management happens because this happens automatically, but you can affect how MFA processes mailboxes by changing the mailbox properties that govern retention policy. To view details of a mailbox's assigned retention policy, open the *Manage mailbox policies* section of mailbox properties in EAC. The *Manage mailbox archive* section of mailbox properties shows if the mailbox has an archive and if so, how much quota the archive uses. Alternatively, you can run the `Get-ExoMailbox` cmdlet to retrieve the same information:

<code>Get-ExoMailbox -Identity Kim.Akers -PropertySets Archive -Properties DisplayName, RetentionPolicy Format-Table DisplayName, RetentionPolicy, ArchiveName</code>		
DisplayName	RetentionPolicy	ArchiveName
Kim Akers (She/Her)	Management Retention	{In-Place Archive - Kim Akers}

Exchange Online assigns the default Messaging Retention Management (MRM) retention policy to all mailboxes upon creation, including migrated on-premises mailboxes. In contrast, an on-premises administrator must make an explicit choice to assign a retention policy to a mailbox. The rationale for having a default retention policy in place for all mailboxes is that it allows MFA to exert some level of control over mailbox contents.

Figure 5-3Figure 5- shows some of the Exchange mailbox retention tags included in the Default MRM Policy, with the "Default 2 year move to archive" tag selected. This is a default tag, meaning that the Managed Folder Assistant applies its action to all items not governed by a more explicit retention tag. The action is to move items to the archive once they are 730 days (2 years old). In effect, MFA checks the retention period on items each time it processes a mailbox and will move any older than 2 years to the archive mailbox. Logically, this action can only happen if a mailbox has been archive-enabled. If not, MFA ignores the directive contained in the default archive tag. Unlike other retention policies that you might be aware of, the default MRM policy used by Exchange Online does not include a default delete tag, so if items are not archived, they continue to accumulate in the primary mailbox unless the user deletes them.

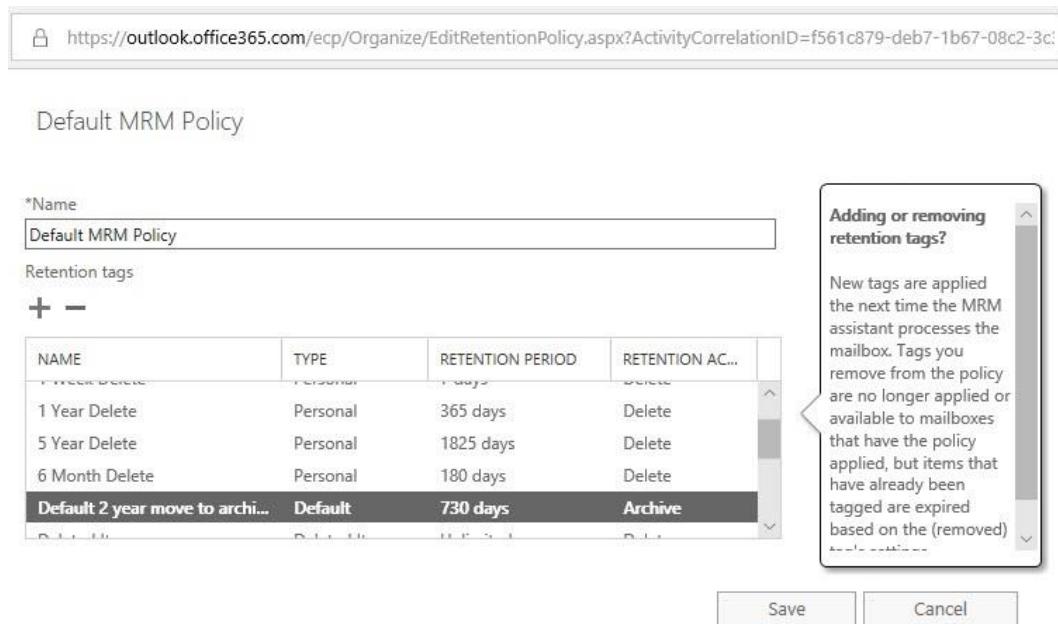


Figure 5-3: Retention tags in the Default MRM Policy for Exchange Online

Extended Email Retention for Deleted Items: Exchange Online includes a default retention tag called Deleted Items. This tag removes items from the Deleted Items folder after 30 days. It is not included in the Default MRM policy and cannot be added to this policy. Microsoft blocks the addition of the Deleted Items retention tag to the Default MRM policy to ensure that mailboxes subject to the Default MRM policy do not “lose” items from the Deleted Items folder through retention processing and is part of an [extended email retention initiative](#) launched in 2015. If you want items from the Deleted Items folder to be subject to retention processing, you must create a new retention policy that includes the Deleted Items retention tag (or a similar retention tag for the Deleted Items folder) and assign it to mailboxes.

Mailbox Data Retention

Here are some aspects of mailbox management to consider:

- As explained above, the default retention policy applied to Exchange Online mailboxes does not force the removal of items from the Deleted Items folder. You can change this behavior by updating the retention policy assigned to user mailboxes. If not, items stay in the Deleted Items folder until the user empties the folder or the items move to an archive mailbox.
- Exchange Online enables Single Item Retention (SIR) for every mailbox so that items moved into Recoverable Items stay in the database for the full retention period set on the mailbox. The default for the deleted items retention period used to be 14 days but (since 2017) it is 30 days, which is also the longest period you can set for this property. Exchange retains deleted Calendar items for up to 120 days.
- To update mailboxes that have a retention period less than 30 days with a 30 day retention period, use this command:

```
Get-ExoMailbox -RecipientTypeDetails UserMailbox -Properties RetainDeletedItemsFor | Where-Object {$_._.RetainDeletedItemsFor -lt 30} | Set-Mailbox -RetainDeletedItemsFor 30
```

If the deleted items retention period for a mailbox does not update when you run the command, check its *UseDatabaseRetentionDefaults* property. This must be *\$False* before you can update *RetainDeletedItemsFor*. Some older mailboxes have this property set to *\$True* (it's a legacy of the on-premises heritage of Exchange Online).

- Compared to the frequent access for items in primary mailboxes, archive mailboxes usually experience infrequent access. The default retention period moves items from the primary mailbox to the archive after they are two years old.

Recovering Deleted Items

It is possible users will discover that they need to recover some items after they empty the Deleted Items folder, or a retention policy removes items from the folder. Exchange Online's Single Item Recovery feature ensures that deleted items remain in Recoverable Items for the full deleted items retention period configured for the mailbox.

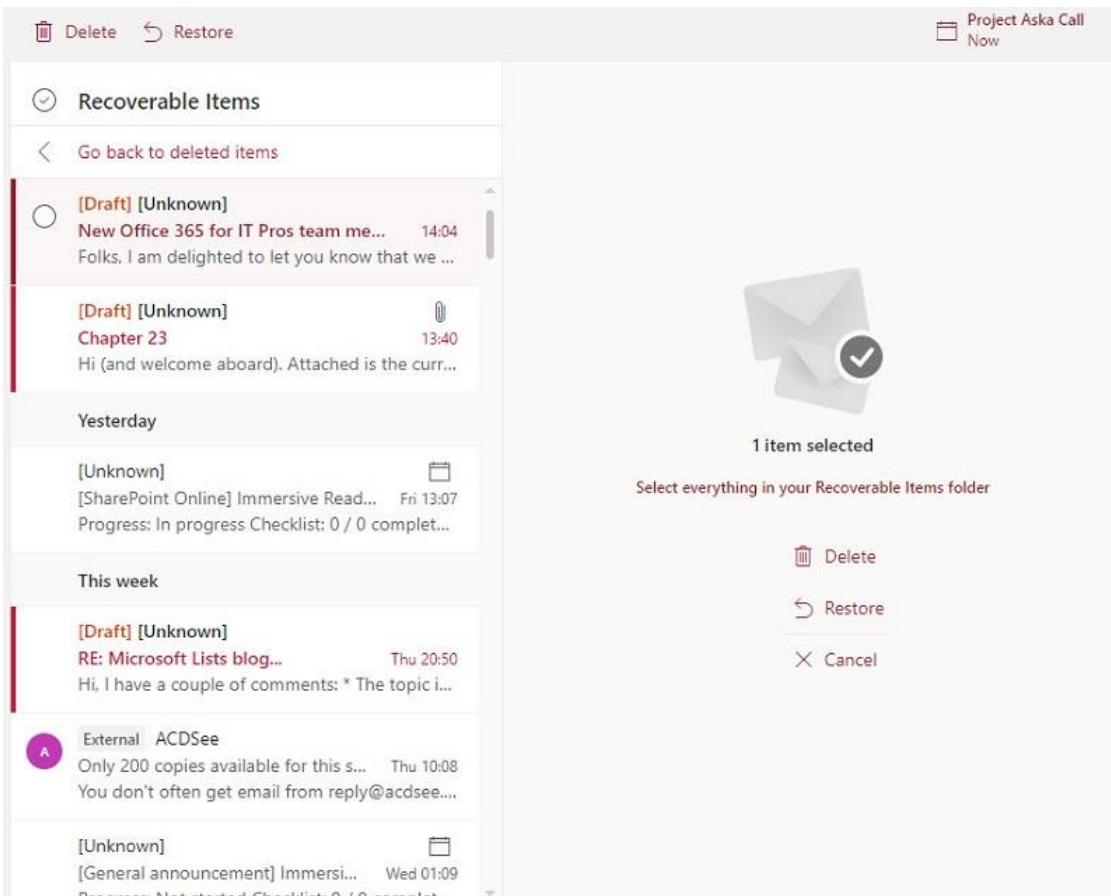


Figure 5-4: OWA lists recoverable items

Under Recoverable Items, two important sub-folders hold items:

- The **Deletions** folder stores deleted items removed from the Deleted Items folder (by emptying the complete folder or removing individual items) or items removed from other folders with the SHIFT+Delete command. While items remain in the Deletions folder, users can recover them by opening the Deleted Items folder and then using the **Recover items deleted from this folder** feature supported by Outlook or OWA (Figure 5-4).
- The **Purges** folder (which is invisible to clients like Outlook) stores items removed from Deletions. For example, if someone uses the Recover Items feature to find items and then purges them, Exchange removes the items from Deletions into Purges. The items remain there until the Single Item Retention period passes or, if the mailbox is on hold, any relevant holds lapse.

As explained below, it's also possible for administrators to recover items on behalf of users by running PowerShell cmdlets or using an option in the EAC. Once the retention period elapses, the Managed Folder

Assistant removes the items from the database the next time that it processes the mailbox. At this point, the items become irrecoverable.

Microsoft does not backup Exchange Online mailbox databases. Once Exchange removes an item from a database, it is permanently gone and no number of appeals to Microsoft Support will result in its recovery. For this reason, some administrators place some mailboxes on a permanent in-place hold or a litigation hold. The logic is as follows:

- An in-place hold keeps deleted items needed by the hold in the hidden Purges subfolder of the Recoverable Items folder until the hold lapses. The in-place hold feature is not part of every plan and a mailbox needs to have at least an E3 or Exchange Online Plan 2 license before an administrator can put the mailbox on hold.
- Problems are more severe if items are irrecoverable for mailboxes belonging to executives or other critical personnel.
- Users will not remember to protect every piece of sensitive information – the system must do this for them.
- Exchange Online makes sufficient quota available to the Recoverable Item folder (and its sub-folders) to store deleted mailbox items to satisfy the requirements of Single Item Recovery or in-place holds.
- Deleted items under hold are invisible to the user and clients. An administrator can retrieve these items by executing an eDiscovery search. Once found, exporting the search results to a PST makes the items available for return to the user (or, in the case of an investigation, to investigators).

It is difficult to estimate how much of the Recoverable Items quota a hold will consume. Even a busy mailbox will remove less than 10 GB of unwanted messages annually and a hyperactive mailbox will consume perhaps 20 GB. The default quota is therefore capable of holding five years of deleted items – and probably more for less active mailboxes. However, when you have the combination of a busy mailbox and litigation hold (or multiple in-place holds), you need to keep an eye on the growth of Recoverable Items to ensure that a mailbox does not exceed its quota ([premium monitoring](#) includes this capability). Once the quota consumed approaches 85% of its limit, it's time to talk to Microsoft Support to see if they can assign some additional mailbox quota. If not, you might need to take another approach, such as:

- Use the Mailbox Folder Assistant (MFA) to remove duplicate items from Recoverable Items. Often a surprising amount of information accumulates that can be safely removed without compromising the effectiveness of a hold. To have the MFA scan and remove duplicate items, run the *Start-ManagedFolderAssistant* cmdlet and specify the *HoldCleanUp* parameter. For example:

```
Start-ManagedFolderAssistant -Identity Kim.Akers -HoldCleanUp
```

- Use retention tags and policies to [move data from Recoverable Items to the archive mailbox](#) (and exploit auto-expanding archives).
- After securing approval to do so, [delete some items from the Recoverable Items folder](#).
- Leverage a backup solution that can backup recoverable items, in conjunction with a more time-limited retention policy.

Administrator Recovery of Deleted Items

Users sometimes need help to recover items. In the past, an administrator had to sign in to the user mailbox to perform recovery on behalf of the user. The problem with this approach is that it compromises the privacy of the mailbox. For this reason, Exchange Online includes two cmdlets to help administrators recover user data without needing to access the mailbox with a client:

- *Get-RecoverableItems* searches the Deleted Items folder and the Purges and Deletions sub-folders within the Recoverable Items structure of the target mailbox to find items. The administrator doesn't need to sign into the target mailbox, which can be a user or a shared mailbox.
- *Restore-RecoverableItems* finds and copies items from Deleted Items and the Purges and Deletions sub-folders of Recoverable Items to their original folders.

Administrators can recover deleted items from three locations, each referred to as a source folder:

- **DeletedItems**: The Deleted Items folder from the user's mailbox.
- **RecoverableItems**: The Deletions subfolder in the Recoverable Items folder of the user's mailbox.
- **PurgedItems**: The Purges subfolder in the Recoverable Items folder. Deleted items kept due to a retention policy stay here until the retention period set in the policy expires.

These names are language-independent. To search for deleted items across all locations, don't pass a *SourceFolder* parameter to *Get-RecoverableItems*.

The basic idea is that you use *Get-RecoverableItems* to construct a search to find the desired items and then use the search results as input to *Restore-RecoverableItems* after you've found the right items. Before trying to run these cmdlets, make sure that the account you use to sign into PowerShell holds the Exchange "Mailbox Import Export" RBAC role. To find out who has the role already, you can run the following command. In this example, the members of the Organization Management role group have the role as does the Administrator account.

```
Get-ManagementRoleAssignment -Role "Mailbox Import Export" | Format-Table RoleAssigneeName
```

RoleAssigneeName

Organization Management
Administrator

An example of using *Get-RecoverableItems* to search a mailbox for items is shown below. The search looks for any item of type *Ipm.Note* (messages) moved into Recoverable Items during a certain period. This happens when the user or the Managed Folder Assistant moved the item into its current folder. For instance, if a mailbox has a retention policy that moves items from Deleted Items into Recoverable Items after 120 days, the Managed Folder Assistant might have processed the items found by the search above at least four months ago. A user can bypass Deleted Items and send an item direct to Recoverable Items by using the *SHIFT+Delete* key combination. In this case, the *LastModifiedTime* property (used for date filters) is the date when the user executed *SHIFT+Delete*.

```
Get-RecoverableItems -Identity Kim.Akers -SourceFolder RecoverableItems -FilterStartTime "2/16/2018 10:00:00" -FilterEndTime "2/20/2018 17:00:00" -FilterItemType Ipm.Note
```

Capturing the items returned by a search in an array makes it easier to process them afterward.

By default, the *Get-RecoverableItems* cmdlet searches the primary mailbox. It can also search the online archive. To do this, pass the GUID for the archive in the identity parameter. For example, this command searches the Deleted Items folder in the online archive for a user:

```
$ArchiveGuid = Get-ExoMailbox -PropertySets Archive -Identity Kim.Akers | Select-Object -ExpandProperty ArchiveGuid
[array]$Items = Get-RecoverableItems -Identity $ArchiveGuid -FilterStartTime "01-Jul-2024 10:00:00" -FilterEndTime "21-Aug-2024 17:00:00" -FilterItemType Ipm.Note -SourceFolder 'DeletedItems'
```

Finding Specific Deleted Items

Although you could go through every deleted item from all locations to find something to restore, it's better when the user for whom you're restoring items gives some hints about the items they want to recover. Users

might not be sure when an item was deleted, but they should be able to tell you something about the message subject. Here's an example of using `Get-RecoverableItems` to find a message by subject.

```
$Items = (Get-RecoverableItems -Identity Kim.Akers -SourceFolder RecoverableItems -SubjectContains "disgruntled")
```

Be aware that a search based on `SubjectContains` finds any item which contains the provided string in its subject, so it's good to be as precise as possible. For instance, this search would find items with subjects like "Disgruntled at work" or "Handling disgruntled employees."

An example of the data returned for an item in Recoverable Items is shown below.

<code>LastParentPath</code>	:	Junk Email
<code>LastParentFolderID</code>	:	EBA28A7861EE1F4485DA85FE1279C88C000009CA9700
<code>OriginalFolderExists</code>	:	True
<code>Identity</code>	:	Kim.Akers
<code>MailboxIdentity</code>	:	b662313f-14fc-43a2-9a7a-d2e27f4f3478\ea58dd70-4581-4190-aef-52075e470846
<code>ItemClass</code>	:	IPM.Note
<code>Subject</code>	:	How to Catch Attacks by Disgruntled Employees
<code>EntryID</code>	:	00000000E4D17F986EC65C4EB677E1EB8F1015F20700EBA28A7861EE1F4485DA85FE1279C88C0005228415330000
<code>SourceFolder</code>	:	Recoverable Items\Deletions

Obviously, the more precise the search, the more likely you are to find the right item. For instance, it's possible that the user will be able to give an approximate period when an item was deleted, so you could use that to refine the search. For example:

```
$Items = (Get-RecoverableItems -Identity Kim.Akers -SourceFolder PurgedItems -FilterStartTime "13-Jun-2020 00:17" -FilterEndTime "13-Jun-2020 00:35")
```

A date-based search only works against a single location.

Searching for Specific Types of Deleted Items

You can specify different types of items to look for, but you cannot combine different item types in a search. Instead, if you want to find items of multiple types, don't pass a `FilterItemType` parameter and the search will return items of all supported items. If needed, you can then apply a filter using PowerShell to isolate the required items. The valid item types include:

- IPM.Note: A standard email message item.
- IPM.Appointment: A calendar meeting or appointment.
- IPM.Task: A task.
- IPM.Contact: A contact.
- IPM.File: A file stored in the mailbox. These include files created by Office 365 as the result of some processing.

Restoring Deleted Items

Once you are happy that your search finds the right items, you can proceed to recovery. The `Restore-RecoverableItems` cmdlet takes the same search that you use to find items and restores each item to its original location. You can input the same search as you used to find the item, but if multiple items are returned and you only want to restore a single item, pass the `EntryID` (a unique identifier) for the item. For example, let's assume that the search returned twenty items. The items are stored in the `$Items` variable, so we can pass a reference to the exact item we want to restore with:

```
Restore-RecoverableItems -Identity Kim.Akers -EntryID $Items[0].EntryID -SourceFolder RecoverableItems
```

The response to a successful restore will confirm the folder the item has been restored to:

RestoredFolderPath	:	Junk Email
RestoreFolderId	:	EBA28A7861EE1F4485DA85FE1279C88C000009CA9700
WasRestoredToOriginalFolder	:	True
WasRestoredSuccessfully	:	True
Identity	:	Kim.Akers
MailboxIdentity	:	b662313f-14fc-43a2-9a7a-d2e27f4f3478\ea58dd70-4581-4190-aeef-52075e470846
ItemClass	:	IPM.Note
Subject	:	How to Catch Attacks by Disgruntled Employees
EntryID	:	00000000E4D17F986EC65C4EB677E1EB8F1015F20700EBA28A7861EE1F4485DA85FE1279C88C000000001140000EBA28A7861EE1F4485DA85FE1279C88C0005228415330000
SourceFolder	:	Recoverable Items\Deletions

Of course, it's possible to restore messages in several mailboxes, possibly after an administrator makes a mistake and deletes messages in error using a content search purge. Here's an example:

```
$Mbx = (Get-ExoMailbox -RecipientTypeDetails UserMailbox -Filter {CustomAttribute1 -eq "IT"} | Select Alias, DisplayName)
Write-Host "Recovering items for" $Mbx.Count "mailboxes..."
ForEach ($M in $Mbx) {
    Write-Host "Checking mailbox" $M.DisplayName
    Restore-RecoverableItems -Identity $M.Alias -SourceFolder RecoverableItems -SubjectContains "Important and Critical Message" }
```

Recover Deleted Items in EAC

The EAC includes a GUI for the *Get-RecoverableItems* and *Restore-RecoverableItems* cmdlets to recover items for user and shared mailboxes (Figure 5-5Figure 5-). To use the EAC to recover deleted items, select the mailbox and then the **Recover deleted items** option. The GUI leverages the cmdlets and can do much of the functionality described above. The differences are:

- EAC offers fixed date ranges (7, 14, and 30 days) and a custom date picker.
- EAC can process a single mailbox at a time.

For performance reasons, EAC shows the latest 50 deleted items. Use the filters to search through recoverable items. For instance, use part of a message subject to find a deleted email.

When an administrator recovers items on behalf of a user by running the cmdlet in PowerShell or the EAC, Exchange Online generates a *Restore-RecoverableItems* audit record for each recovered item in the audit log. An example script showing how to report these audit records can be [downloaded from GitHub](#).

Deleted on	Entry ID	Subject line	Item type	Folder type
6/9/2024 12:35:22 PM	00000000BC908...	[SharePoint Online] Microsoft SharePoint Online: Creat...	IPM.Task	Recoverable Items\Deletion
6/18/2024 4:41:51 PM	00000000BC908...	Important: confirm your subscription	IPM.Note	Deleted Items
6/18/2024 4:41:50 PM	00000000BC908...	You have late tasks	IPM.Note	Deleted Items
6/18/2024 4:41:50 PM	00000000BC908...	You have late tasks	IPM.Note	Deleted Items
6/18/2024 4:41:50 PM	00000000BC908...	You have late tasks	IPM.Note	Deleted Items
6/18/2024 4:41:50 PM	00000000BC908...	From the Sandbox	IPM.Note	Deleted Items

Figure 5-5: Recover deleted items in the Exchange admin center

Archive Mailboxes

The motivation to introduce archive mailboxes (also known as “in-place archives” or “online archives”) for Exchange arose for many reasons. Over the years, Microsoft did not like the fact that customers deployed third-party products like Symantec Enterprise Vault to offload information from user mailboxes to a separate repository. Often there was good reason to move data, especially when Exchange mailbox quotas were small, and databases ran on expensive SAN storage. Moving data to secondary storage managed by other products allowed Exchange mailboxes to continue without the need for increased quotas, albeit with “stubs” left behind in mailboxes as pointers to the actual items. If you plan to move previously archived items from external repositories back into Exchange Online, it is important to ensure that the stubs are “rehydrated” (become fully complete Exchange items) as part of the process.

From a Microsoft perspective, moving information out of Exchange databases implied a certain loss of control as the data could be as easily migrated to a different server as moved back to Exchange. Another issue that has become increasingly important is that PST data are invisible to compliance and data governance features. An example of how important it is for companies to protect their commercial interests and business reputation is seen in [the Sony hack of December 2014](#) when hackers stole and shared valuable contractual information held in PSTs. The messages revealed to the public had details of negotiations, strategies, opinions about business partners, and so on. It would have been so much better had this data been securely kept in online databases rather than being vulnerable to hackers.

Small mailbox quotas encouraged the proliferation of PSTs and created a plague of insecure and potentially corruptible files holding valuable user information. Because email messages are commonly shared between multiple users, PST data usually includes a high percentage of duplicate items. The existence of so much duplicated information slows down the transfer of data from PSTs to online mailboxes. In addition, users can attempt to protect PSTs with passwords that range from very easy to very difficult to crack. If you gather PSTs from users for migration, you must remove passwords from the PSTs to make their data accessible for migration processing. Some third-party PST migration engines can deduplicate content extracted from PST

before ingestion and crack open any password-protected files to extract the information contained within. These are valuable features that you should consider and evaluate during any PST migration (eradication) project.

Because PST migration is often tiresome and expensive, a better solution is to encourage users to keep their data online. The solution to allow online storage to replace PSTs came about in two parts. To make it feasible to provide very large mailbox quotas to users, Microsoft engineered the mailbox database engine to support JBOD. This effort included the introduction of the Native Data Protection features used within Exchange Online today. Archive mailboxes, first introduced in Exchange 2010, are the second part. At that time, the plan envisaged that larger mailboxes meant that no one would ever want to use a PST because their mailbox had so much available space. The accompanying archive mailboxes are the repository for long-term information and avoided the need for Exchange customers to buy a third-party archiving product. Mailboxes have become larger and archive mailboxes are in common use, but users have not yet discarded PSTs. It takes a long time and much effort for Outlook users to break working habits based on PSTs, including using these files as shared repositories when much better options exist like Groups or SharePoint team sites.

Keeping everything in the primary mailbox: [Enterprise plans \(E3 - E5\)](#) grant 100 GB primary mailbox quotas to users, which then creates a question of whether archive mailboxes are necessary. After all, 100 GB should be enough to hold as much data as anyone would want to keep. Although large mailboxes enable people to avoid using archive mailboxes, a workable case exists to separate information into the data which needs to be on hand and items users must keep for reference purposes. In this scenario, the items you need on-hand remain in the primary mailbox, and those needed for reference (or compliance) go into the archive. Good retention policies help users achieve the split by automatically moving items into the archive after a set period (two years is the default).

Archive mailboxes are now available to any Exchange on-premises or cloud mailbox except those using online frontline (kiosk) plans. Some plans like Office 365 E1 [limit the combined storage for primary and archive mailboxes](#) but the Office 365 E3 and plans above include "unlimited" storage. This used to mean unlimited in that auto-expanding archive mailboxes could grow to well over 2 TB. Such massive mailboxes caused operational difficulties, such as problems moving mailboxes between databases, so Microsoft decided to limit the size of archive mailboxes to 1.5 TB.

Microsoft offers Exchange Online Archiving to allow on-premises customers to use a cloud-based archiving service. In this scenario, mailboxes hosted on Exchange on-premises servers can connect to unlimited Exchange Online archive mailboxes without having to perform a full hybrid deployment. The reverse (archive on-premises and mailbox in the cloud) is unsupported. Exchange Online Archiving is also available as an add-on plan for Exchange Online kiosk mailboxes.

An archive mailbox is an online-only extension of the primary mailbox. The link between the two is through the *ArchiveGuid*, a property of the user mailbox that points to the location of the archive. Other archive-related properties set when a mailbox becomes archive-enabled include:

- **ArchiveDatabase:** The Exchange Online database holding the archive mailbox.
- **ArchiveName:** A user-friendly name for the archive mailbox that shows up in a client's resource list. You can change the name to whatever value you like. For example, "Joe's Online Archive."
- **ArchiveQuota:** The current storage quota assigned to the archive. The current default for Exchange Online is 100 GB. Administrators can apply to Microsoft support to have the quota increased.
- **ArchiveWarningQuota:** The threshold for the user to receive warning messages to tell them that space is running out in the archive. The current default is 90 GB.
- **ArchiveStatus:** Set to "Active" when the archive mailbox is available to a user. It is set to "None" when an archive mailbox is not present. In some cases, you might see other values in this property, which is really intended for internal use only.

- **ArchiveState:** Set to "Local" when the mailbox and archive are on the same platform (the case when Exchange Online hosts both).

To assign an archive to a mailbox, select the mailbox in the EAC, go to the Others section in mailbox properties, and use the Manage mailbox archive option to enable or disable the archive. The equivalent PowerShell command is:

```
Enable-Mailbox -Identity 'Joe Smith' -Archive
```

Outlook desktop, the New Outlook for Windows, and OWA support client access to archive mailboxes. Online Archive support for Outlook Mobile is scheduled for October 2024. This update introduces an Online Archive folder for navigation and allows the user to search for items in the online archive. Clients based on the Exchange ActiveSync (EAS) protocol, such as the native mail app client for iOS and Android devices, do not support client access to archive mailboxes.

Shared and room mailboxes can both be enabled with an archive. Although there are many reasons why you might need an archive for a shared mailbox, the case is much less obvious for a room mailbox. You can't enable an archive for a group mailbox. If you archive-enable a shared or room mailbox, remember that you must assign at least an Exchange Online Plan 1 license to the mailbox.

To see what mailboxes are archive-enabled, go to the mailboxes section of the EAC. The archive status is one of the default properties shown for each mailbox. The property is sortable, so you can group the archive-enabled mailboxes together if you sort them. The equivalent PowerShell command to find the set of archive-enabled mailboxes is:

```
[array]$Mbx = Get-ExoMailbox -RecipientTypeDetails SharedMailbox, UserMailbox -Filter {ArchiveDatabase -ne $Null} -ResultSize Unlimited -Properties ArchiveQuota, ArchiveStatus, AutoExpandingArchiveEnabled, RecipientTypeDetails, ArchiveGuid
```

To report the current archive status for these mailboxes, run the *Get-ExoMailbox* cmdlet and specify the Archive property set. The output shown here is for three mailboxes. The first is a user mailbox without the auto-expanding archive enabled. The second is a shared mailbox with a reduced initial archive quota of 50 GB. The last is a user mailbox with the auto-expanding archive enabled. In this instance, the initial archive quota is higher at 110 GB.

```
$Mbx = Get-EXOMailbox -PropertySets Archive -Properties DisplayName -RecipientTypeDetails UserMailbox, SharedMailbox | Sort ArchiveStatus | Format-Table DisplayName, ArchiveStatus, ArchiveQuota, AutoExpandingArchiveEnabled
```

DisplayName	ArchiveStatus	ArchiveQuota	AutoExpandingArchiveEnabled
Michael King	None	100 GB (107,374,182,400 bytes)	False
Office 365 Book Comments	None	50 GB (53,687,091,200 bytes)	False
Jeff Guillet	Active	110 GB (118,111,600,640 bytes)	True

To see how much information Exchange has moved into an archive mailbox, run the *Get-ExoMailboxStatistics* cmdlet and specify the Archive switch. For example:

```
$Mbx = Get-EXOMailbox -PropertySets Archive -Properties DisplayName -RecipientTypeDetails UserMailbox, SharedMailbox -Filter {ArchiveStatus -eq "Active"}
ForEach ($M in $Mbx) {
    $Stats = Get-ExoMailboxStatistics -Identity $M.ExternalDirectoryObjectId -Archive
    Write-Host ("Mailbox {0} Archive Items {1} Size {2}" -f $M.DisplayName, $Stats.ItemCount, $Stats.TotalItemSize)
}
```

Disabling an archive means that you break the connection between the primary and archive mailboxes to remove the mailbox owner's access to the archive. The data in the archive remains intact and does not move back to the primary mailbox. To disable an archive with EAC, open mailbox properties, select the **Others** tab

and open the **Manage mailbox archive** link. Move the option slider to Off and save the change. The PowerShell command to disable an archive is:

Disable-Mailbox -Identity 'Joe Smith' -Archive

Exchange Online does not allow the disablement of an archive if any retention holds exist for a mailbox. This restriction exists to ensure that no one can remove data potentially needed for eDiscovery. Neither EAC nor PowerShell check that a retention hold exists before attempting to disable a mailbox's archive, so you can expect to see errors if you attempt to disable an archive and Exchange then finds that a retention hold exists.

Although disabling an archive prevents user access, it does not remove any archive content. Instead, a 30-day retention period starts. During this time, you can recover the archive and reconnect it to the primary mailbox by re-enabling the archive. Exchange Online removes the archive mailbox after the 30-day deleted mailbox retention period expires. If you examine mailbox properties after disabling an archive, you'll see that the *ArchiveGuid*, a unique value used by Exchange to find the archive mailbox within a database, is a set of zeros. This is how clients know that they shouldn't try to open an archive for this mailbox. However, Exchange preserves the original value of the *ArchiveGuid* in the mailbox's *DisabledArchiveGuid* property, which means that it is easy to re-establish the link to the archive by running the *Enable-Mailbox* cmdlet. After the archive is re-enabled, the two GUID values should be identical.

```
Get-ExoMailbox -Identity 'Joe Smith' -PropertySet Archive | Format-List *ArchiveGuid
```

```
ArchiveGuid      : 00000000-0000-0000-0000-000000000000
DisabledArchiveGuid: d7c65fee-c983-4eac-8fa3-6381a8673212
```

```
Enable-Mailbox -Identity 'Joe Smith' -Archive | Format-List *ArchiveGuid
```

```
ArchiveGuid      : d7c65fee-c983-4eac-8fa3-6381a8673212
DisabledArchiveGuid: d7c65fee-c983-4eac-8fa3-6381a8673212
```

Several of the PowerShell cmdlets that are commonly used to work with mailboxes include an *Archive* switch to point them to the archive rather than the primary mailbox. The *Get-ExoMailboxStatistics* and *Get-ExoMailboxFolderStatistics* cmdlets are good examples:

```
Get-ExoMailboxStatistics -Identity 'Kim Akers' -Archive
```

```
DisplayName      : Online Archive - Kim Akers
MailboxGuid     : afc1e472-0826-498e-b990-85de223e809d
DeletedItemCount : 508953
ItemCount       : 75218
TotalDeletedItemSize : 40.34 GB (43,317,558,017 bytes)
TotalItemSize    : 9.129 GB (9,802,226,010 bytes)
```

```
Get-ExoMailboxFolderStatistics -Identity 'Kim Akers' -Archive | Format-Table Name, ItemsInFolder, FolderSize
```

Inbox	14542 2.551 GB (2,739,174,211 bytes)
Things to Do	2 4.849 MB (5,084,299 bytes)
Office 365 for IT Pros (Management)	4 1.014 MB (1,062,798 bytes)

Note that the *DeletedItemCount* and *TotalDeletedItemSize* properties reported by *Get-ExoMailboxStatistics* refer to information stored in the Recoverable Folders structure. The storage occupied by these items does not count against mailbox or archive quotas. They do apply against the overall 1.5 TB limit for an auto-expanding archive mailbox.

Naming archives: The default name for an archive mailbox is "*In-Place Archive – User*" (for example, "In-Place Archive – Tony Redmond"). However, you can assign whatever name you like by running the *Set-Mailbox* cmdlet. The name can be at least 80 characters (the largest value I have tested). OWA is the only

archive-capable client that will display the name that you assign as Outlook ignores the value and uses a normalized name of "*Online archive – primary SMTP address*". There is no reason why the two client development teams decided to display different default names for archive mailboxes or why Outlook did not follow OWA in allowing the display of user-specific names. It is just another Exchange quirk.

Moving Information into Archive Mailboxes

After a mailbox is archive-enabled, it appears automatically in client interfaces. OWA recognizes the archive the next time the user connects to Exchange Online, and the Outlook desktop client learns that the archive exists when it refreshes the list of available resources through the Autodiscover process. When the archive appears, the user can move information to it by creating folders and dragging and dropping items from their primary mailbox.

Exchange Online uses mailbox plans to assign default values to new mailboxes. One of the values in a mailbox plan defines the retention policy for the mailbox. This isn't a Microsoft 365 retention policy. Instead, it's an Exchange mailbox retention policy that can contain a default archive tag to control how items move from the primary mailbox into the archive (if a mailbox is archive-enabled). For instance, if the default archive tag defines a retention period of two years, the Managed Folder Assistant moves items that don't have another retention tag from the primary to the archive mailbox once they reach two years old. The items go into a folder with the same name.

Using a default archive tag means that archive mailboxes grow on an ongoing basis as items move from the primary mailboxes. To remove items from the archive, the retention policy can include a default delete tag. For instance, if the retention period for the default delete tag is five years, the MFA will:

- Obey the retention period specified in the default archive tag and move items from the primary mailbox to the archive after two years.
- Obey the retention period specified in the default delete tag to remove items from the archive after a further three years (the items reach the five-year limit).

In addition, when a mailbox is archive-enabled, MFA moves items captured because of retention processing in the Purges, Versions, and DiscoveryHolds sub-folders under the Recoverable Items folder one day after their creation (depending on when the MFA processes a mailbox, the actual move might take place two or three days after creation). This action frees up space in the Recoverable Items quota assigned to mailboxes (100 GB when a mailbox is under hold) to allow the primary mailbox to store more time-critical data such as the items in the Deletions folder.

Of course, most users are blissfully unaware of the boring details of retention policies. They might not even notice the movement of items from the primary mailbox to the archive mailbox until they look for something and can't find it because the item is not where they thought it should be – in their mailbox. Of course, the item is still available, and it is, in a roundabout way, still in their mailbox. It is just invisible in some respects because the user doesn't know where it is or understand how it got there.

Microsoft defines archive mailboxes as personal repositories. [Microsoft explicitly prohibits](#) the use of transport rules, journal rules, auto-forwarding, or other methods to move information into a mailbox from multiple sources for archiving purposes. However, it is permissible to import data from multiple PSTs that might have originated from multiple users into an archive mailbox. The difference between the two is that using an archive mailbox as an archive destination creates the potential that the archive mailbox will expand on an ongoing basis to cope with the items moving into the archive. On the other hand, if you perform a once-off import to an archive mailbox, its content will probably not change all that much in the future as the archive is essentially historical rather than live. In other words, it's a question of dealing with "hot" data that is constantly growing or "cold" data imported once and hardly ever accessed thereafter.

Effective Use of Archive Mailboxes

Because primary user mailboxes can hold up to 100 GB, many users can quite happily get along by just using their primary mailbox and never need to use an archive. Consider the following:

- It will take most users several years to accumulate 10 GB of mailbox data. Some users accumulate 20 GB+ of new mailbox content annually, but they are exceptional. On the other hand, people have had quite a while to accumulate information in their mailboxes at this point and many of the mailboxes that move to Exchange Online are already up at the 20 GB mark (or higher).
- In the past, many caveats were expressed about the desirability of holding more than 2 GB in the primary mailbox. Apart from the cost of storage, most problems related to offline access and the need to synchronize such a large amount of data to an OST file whose internal structure was never designed to cope with large volumes. These issues have largely been dealt with today due to faster networks and smarter Outlook synchronization. The larger amounts of data synchronized to clients do slow down OST access speeds, a factor that can be handled by equipping laptops with SSDs that effectively disguise the inefficiency of the OST.
- Archive mailboxes are only available online. Outlook does not synchronize any folder from the online archive into the OST. While users might never access items stored in their archive mailboxes again, the potential that someone might need an archived item when a network connection is not available does exist.
- Searches can find items stored in archives but only if the user specifies that Outlook should search "All Mailboxes." Searching the archive in OWA requires the user to open a folder within the archive. Neither of these operations is especially intuitive to someone who might be unaware that they have an archive.
- Mobile clients cannot access items held in archive mailboxes because the protocols used by mobile clients to interact with Exchange Online do not include the ability to open archive mailboxes.
- Users are seldom able to decide what items should be always available (and in their primary mailbox) and those that should be in the archive. Expecting users to decide on a data storage strategy is an act of folly. Implementing automatic archival via mailbox retention policies is the best strategy.

With these points in mind, it should come as no surprise to find that some tenants avoid the use of archive mailboxes and tell users to exploit the storage now available in primary mailboxes. Indeed, some companies have reversed course and decided to only use primary mailboxes. In some cases, they have had to move information back from archives to primary mailboxes. Apart from dragging and dropping items from folder to folder using Outlook or OWA or exporting archive items to a PST and importing them back into the primary mailbox, there is no in-built method to do this. In most cases, the solution is to create a script to move items using a combination of PowerShell and Exchange Web Services.

On the other hand, some tenants consider archive mailboxes to be the perfect answer to the problem of unmanaged and proliferating PSTs and make strenuous efforts to import data from user PSTs into archive mailboxes so that everything is online and available for compliance. The availability of Microsoft's Import Service, which allows tenants to load PSTs into Azure for later import into user mailboxes (primary or archive) has spurred many companies to consider how they should deal with PSTs in the future. Moving information from PSTs into archive mailboxes exposes the data for compliance purposes, but this is an exercise that involves much more than ingesting data from individual PST files. Before importing anything, you must decide how to collect the PSTs, clean them up (remove corruptions), crack passwords set on the PSTs, and possibly deduplicate the content so that the import processes clean information. Remember the adage that rubbish in equals rubbish out.

Another effective use of archive mailboxes is to hold data migrated from older POP3 or IMAP4 systems. It is also fair to say that companies who have moved data back from third-party archiving solutions to Exchange

Online find archive mailboxes to be a natural evolution. In summary, the decision to use or ignore archive mailboxes comes down to the circumstances and business conditions that exist within a tenant.

PST Import Tools: Many tools are available to help you move data from user PSTs into primary or archive mailboxes. Like any software utility, you should carefully test the software in your environment to discover which product best meets your needs. Once you have collected and prepared (made sure no corruption exists) the PSTs, you can use the Import service to either upload the PSTs over the network or send them on hard drives to a Microsoft data center for processing. In either case, the PST data will be ingested into Azure and can be imported from there into user mailboxes.

Auto-Expanding Archives

Archive mailboxes store information that's not needed daily but users need to retain for the long-term. The default simple archive mailbox assigns 100 GB of storage to hold data moved to the archive by users or Exchange mailbox policies. This quota is sufficient in most cases, but some mailboxes have the need to hold much higher quantities of data. Microsoft's solution is the "auto-expanding archive," meaning that the archive mailbox automatically expands up to a 1.5TB limit.

User mailboxes and shared mailboxes with E3 and E5 licenses or with the Exchange Online Plan 2 license or the Exchange Online Archiving add-on can use auto-expanding archives. Exchange Online won't enable a mailbox with an auto-expanding archive unless it is eligible. You can check a mailbox's persisted capabilities, which expose the capabilities available to the mailbox. In this case, the presence of *BPOS_S_Enterprise* means that the account that owns the mailbox has the Exchange Online Plan 2 service plan as part of its assigned licenses and therefore can use auto-expanding archives. The other values are *BPOS_S_ArchiveAddOn* (Exchange Online Archiving) and *BPOS_S_Archive* (standalone Exchange Online Plan 2).

```
Get-ExoMailbox -Identity TRedmond -Properties PersistedCapabilities | Select -ExpandProperty PersistedCapabilities
```

```
BPOS_S_ThreatIntelligenceAddOn  
BPOS_S_EquivioAnalytics  
BPOS_S_CustomerLockbox  
BPOS_S_Analytics  
BPOS_S_Enterprise
```

In some respects, the technique used to expand archives borrows from the auto-split capability built into public folder mailboxes. When a public folder mailbox approaches 50 GB, the Mailbox Replication Service creates a new mailbox and (MRS) transfers folders to the new mailbox to balance the load.

Auto-Expand Archive Limits: Microsoft imposed a 1.5 TB limit for auto-expanding archives from November 1, 2021. While there are thousands of terabyte-plus archives in use, the limit is unlikely to affect many tenants. If the change affects your organization, you should contact Microsoft support. A script to report how close archive-enabled mailboxes are to the limit is [downloadable from GitHub](#).

[Microsoft's guidelines](#) say that only individual or shared mailboxes with a growth rate that does not exceed 1 GB per day support expandable archives. The reason for this restriction is to ban the use of archive mailboxes as targets for the migration of non-personal data from legacy services. It is perfectly acceptable to use an archive mailbox as a migration target for personal data such as PSTs.

Enabling Auto-Expanding Archives

Before enabling auto-expanding archives for some or all mailboxes, consider the following:

- Once an archive mailbox is auto-expanding, it remains in that state and cannot be reverted to be a simple archive.
- An archive mailbox enabled for auto-expanding has its *AutoExpandingArchiveEnabled* property set to true and a 110 GB quota (as opposed to the 100 GB norm). After an archive adds additional storage

- to expand, you can also check its mailbox locations to see how many “chunks” of storage the expanded archive occupies.
- Exchange Online doesn’t support the recovery or restoration of an inactive mailbox with an auto-expanding archive. To recover data from an inactive mailbox in this state, use a content search to find the mailbox contents and export the search results to a PST. Then import the PST into a target mailbox.
 - No version of Exchange Server supports auto-expanding archives. It is therefore impossible to move an auto-expanding archive to Exchange Server. You can move the primary mailbox back to Exchange Server, but the auto-expanding archive must remain in the cloud. The same restriction applies to hybrid deployments where on-premises mailboxes use cloud archives.

Enablement of auto-expanding archives on an organization-wide or per-mailbox basis is only possible using PowerShell. To enable auto-expanding archives for the entire organization, run the *Set-OrganizationConfig* cmdlet to update the tenant configuration:

Set-OrganizationConfig -AutoExpandingArchive

After configuring the organization, existing archive mailboxes automatically become auto-expanding and new archives will be auto-expanding. The process of enabling existing archives can take some time to complete due to the need for the Managed Folder Assistant to process each mailbox. Only [a subset of Exchange Online clients](#) support access to the data in an auto-expanding archive. Other clients can access information in the primary archive but cannot access any data moved into an auxiliary archive.

If you do not want to enable auto-expanding archives for the entire organization, you can control the capability on a selective per-mailbox basis using the *Enable-Mailbox* cmdlet. An archive must already exist for the mailbox before you can make it auto-expanding. For instance, to enable an auto-expanding archive for Kim Akers:

Enable-Mailbox -Identity "Kim Akers" -AutoExpandingArchive

When you enable auto-expanding archives for a mailbox, Exchange:

- Increases the normal archive 100 GB quota for the primary mailbox to 110 GB and modifies the quota warning threshold from 90 GB to 100 GB.
- If the mailbox comes within the scope of a hold, Exchange increases the Recoverable Items quota from 100 GB to 110 GB.

It can take up to 30 days before the process to enable auto-expansion for an archive completes. The changes to the primary mailbox quotas reflect the fact that heavily-trafficked mailboxes use auto-expanding archives. It makes sense to give the initial archive quota a little extra headroom to ensure that the mailbox can continue operating while the process to enable the auto-expanding archive proceeds.

One limitation is that if you need to search auto-expanding archives with OWA or Outlook, you can only search within a specific folder. eDiscovery content searches can find information stored in any part of an auto-expanding archive, which also supports litigation and in-place holds as normal.

In most cases, it is preferable to enable auto-expanding archives for selected accounts instead of a complete tenant. Those accounts usually have a genuine business need to keep massive quantities of information for certain periods.

How an Archive Mailbox Expands

When you enable a mailbox for archiving, it starts with a single 110 GB archive mailbox. After the occupied space within the archive mailbox approaches the transition threshold (90% of quota, or 99 GB), a mailbox assistant automatically provisions a new archive mailbox. Exchange calculates the occupied size from the total

size of folders in the archive mailbox with their *Movable* flag set to *\$True* or the *FolderType* set to *DeletedItems* or *RecoverableItems*.

To find the set of mailboxes enabled for auto-expanding archives, run the command:

```
Get-EXOMailbox -RecipientTypeDetails UserMailbox, SharedMailbox -Properties AutoExpandingArchiveEnabled -ResultSize Unlimited | Where-Object {$_.AutoExpandingArchiveEnabled -eq $True } | Format-Table DisplayName, RecipientTypeDetails
```

Exchange Online only transforms eligible mailboxes to have auto-expanding archives when the original archive is more than 90% full. To find the set of mailboxes currently using archives that Exchange Online has expanded, use the command:

```
Get-ExoMailbox -ResultSize Unlimited -RecipientTypeDetails UserMailbox, SharedMailbox -Properties MailboxLocations| Where-Object {$_.MailboxLocations -like "*AuxArchive*"} | Format-Table DisplayName, MailboxLocations
```

To see details of the current state of the primary archive for an individual mailbox, we can use PowerShell to scan the folders in the primary archive to report the occupied space. Later in this section, we discuss how to retrieve the GUID for the primary archive to use as input for the *Get-ExoMailboxFolderStatistics* cmdlet. The *Report-PrimaryArchiveFolderSizes.ps1* script is available from our [GitHub repository](#). An example of the output is below:

```
Enter User to check: James.Ryan
106 movable folders found. Occupied space 8550286513 bytes or 7.963 GB. At 8.04% of 99 GB transition threshold
```

The new “chunk” or “shard,” or more correctly “auxiliary archive,” joins the auto-expanding archive mailbox. Exchange links the GUID pointing to the new auxiliary archive to the GUIDs of the existing auxiliaries and primary archive to form a chain or set of mailboxes that the Information Store considers a single logical entity. The expansion of an archive to form an archive chain occurs without user intervention and without affecting supported clients, which continue to query the Information Store for data and receive data back without knowing which part of the archive holds the data.

The Managed Folder Assistant coordinates the movement of information out of the primary archive to an auxiliary archive to reduce the size of the primary archive under the transition threshold. This exercise aims to move enough data to the auxiliary archive to get the primary archive under 50% of its current size. So, if the primary archive grows to 95 GB, the Managed Folder Assistant examines the folders in the primary archive and selects enough to move approximately 47.5 GB to the auxiliary archive. The Deleted Items and Recoverable Items folders are not movable, but the Managed Folder Assistant can create sub-folders under these folders in the target archive and move content there.

The Mailbox Replication Service moves the data from the primary to the auxiliary archive and takes care of ongoing synchronization to ensure that any changes made to data while the move progresses are in the moved data. The copying of content occurs in the background. To ensure that no data loss occurs during the rebalancing of the archive, the primary archive keeps the copied data for 30 days. When this period elapses, the Managed Folder Assistant flushes the copied data from the primary archive to release the space.

Archive Links

Archives link to their primary mailboxes by storing the GUID pointing to the archive as a mailbox property. The GUID is enough for Exchange to find the archive in a database. The auto-expanding archive replaces the single GUID that connects the mailbox to the archive with a linked list of GUIDs. Each of the GUIDs points to a separate auxiliary archive of up to 50 GB, which Exchange Online combines with the other auxiliary archives and the primary archive to form a logical archive mailbox.

You can see the details of the GUIDs by running the `Get-ExoMailbox` cmdlet to examine a mailbox's properties. If you look at the `MailboxLocations` property, you will see something like this:

```
Get-ExoMailbox -Identity TRedmond -Properties MailboxLocations | Select -ExpandProperty MailboxLocations
1;0370f354-2752-4437-878d-cf0e5310a8d4;Primary;eurprd04.prod.outlook.com;d96ca5a2-340d-4c83-be33-d4a7a8c9b1d6
1;afc1e472-0826-498e-b990-85de223e809d;MainArchive;eurprd04.prod.outlook.com;e46d4e31-3734-47dc-801d-5d59f9988766
```

The information about mailbox locations reported by `Get-ExoMailbox` divides into two sections: one for the primary mailbox and the second for the archive. Only the primary mailbox and the primary archive are shown here. If other auxiliary archives are present, the archive section lists them as mailboxes 2, 3, 4, and so on. The information for the two mailboxes is:

Primary mailbox:

- The `ExchangeGUID` (which ties the mailbox back to a user account).
- "Primary" to show that this data refers to the user's primary mailbox.
- If, as in this case, the mailbox database is in Exchange Online, the name of the Exchange Online forest is noted (eurprd04).
- The GUID of the database holding the mailbox.

Archive mailbox:

- The `ArchiveGUID` (which is only present when a mailbox is archive-enabled).
- "MainArchive" to show that this data is an archive set. When auxiliary archives are part of the set, they are tagged with "AuxArchive."
- The name of the Exchange Online forest hosting the archive mailbox. This value is empty for on-premises mailboxes.
- The GUID of the database holding the archive.

In this case, the mailbox and the archive are in the same database (you can confirm this by using `Get-Mailbox` to examine the `Database` and `ArchiveDatabase` properties). And, as you would expect, both the primary and archive mailboxes are in the same Exchange Online forest. Another way of accessing information about these archives is with the `Get-MailboxLocation` cmdlet. For example:

```
Get-MailboxLocation -User TRedmond | Sort MailboxLocationType -Descending | Format-Table
MailboxGUID, MailboxLocationType
-----
0370f354-2752-4437-878d-cf0e5310a8d4 Primary
afc1e472-0826-498e-b990-85de223e809d MainArchive
bb131464-1461-147e-b774-41646ddadd11 AuxArchive
```

In this case, the `MailboxGuid` property for the user's primary mailbox and all the parts of the archive are more obvious. The `MailboxGuid` is needed if you want to check how much data Exchange has moved to an auxiliary archive. For example:

```
Get-ExoMailboxStatistics -Identity bb131464-1461-147e-b774-41646ddadd11 | Format-Table ItemCount,
TotalItemSize
-----
30225 4.398 GB (4,722,299,639 bytes)
```

We now know that Exchange has moved a certain amount of data to the auxiliary archive.

Migrating Large On-Premises Archives: On-premises archive mailboxes can grow past 100 GB. At this point, they can no longer be migrated to Exchange Online using the online migration tools. The reason is that even for auto-expanding archives, the initial quota assigned by Exchange Online is all that's available until the auto-expansion provisioning process completes. Even then, an auto-expanding archive cannot add storage dynamically in the middle of an online migration. For this reason, two options exist if you have large on-premises archive mailboxes to move to Exchange Online: reduce the archives to under 100 GB and use the online migration tools or find a different migration tool. One approach is to export archive data to PSTs and import the PSTs into Exchange Online using the Office 365 Import Service. A third-party migration service might be able to automate much of the processing needed to get the data imported into Exchange Online.

Outlook's Archive Folder

Exchange Online mailboxes include an Archive folder in the default set of folders created for all mailboxes. Apart from a user being able to apply a retention tag to the Archive folder to move items in the folder to the archive mailbox after a period, the Archive folder has no relationship to the "online archive." Instead, Microsoft envisages the Archive folder as a convenient place to move items from the Inbox after a user has finished processing the items but wishes to keep them for a period. It's also a way for users to file items that they want to keep when they don't have the licenses necessary to use Exchange online archives.

Two tenuous reasons support the use of the Archive folder:

- It is available offline because Outlook can synchronize the folder and its contents, just like any other folder in the primary mailbox.
- It is available to mobile clients. Neither the Exchange ActiveSync nor Outlook mobile protocols support access to archive mailboxes, but they can access the Archive folder.

The argument against the Archive folder is that it's as easy to leave items in their original folder in the primary mailbox and access the items there.

Outlook, OWA, and Outlook Mobile include options to allow users to easily move items to the Archive folders. Outlook for Windows uses the backspace key to move items to the Archive folder. This can be annoying as items invariably end up in the folder that you never intended to move there. To disable this one-click-to-archive behavior, update the system registry and add the *DisableOneClickArchive* DWORD value at *HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\outlook\options*. Set the value to 1 to stop the action.

Shared Mailboxes

Shared mailboxes have been part of the Exchange product since Exchange 2000. They meet the need to have a mailbox to handle messages that a team of people share responsibility for, such as the team staffing a support desk. The implementation of shared mailboxes in Exchange Online is like that found on-premises, with an Entra ID user account used to provide an identity for the shared mailbox. All access to shared mailboxes is delegated. In other words, users receive the rights to access the shared mailbox and use those rights to open and interact with the mailbox contents. Although you can change the password of the Entra ID account used by a shared mailbox and sign into the account to access the mailbox directly, this is a Microsoft licensing violation, and you shouldn't do it.

Shared mailboxes have many uses, including:

- To allow groups of users shared access to functional email. For example, all the support agents who staff a help desk can use a shared mailbox to review and respond to messages sent to the help desk by users asking for help. Sometimes these mailboxes are called functional mailboxes and are often used to ensure that incidents can be managed effectively by multiple people across shift boundaries.

A major attraction of this use is that messages sent in response come from the shared mailbox rather than the individual user.

- To allow access to the mailbox of a colleague who has left the company. This is done by converting the user (regular) mailbox into a shared mailbox and assigning access to the mailbox to those who need access. This technique is used extensively in on-premises organizations where inactive mailboxes are unavailable. To change a user mailbox to a shared mailbox with PowerShell, run the *Set-Mailbox* cmdlet:

```
Set-Mailbox -Identity Tom.Sawyers -Type Shared
```

To convert the mailbox back to a user mailbox, run:

```
Set-Mailbox -Identity Tom.Sawyers -Type Regular
```

Mailbox delegation goes together with shared mailboxes because there is not much point in creating a shared mailbox if you cannot then access the mailbox. Because a shared mailbox is linked to a user object in Entra ID, access to its contents must be gained by delegating or granting permissions over the mailbox to other users. The *Get-ExoMailbox* cmdlet enables us to discover the set of shared mailboxes known in a tenant:

```
Get-ExoMailbox -RecipientTypeDetails SharedMailbox | Format-Table Name, DisplayName, Alias
```

Name	DisplayName	Alias
Customer Services	Customer Services	CServices
Book Feedback	Book Feedback	BookComments
Help Desk	Corporate Help Desk	HelpDesk

A shared mailbox can be hosted by Exchange Online or, in a hybrid environment, on-premises. In this instance, the shared mailbox is known as a remote shared mailbox when accessed from the other platform. It is best to keep shared mailboxes on the same platform as used by the accounts that have delegated access to the mailboxes. In other words, if you want to move some shared mailboxes to Exchange Online, move the mailboxes that access those shared mailboxes to Exchange Online too. Exchange Online places no limit on the number of shared mailboxes that you can create within a tenant.

Licensing, Quotas, and Limitations of Shared Mailboxes

Usually, a shared mailbox does not need a license. However, shared mailboxes [need an Exchange Online Plan 2 license](#) if:

- The contents of the shared mailbox exceed 50 GB.
- The shared mailbox is archive-enabled. This allows the Managed Folder Assistant to offload older items through an Exchange Online mailbox retention policy.
- The shared mailbox is on litigation hold. Unless the shared mailbox is assigned an Exchange Online license, it cannot be placed on litigation hold. If a shared mailbox is under litigation hold, the implication is that the mailbox originally belonged to a user prior to [conversion to a shared mailbox](#). Organizations sometimes preserve the mailboxes of ex-employees by converting them into shared mailboxes. In many cases, [making the mailboxes inactive](#) is a better choice.

To assign a license, go to the Active users view in the Microsoft 365 admin center, select the shared mailbox, edit its properties, and assign the license under **License and Apps**. In effect, you assign the license to the user account automatically created by Exchange Online for the shared mailbox. If you don't have any Exchange Online Plan 2 licenses available, you can assign a license that contains the Exchange Online Plan 2 service plan, like Office 365 E3.

Microsoft documentation has always said that the default quota for shared mailboxes is 50 GB. Because of some errors in the provisioning process, some shared mailboxes received a 100 GB quota. These mailboxes

keep their 100 GB quota unless the mailbox state changes. For example, if you convert a shared mailbox to be a user mailbox and then convert it back again, the shared mailbox object then needs a license to keep its 100 GB quota. New shared mailboxes receive the correct 50 GB quota.

A PowerShell script [described in this article](#) reports on the set of shared mailboxes in a tenant. The report shows the current number of items in each mailbox, the size of the mailbox, the assigned quota, whether it is licensed, and if it has an archive. In this case, only one shared mailbox is licensed, one was previously licensed but had the license removed, and the others have never been licensed. Some of the mailboxes existed before Microsoft put the new provisioning process in place, so they have 100 GB quotas. Others have 100 GB quotas because they have licenses. An article and accompanying script have been published. Some sample output is shown below:

Mailbox	Total Items	Mailbox Size	Quota	Licensed	Archive
Customer Services	213	7.484 MB	50 GB	False	Enabled
Book Feedback	301	7.278 MB	50 GB		Enabled
Redirect for Removed Mailboxes	198	814 KB	50 GB		Disabled
Redmond Shared Events	3777	190.5 MB	100 GB	True	Disabled
Company Information	252	897.4 KB	100 GB		Disabled

If a shared mailbox without a license exceeds 50 GB, Exchange Online prevents the mailbox from being able to send new emails and stops delivering inbound messages to the mailbox. The block lasts until the mailbox receives a license. Because Exchange Online caches mailbox information, the newly licensed status, and the 100 GB quota, take about 15 minutes to become effective, after which email delivery recommences.

If you convert a user mailbox holding more than 50 GB to a shared mailbox (often done to keep mailboxes for former employees), Exchange continues to deliver mail to the mailbox while the mailbox is licensed. In most cases, people convert user mailboxes to shared mailboxes to free up licenses, so if you go ahead and do this, Exchange detects that the mailbox holds more than 50 GB and ceases email delivery. You can restore delivery by removing content from the mailbox to get it under the 50 GB quota or by assigning a license.

Migrating shared mailboxes from on-premises Exchange organizations will fail if they hold more than 50 GB and the user account for the target shared mailbox in Exchange Online is unlicensed. To allow migrations to succeed (up to the 100 GB quota), assign a license to the MailUser object. This limitation exists for all migrations performed by the Mailbox Replication Service (MRS) or third-party migration utilities.

An unlicensed shared mailbox can be placed on hold or archive-enabled as Exchange Online does not perform a licensing check before enabling the feature. These are technical licensing breaches that will only come to light in an audit. Even if the mailboxes continue to work without a license, the danger always exists that Microsoft might turn on code to enable restrictions to stop unlicensed shared mailboxes from working, so it's best to make sure that the correct licenses are in place.

Although companies often use shared mailboxes for functional purposes, apart from inbox rules, Exchange doesn't have any out-of-the-box way to automate the processing of messages arriving in a shared mailbox, so a mailbox delegate must sign into the mailbox to handle new emails. Performance for a shared mailbox can be problematic if more than twenty users try to access it concurrently. Finally, users who have an Exchange Online frontline/kiosk license cannot add delegates to their mailbox, but they can access a shared mailbox if someone makes them a delegate for that mailbox.

Creating a New Shared Mailbox

New shared mailboxes are created through the **Groups** section of the Microsoft 365 admin center, the Exchange admin center, or with PowerShell. Not much information is needed to create a shared mailbox. After completing the add process, Exchange Online needs a short delay to provision the mailbox and make it ready

to add the users who will access and use the mailbox. Remember that users do not log into a shared mailbox as happens with a regular mailbox and that access to its contents

Mailbox Delegates and Permissions

After creating a shared mailbox, you must assign permission to the mailbox to allow access to those who need to work with it (its delegates). You can assign permissions when creating a new shared mailbox or by editing the mailbox object in the Microsoft 365 admin center, Exchange admin center, or using PowerShell. Mailboxes support three types of delegate permissions:

- **Full Access** permission allows a user to open the shared mailbox and access its contents. Full Access does not mean that a user has *SendAs* permission. Microsoft 365 refers to this permission as “Read and manage mail to this mailbox.”
- **Send As** permission allows a user to send messages from the shared mailbox that appear as if the messages came from the shared mailbox rather than the user. In effect, a user with this permission can impersonate the mailbox. This is the best situation when you want replies to conversations started from the mailbox to flow back to the shared mailbox.
- **Send On Behalf Of** permission means that a user can send an email on behalf of the mailbox. Unlike the Send As permission, the name of the user who sends the message is obvious. You can only set this permission for a shared mailbox through PowerShell.

Full Access permission allows a user to work with all folders and items inside the shared mailbox. Users need both Full Access and Send As permissions to work with a shared mailbox as if it was their personal mailbox. In addition to shared mailboxes, which is why these are the two permissions featured in the admin centers, Exchange Online supports the assignment of the Send As and Send on Behalf of permissions to user and group mailboxes.

After creating a shared mailbox with the Microsoft 365 admin center or EAC, you can use the **manage mailbox permissions** option (Microsoft 365 admin center) or **Manage mailbox delegation** option (EAC) to define permissions for the shared mailbox. As noted above, the following permissions are available for shared mailboxes:

- Read and manage (Full Access).
- Send As.

Figure 5-6 shows that two users have full access to a shared mailbox (oddly, three have the Send As permission). Because Exchange Online caches permissions for better performance, it can take up to an hour for the new permission to be effective. In addition to a refresh of the server caches, clients must learn that users have permissions for a shared mailbox. For example, Outlook clients learn about access to a shared mailbox through its Autodiscover process, which runs every 15 minutes for this purpose.

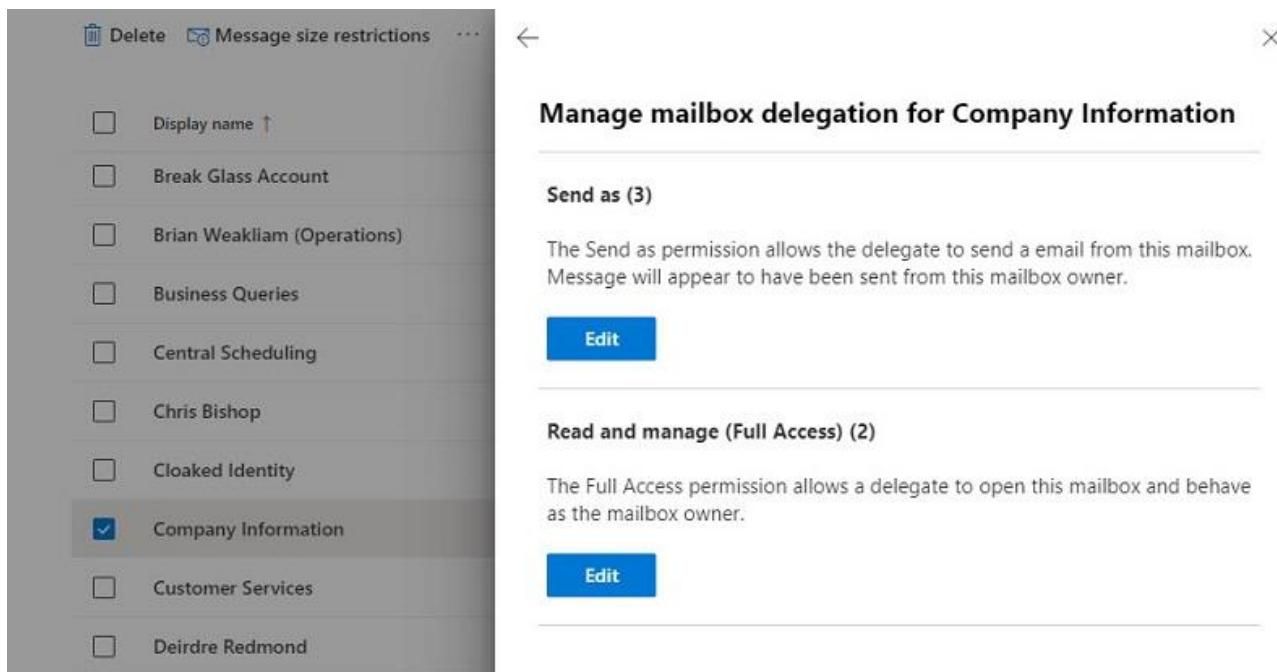


Figure 5-6: Assigning delegate permissions for a shared mailbox (EAC)

If you need to assign access to a shared mailbox to multiple users, it is often more convenient to assign permission to a distribution list, which must be a security-enabled group. You cannot assign permissions for a shared mailbox to a normal distribution list because these groups are not security principals, and you cannot assign permissions to a group or a dynamic distribution list either.

Shared mailbox or Groups: On the surface, Groups seem like a better and more modern choice as the basis for team sharing than a shared mailbox. That statement might be true if the requirement is to collaborate based on shared documents, meetings in the group calendar, and threaded conversations with perhaps a link to a plan managed by Planner. However, shared mailboxes still have some unique strengths. For instance, shared mailboxes allow access to a full range of folders rather than the limited set used in a group mailbox. In addition, shared mailboxes support shared contacts and tasks while these are unavailable to groups. Shared mailboxes also support categories, rules, and Outlook add-ins, all of which can be very important to customer support or sales teams. The point is that the two types of mailboxes are suitable for different purposes. Think about how people need to share information and what type of information they need to work with before you select which type to use.

Handling Messages Sent from Shared Mailboxes

If you use a shared mailbox for customer communications or a similar purpose, you probably want to keep any replies sent by people using the *SendAs* or *Send on Behalf Of* permission in the mailbox. The default behavior is that Exchange keeps messages in the mailbox of the person who sends a message, even if they are replying as or on behalf of the shared mailbox. This is fine for personal mailboxes, but not so good for shared mailboxes. Consider the example of a mailbox used to receive customer comments or complaints where a team of support agents accesses the mailbox. If an agent answers a message, their mailbox stores the reply and none of the other team members know that the customer has received a response (or what that response said).

You can control these settings with PowerShell by running the *Set-Mailbox* cmdlet. For example, this command tells Exchange to retain copies of messages sent using the *Send As* and *Send on Behalf Of* permissions in a shared mailbox.

```
Set-Mailbox -Identity SharedMailbox -MessageCopyForSendAsEnabled $True  
-MessageCopyForSendOnBehalfEnabled $True
```

To ensure consistency and enable these settings across all shared mailboxes in the tenant, the command is:

```
Get-ExoMailbox -RecipientTypeDetails SharedMailbox -PropertySet All | ?  
{$_._MessageCopyForSendAsEnabled -eq $False -or $_._MessageCopyForSendOnBehalfEnabled -eq $False} |  
Set-Mailbox -MessageCopyForSendOnBehalfEnabled $True -MessageCopyForSentAsEnabled $True
```

Somewhat along the same vein is the situation that occurs when a member removes items from a shared mailbox. Logically, you might think that these items would go into the Deleted Items folder of the shared mailbox. However, Outlook moves such items into the Deleted Items folder of the delegate's mailbox. To change this behavior, update the system registry by creating a new DWORD value at:

```
HKEY_CURRENT_USER\Software\Microsoft\Office\[xxx]\Outlook\Options\General\DelegateWastebasketStyle
```

Replace [xxx] with 15.0 for Outlook 2013, and 16.0 for both Outlook 2016 and Outlook 2019. Set the value to 4 (four) and restart Outlook. Deleted items will now stay in the Deleted Items folder of the shared mailbox, which is really where they should be.

Since this is a client setting, the behavior of other clients such as the new Outlook for Windows or OWA will not change.

Creating and Managing Shared Mailboxes with PowerShell

The PowerShell command to create a new shared mailbox is straightforward as all you must specify is the name. However, it's good practice to specify an alias, and primary SMTP address (which must belong to the tenant domain) to make sure that they have the expected values. Other important mailbox properties such as the MRM policy, RBAC role assignment policy, and mailbox quotas are set automatically. This command is an example of how to create a new shared mailbox.

```
New-Mailbox -Shared -Name "End User Services" -Alias Shared.EndUserServices  
-PrimarySmtpAddress "EndUserServices@Office365ITPros.com"
```

Remember to create a unique alias for the new shared mailbox. In the example above, the alias is created by prefixing "Shared" and a period in front of a value derived from the mailbox's display name. This should be enough to ensure uniqueness.

After creating the new shared mailbox, we need to add some members. Somewhat confusingly, we need to run two different cmdlets to grant the full set of permissions over the mailbox. The reason why this situation exists is that we need to grant a user permission to open the mailbox and work with folders and then the right to send as (impersonate) the mailbox. In other words, the first is an access right, the second is the right to do something for the mailbox. In this example, we use the *Add-MailboxPermission* and *Add-RecipientPermission* cmdlets to grant Kim Akers *FullAccess* rights to the mailbox and then the *SendAs* permission.

```
Add-MailboxPermission -Identity 'Book Feedback' -User 'Kim Akers' -AccessRights FullAccess
```

```
Add-RecipientPermission -Identity 'Book Feedback' -Trustee 'Kim Akers' -AccessRights SendAs -  
Confirm:$False
```

You can remove any extraneous permissions with the *Remove-MailboxPermission* or *Remove-RecipientPermission* cmdlets. For example:

```
Remove-MailboxPermission -Identity 'Book Feedback' -User 'Kim Akers' -AccessRights FullAccess  
-Confirm:$False
```

```
Remove-RecipientPermission -Identity 'Book Feedback' -Trustee 'Kim Akers' -AccessRights SendAs  
-Confirm:$False
```

It is sensible to conduct periodic reviews of the permissions that are assigned to shared mailboxes and to remove permissions that are no longer needed. You can use the *Get-ExoMailboxPermission* and *Get-*

RecipientPermission cmdlets to check who has access to a mailbox and what they can do. Here is an example of using the *Get-RecipientPermission* cmdlet to view details of accounts that have the *SendAs* permission for a mailbox. The same command works for both shared and personal mailboxes.

```
Get-RecipientPermission -Identity 'Book Feedback'
```

Identity	Trustee	AccessControlType	AccessRights	Inherited
Book Feedback	NT AUTHORITY\SELF	Allow	{SendAs}	False
Book Feedback	Tony Redmond	Allow	{SendAs}	False
Book Feedback	Kim Akers	Allow	{SendAs}	False

The *Get-ExoMailboxPermission* cmdlet returns access permissions for a mailbox. In the past, the full set included many system accounts and management role groups that have access to mailboxes. Today, the set is limited to users, groups and system entries like NT AUTHORITY\SELF. In this example, we use the *Get-ExoMailboxPermission* cmdlet to check the permissions for a mailbox and trim the returned set to only report delegated user accounts:

```
Get-ExoMailboxPermission -Identity 'Book Feedback' | Where-Object {$_.User -notlike "NT AUTHORITY\*"} | Format-Table User, AccessRights
```

User	AccessRights
Tony.Redmond@office365itpros.com	{FullAccess}
Kim.Akers@office365itpros.com	{FullAccess}

A more complete script to create a report of all non-standard permissions (FullAccess, Send on Behalf Of, and SendAs) currently present on user and shared mailboxes is [available on GitHub](#).

We can also use the permissions on shared mailboxes to discover the list of shared mailboxes that a user can access:

```
Get-ExoMailbox -RecipientTypeDetails SharedMailbox | Get-MailboxPermission -User "Kim.Akers@Office365itpros.com"
```

Send on Behalf Of permission

Exchange Online also supports assigning the *Send on Behalf Of* permission for a mailbox. The difference in terms of functionality between the *SendAs* and *Send on Behalf Of* permissions is the degree of impersonation implied. When a user sends a message on behalf of another person, the message is marked as such and you know that someone else has taken responsibility for composing the message. The *Send On Behalf Of* permission is intended to cover scenarios such as when an assistant processes emails on behalf of an executive. You know that the executive did not personally send the message (because that fact is clear in the message header), but the message has still come from their mailbox. In the world of letter-writing, using the *Send on Behalf Of* permission to send a message is the equivalent of signing a letter for someone and adding "pp" (per pro) beside your signature.

You can use the *Set-Mailbox* cmdlet to grant the *Send on Behalf Of* permission to a shared mailbox, just like you can grant the permission to send messages on behalf of distribution lists or dynamic distribution lists with the *Set-DistributionGroup* and *Set-DynamicDistributionGroup*, or indeed, for a Microsoft 365 Group using the *Set-UnifiedGroup* cmdlet. The same syntax is used in all cases. For instance, to grant the permission for the Customer Services shared mailbox to Jill Smith:

```
Set-Mailbox -Identity "Customer Services" -GrantSendOnBehalfTo "Jill Smith"
```

The command above overwrites any existing permission. To add someone to the list of those allowed to send on behalf of a mailbox, use this format to add the user.

```
Set-Mailbox -Identity "Customer Services" -GrantSendOnBehalfTo @{Add="Terry.Hegarty"}
```

You can pass a comma-separated list of user accounts to grant permission at the same time, as in this example:

```
Set-Mailbox -Identity "Customer Services" -GrantSendOnBehalfTo @{Add="Ken.Bowers","James.Ryan"}
```

To view the accounts that hold *Send on Behalf Of* permission to mailboxes, you can run this command:

```
Get-ExoMailbox -RecipientTypeDetails SharedMailbox -Properties GrantSendOnBehalfTo | Where-Object {$_._.GrantSendOnBehalfTo -notlike ""} | Format-Table Name, GrantSendOnBehalfTo
```

Even if you grant an account the *FullAccess* and *Send on Behalf Of* permissions to a mailbox, this is different from giving the account the *Send As* permission. *Send As* is a different permission to assign users the ability to send messages as if the sender is the mailbox owner. If a user has both the *Send As* and *Send on Behalf Of* permissions for a mailbox, the client applies the *Send As* permission when they send a message.

Remember to change the behavior for Sent Items storage as described earlier if you want to keep copies of messages sent using the *Send As* or *Send on Behalf Of* permissions in the mailbox.

Mailbox Automapping

When a user receives full access permission for a mailbox (shared mailbox or another user's mailbox), Exchange Online tags the mailbox for inclusion in the set of "alternate" (secondary) mailboxes returned by the Autodiscover service when Outlook desktop clients query Autodiscover for details of available services. The Autodiscover service returns details of alternate mailboxes in the XML manifest sent to an Outlook client. Because secondary mailboxes are part of its resource set, Outlook automatically opens these mailboxes along with the user's primary mailbox. Automapping occurs every time the Autodiscover component refreshes information for Outlook, so it will occur shortly after Outlook starts and every 60-90 minutes thereafter. After Outlook refreshes its set of resources, any newly-added secondary mailbox appears in the set of resources just like any other mailbox.

An example of the XML from an Autodiscover manifest to define a shared mailbox as a resource is below.

```
<AlternativeMailbox>
  <Type>Delegate</Type>
  <DisplayName>Editing Team</DisplayName>
  <SmtpAddress>EditingTeam@Office365ITPros.com</SmtpAddress>
  <OwnerSmtpAddress>EditingTeam@Office365ITPros.com</OwnerSmtpAddress>
</AlternativeMailbox>
```

Including a shared mailbox in the Autodiscover manifest means that the Outlook desktop client opens the mailbox no matter what workstation the user uses to run Outlook. Although automapping usually is convenient, you might not always want to automap a shared mailbox for all users. One reason is that Outlook includes content for automapped mailboxes in the OST file for the primary mailbox. Usually, this isn't a problem as the OST can cope with the performance demands of user access and synchronization to contents for both the primary and secondary (automapped) mailboxes. However, if Outlook must open several very large secondary mailboxes, the size of the OST can grow to a point where the workstation's local drive begins to suffer performance problems. To solve the problem, you can remove automapping for one or more secondary mailboxes and add the mailboxes back to the Outlook profile.

To remove automapping for a secondary mailbox, you first remove the *FullAccess* permission for the mailbox from the user's account and then grant it again, this time specifying that auto-mapping should not occur. No options are available to control automapping in the administrative portals, so it must be done through PowerShell. After re-adding full access permission to the mailbox, you can add the mailbox to the Outlook profile (use File/Account Settings). After adding the mailbox to the profile, Outlook will open it like any other

resource. The offline data for a secondary mailbox added in this manner uses separate OST (mailbox contents) and NST (Outlook group contents) files.

Another way of handling the issue is to use the *Remove-MailboxPermission* cmdlet. For example, this command removes all automapping for the shared mailbox passed in the identity parameter. After running the command, users who have Full Access to the shared mailbox will continue to have access but automapping does not happen.

Remove-MailboxPermission -Identity 'Customer Services' -ClearAutoMapping

You can clear the complete set of mailbox permissions from a mailbox by running *Remove-MailboxPermission* with the *ResetDefault* switch. This instructs Exchange to reset the mailbox back to its default state by removing all delegated permissions. The *Send As* and *Send on Behalf Of* permissions are unaffected.

Remove-MailboxPermission -Identity 'Customer Services' -ResetDefault

You cannot simply flip the automapping switch from *\$True* to *\$False* once a set of permissions exist. If you make a mistake, you must remove the permissions and then add them back to the mailbox, making sure that the correct automapping choice is in place this time. In this example, we use the *Remove-MailboxPermission* cmdlet to remove the permission from the mailbox and then the *Add-MailboxPermission* cmdlet to add the permission back again:

```
Remove-MailboxPermission -Identity "Shared Mailbox" -User "UserWithAccess" -AccessRights FullAccess  
Add-MailboxPermission -Identity "Shared Mailbox" -User "UserWithAccess" -AccessRights FullAccess  
-AutoMapping:$False
```

The next time Outlook refreshes its list of resources from Autodiscover, it will remove the shared mailbox. Alternatively, you can close and re-open Outlook to accelerate the process.

Delegated Folder-Level Permissions

Outlook and OWA support folder-level permissions to allow delegates access to specific folders in a mailbox. This is an older form of delegate access that has existed in Outlook for almost 20 years to support the classic manager-assistant scenario where the manager delegates access over their inbox and calendar to the secretary to allow that user to process inbound emails. You can find more information about how to use folder-level delegation in this [support article](#).

Folder-level permissions are set with the *Set-MailboxFolderPermission* cmdlet and retrieved with *Get-MailboxFolderPermission* (or *Get-ExoMailboxFolderPermission*). As an example of their use, [this script](#) generates a report of all folder-level delegated permissions in a tenant. As with mailbox permissions, it is wise to conduct periodic reviews of folder-level permissions to ensure that people don't hold permissions that they no longer need.

Accessing Shared Mailboxes

Once created, users can access the new shared mailbox through Outlook or OWA. If a user has *FullAccess* permission for a mailbox and auto-mapping was left enabled (which is the default), they do not have to do anything specific as an auto-mapping process kicks in to inform Outlook to include the shared mailbox in the list of resources that it opens. For more information on opening and using shared mailboxes in Outlook, see [this support article](#).

You can override disabled Automapping for Classic Outlook by including the shared mailbox in an Outlook profile. This is an explicit instruction to open the mailbox for every Outlook session and is the older method used to access a shared mailbox. In this case, you click **More Settings** when editing the profile, go to the

Advanced tab, and click **Add** to enter the names of the shared mailboxes that you want Outlook to open. You can use the SMTP address, alias, or display name to tell Exchange which shared mailbox to use.

If you use Outlook in cached Exchange mode, Outlook depends on the OAB to check unknown addresses (except when using SMTP addresses). The new shared mailbox will not be present in the OAB until after Exchange Online has updated the OAB files and distributed them to clients. This process can take 24 hours or more, so if you want to send messages as the shared mailbox in the interim, use the online Global Address List (which has the shared mailbox because the mailbox joins the address list once after its creation) to lookup the name that you enter in the "From:" field. If you do not do this, Exchange Online cannot deliver the messages because the address you enter does not include the necessary information to allow Exchange to check it against its address lists, and you will receive a non-delivery notification containing the following error:

This message could not be sent. Try sending the message again later, or contact your network administrator. Error is [0x80070005-00000000-00000000].

Opening Shared Mailboxes in OWA

Although OWA does not use Autodiscover or have a profile, the client can also open and use shared mailboxes. To access a shared mailbox, expand the full set of folders in your mailbox and right-click **Folders** in the list of OWA resources, and select the "**Add shared folder**" option from the menu. Then input all or part of the name of the shared mailbox to search for it in email contacts and the directory (Figure 5-7). OWA validates that you have the correct permissions and if all is in order, will open the mailbox and display it in the folder list. This operation will not affect the set of resources shown in Outlook, just like auto-mapping does not influence the set of folders available to OWA. The clients function independently of each other.

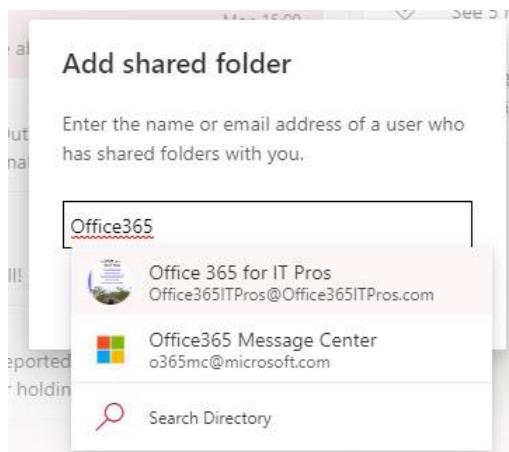


Figure 5-7: Choosing a shared mailbox to open with OWA

A good way of gaining access to a shared mailbox that exposes all the functionality available to the mailbox owner is to click the mailbox icon in the top right-hand corner of the menu bar and then **Open another mailbox**. This method opens another session with the shared mailbox. Once a shared mailbox is open, you can access its contents in the same way as any other mailbox. You can send messages as if they came from the mailbox if you have the *SendAs* permission. You can select the mailbox to use by inputting the name of the shared mailbox into the "From:" field of the message so that the message comes from the shared mailbox rather than you.

The same technique works to open individual folders assigned to delegate users with folder-level permissions.

Logging on to a shared mailbox: The usual course of events is to grant access to a shared mailbox and have users open the shared mailbox as an added resource in either Outlook or OWA. However, at the time of writing, it is possible to change the password for the account for the shared mailbox and log on to the mailbox directly, without going anywhere near a user's account. Using this method is frowned upon for

several reasons. First, it depends on password sharing, which is never a good thing, and second, according to Microsoft's Terms and Conditions, once you perform a direct logon to an account, you need to license that access because the mailbox is considered as no longer shared.

Converting a Shared Mailbox to a Regular Mailbox

The EAC includes a method to convert a shared mailbox to a regular mailbox (and vice versa). Once the conversion is complete, you must assign a license and reset the password. The license is necessary to allow the newly regularized mailbox to have full functionality while the reset password allows the person who takes ownership of the mailbox to access it. Shared mailboxes have user accounts that no one logs into (unless they assign a license to the account), so they do not need a password. Instead, access to the shared mailbox is gained by giving permissions to the users who need to access the mailbox.

When the EAC converts a shared mailbox to a regular mailbox or vice versa, it doesn't assign or remove licenses, nor can the EAC convert multiple mailboxes at one time. If you want to script the entire process, including the granting or removal of a license, you need to run some PowerShell commands. Here's how to convert a regular mailbox to a shared mailbox:

```
Set-Mailbox -Identity "Shared@Office365ITPros.com" -Type Shared
```

If you want to convert a shared mailbox to a regular mailbox:

```
Set-Mailbox -Identity "Shared@domain.com" -Type Regular
```

After converting a mailbox to be a shared mailbox, you should remove any licenses it has. When you convert a shared mailbox to be a regular mailbox, you need to assign an Exchange Online license (either individually or part of a product like Office 365 E3). The commands to assign and remove licenses are covered in the PowerShell chapter.

Redirecting Mail Sent to a Shared Mailbox

Companies often use shared mailboxes as the basis for customer communication. Things are a little more complicated when you have different teams of customer support agents, each using a shared mailbox, but you still want to have all communications recorded in a central mailbox for compliance or other purposes, such as integration with a CRM system that archives and categorizes customer interactions. You can achieve the goal by using a couple of mailbox properties.

Our scenario is as follows: our customer services team handles many different products. We want each product to have its own identity when email links are published on web pages and in other communications, so we create a set of shared mailboxes, one for each product, like this:

- Diapers.
- Cosmetics.
- Cars.

In addition, we have a central Customer Services shared mailbox.

Taking care of outbound emails is simple. The customer service agents simply make sure that they are sending messages as the Customer Services mailbox and that Outlook is configured to store the message in the shared mailbox rather than their personal mailboxes. The email address of the central mailbox will be stamped into the outbound message header so that any response from the customer will flow back into the central mailbox.

Two mailbox properties control the redirection of inbound email. The forwarding address is set to the central mailbox while the deliver and forward property is set to \$True to instruct Exchange Online to both forward a

copy of the message to the central mailbox and keep a copy in the brand mailbox. The address selected for the forwarding address must belong to a mail-enabled object belonging to the tenant, including other mailboxes, public folders, mail contacts, shared mailboxes, and distribution lists.

A case can be argued not to forward a copy of the message to the brand mailbox (by setting the *DeliverToMailboxAndForward* flag to *\$False*) but this means that someone must process all the new mail arriving at the central mailbox and forward it on for attention. It is much better to have one copy captured centrally and another going direct to the people who must deal with the customer. In this scenario, the central copy acts as a customer contact record while the copy delivered to the "action" mailbox initiates the response.

Sending an acknowledgment from a shared mailbox: It is a common requirement to want to issue an acknowledgment for messages that arrive in a shared mailbox. For example, when people send an email to a customer services mailbox, it is good to have them receive a response saying that their email will be answered soon (or whatever is the right text). There is no obvious way to set up an auto-reply message for a shared mailbox, but it is easily done:

- Click your photo in the OWA menu bar.
- Select **Open another mailbox**.
- Enter the name of the shared mailbox and click OK.
- When OWA opens the shared mailbox, click **Options** (cogwheel) then all Outlook settings, and select **Mail**, then **Automatic replies**, and create the automatic reply.

Another way to connect is to include the email address of the shared mailbox in the URL for OWA. For example, <https://outlook.office.com/owa/bookcomments@office365ITPros.com/>. You can then go to Options as before. This procedure is the best approach if you want to use a text editor to format the content of an autoreply. Alternatively, if you are interested in basic text auto-replies, you can use the *Set-MailboxAutoReplyConfiguration* (explained earlier) to set internal and external auto-replies for shared mailboxes. The thing about auto-replies is that Exchange only sends a single response per correspondent. If you want responses for every email, you must use Outlook to create an Inbox rule that forces the server to create a reply to every message using a template.

Using Mobile Devices with Shared and Delegated Mailboxes

Shared mailboxes are a very convenient method for teams to access information on which they need to work together. Given the highly mobile nature of today's workforce, it is natural to assume that you can use shared mailboxes on smartphones or tablets, but this isn't the case. The Exchange ActiveSync protocol only supports access to personal mailboxes. Most mobile email clients bundled with Android and iOS phones use ActiveSync and are limited by the functions built into the ActiveSync protocol, which don't support shared mailboxes.

Current versions of Outlook Mobile (iOS and Android) use a different protocol called the Microsoft sync technology to connect clients to Exchange Online (and Outlook.com). The Microsoft sync technology includes [support for shared mailboxes](#) and [delegate access to user mailboxes](#) along with other advanced features that will never be supported by ActiveSync. These features are available when the target (shared or user) mailbox and the mailbox of the delegate user both use Exchange Online.

To have delegated access to another person's mailbox with Outlook Mobile, a user must be assigned:

- Full access permission to the delegated mailbox. This means that the delegated user has unrestricted access to all folders in the mailbox.
- Either *Send As* or *Send On Behalf Of* permission to send messages for the delegated mailbox.

No other mobile client uses the Microsoft sync technology, which means that if you want to access shared mailboxes using a mobile client in a robust and supported manner, use Outlook Mobile.

Mail Contacts and Mail Users

Exchange Online supports both mail contacts and mail users and includes the two object types in address lists (by default, All Contacts, the GAL, and the OAB), which makes the objects addressable by any Outlook client. Third-party clients can also access and use these objects with the appropriate code. The differences between the two objects are:

- A mail contact is a pointer to a user of an external email system.
- A mail user has an external email address but also has Microsoft 365 credentials and can sign in to access resources such as SharePoint Online or OneDrive for Business sites. Mail user objects are a relic of on-premises systems which only Exchange uses. Other applications such as Microsoft 365 Groups, Teams, SharePoint Online, Yammer, and Planner use Azure B2B Collaboration to enable guest access to their data.

Organizations often use mail contacts to provide users with a GAL (and OAB) entry that points to a known, valid email address. Often, mail contacts hold contact details for external business partners, such as a Public Relations agency. You can create a mail contact with the EAC or Microsoft 365 admin center by completing six fields:

- First Name: Optional.
- Last Name: Optional.
- Initials: Optional.
- Display Name: The name that appears in the GAL. It's a good idea to mark the object as being external to the company and to include a visual clue about which organization the contact belongs to.
- Alias: The alias must be unique, and it can't have any spaces.
- External email address: An SMTP address that is external to the tenant.

Remember that in a hybrid environment, management of mail contacts and mail users is on-premises with changes synchronized to Exchange Online.

Using PowerShell to Create Mail Contacts

The *New-MailContact* and *Set-MailContact* cmdlets are available to create and update mail contacts. In this example we first create a new mail contact, setting their preferred mail format to be HTML, and then run the *Set-MailContact* cmdlet to enforce moderation and to inform senders that moderation applies to any message sent to this address. Note that you cannot create a mail contact with an SMTP address already used by another mail-enabled object, including guest accounts.

```
New-MailContact -ExternalEmailAddress "Danny.Flowers@contoso.com" -LastName "Flowers"  
-DisplayName "Danny Flowers (Contoso)" -FirstName "Danny" -Name "Danny Flowers" -MessageBodyFormat  
HTML -Alias Danny.Flowers  
  
Set-MailContact -Identity Danny.Flowers -ModeratedBy "Kim Akers" -ModerationEnabled $True -MailTip  
"Message will be moderated before dispatch"
```

After creating a mail contact in Exchange Online, a synchronization process creates a contact object in Entra ID. The *Get-MgContact* cmdlet retrieves details about Entra ID contacts.

```
Get-MgContact -OrgContactId (Get-MailContact -Identity  
AlexW@o365maestro.onmicrosoft.com).ExternalDirectoryObjectId
```

You don't have to worry about the contact objects held in Entra ID. They exist for internal purposes and are not used for mail routing.

Some of the mail contact settings supported by Exchange on-premises, such as the ability to set the maximum message size, are unavailable in Exchange Online. Others, such as phone numbers and

organizational information, are updatable with the *Set-Contact* cmdlet. In this example, we use PowerShell to read a simple CSV containing a set of records and create mail contacts for each object found. You can see how the *New-MailContact* cmdlet first creates the new object before the code uses *Set-Contact* to update some extended properties.

```
$InputContacts = import-csv c:\temp\inputcontacts.csv
Write-Host $InputContacts.Count "contacts found"
ForEach ($Contact in $InputContacts) {
    $Alias = $Contact.First + "." + $Contact.Last
    # Real simple code to make sure that we have an alias
    If ($Alias -eq $Null) { $Alias = $Contact.Name.Split("")[0] + "." + $Contact.Name.Split("")[1] }
    If ((Get-Recipient -Identity $Contact.EmailAddress -ErrorAction SilentlyContinue) -eq $Null) {
        # Recipient is not known, so we can add them
        Write-Host "Adding contact" $Contact.EmailAddress
        New-MailContact -Name $Contact.Name -ExternalEmailAddress $Contact.EmailAddress -Alias $Alias
        -FirstName $Contact.First -LastName $Contact.Last
        # Update country and phone numbers
        Set-Contact -Identity $Alias -MobilePhone $Contact.MobilePhone -Phone $Contact.WorkPhone -
        CountryOrRegion $Contact.Country -Company $Contact.Company }
}
```

You can even add a photo to mail contacts. Outlook displays these photos when users view contacts in the GAL. Here's how to use the *Import-RecipientDataProperty* cmdlet to add a photo. For best results, size the JPG file at 150 x 150 pixels (or smaller).

```
Import-RecipientDataProperty -Identity "John Contoso" -FileData ([Byte[]]$([Get-Content -Path
"c:\temp\DefaultGuestPicture.jpg" -Encoding Byte -ReadCount 0])) -Picture
```

Creating Mail Users

Although you can create the new mail user object by running the *New-MailUser* cmdlet, the easiest way to create a mail user is with EAC (you can't create mail users through the Microsoft 365 admin center). You must assign a valid SMTP email address pointing to the user's mailbox on an external email system. Exchange doesn't check that the email address exists. The only validation is that the address is in the correct format.

Behind the scenes, Exchange Online creates a user object in Entra ID which appears in the Microsoft 365 admin center. However, the new user object must have a license before the account can access any services.

The *Set-MailUser* cmdlet updates mail user objects. For example:

```
Set-MailUser -Identity "David Pelton" -CustomAttribute10 "External Recipient"
```

Entra ID creates mail user objects when apps like Teams and Planner add guest accounts (you'll see a record for the *New-SyncMailUser* cmdlet in the audit log). These objects usually have a *RecipientTypeDetails* value of *GuestMailUser* rather than *MailUser* (some guest accounts have *MailUser* in this property). Exchange Online links the mail user objects to the guest accounts and removes the mail user object upon the deletion of the associated guest account.

Recipient Moderation

Moderation (or "message approval") means that a message must first be reviewed and approved by a nominated moderator before Exchange Online can deliver it to the addressee. Up to ten moderators can be assigned responsibility to control messages sent to the following recipient types:

- User Mailboxes.
- Shared Mailboxes.
- Distribution Lists.
- Dynamic Distribution Lists.

- Mail Contacts.
- Mail Users.
- Mail-enabled Public Folders.
- Group mailboxes.

Teams supports moderation for messages posted to channels by restricting the ability to post to certain members.

Moderation for individual recipients (mailboxes, mail contacts, or mail users) is intended to "protect" the recipients against inappropriate email, often because the recipients are sensitive in some way. For example, it's reasonably common to impose moderation on the mailboxes of senior executives so that an executive assistant or another moderator can review inbound messages before passing approved items to the executive. Moderation for distribution lists is often imposed to ensure that posts to very large distributions only appear when it is appropriate to share the content with so many people. In other words, you might not want to have everyone in the company be allowed to send messages to the 50,000-recipient "All Company" distribution list. In all cases, you can arrange for select users to bypass the requirement for moderation so that their messages are delivered to the recipient without going through the approval process.

A moderated recipient can have multiple moderators, in which case all the nominated moderators receive copies of messages for approval. No quorum must be available before a message can be delivered as a simple approval from a single moderator suffices. If a message is declined by a moderator, Exchange Online returns it to the original sender. Logically, a moderator can send a message to the recipient that they are moderating without gaining further approval as can the owner of a distribution list.

A message awaiting moderation is held in an arbitration mailbox (you have no control over which arbitration mailbox is used) and should be processed within two days. The process that expires messages waiting in the arbitration mailbox runs on a weekly workcycle, which means that senders will receive notification that moderation has not occurred any time between two and nine days after the original message is sent – a tenant administrator can do nothing to accelerate the approval process. It is also interesting to note that Exchange Online throttles the number of expired moderation notifications to [300 per hour](#), which means that in periods when heavy usage is made of message moderation, some senders might not receive notifications that their messages have expired while awaiting moderation.

To set up moderation for a distribution list, edit the object's properties in EAC and select Message approval in the settings (Figure 5-8). Here you can set the flag to enable moderation and input the names of the users to act as moderators. Notice that you also can input the names of distribution lists or users who will bypass moderation and select who receives notification if their messages are not approved.



Edit message approval

Specify if messages sent to this group need to be approved, and choose moderators to approve or reject messages.

Require moderator approval for messages sent to this group

Group moderators

Search for users to add

T Redmond X

Add senders who don't require message approval:

Search for users to add

B BoardMembers-convert X

Notify a sender if their message isn't approved:

- Only sender
 Only senders in your organization
 No notifications

Save changes

Figure 5-8: Editing the moderation settings for a distribution list

EAC does not display the message approval UI for mailboxes, groups, contacts, mail users, or public folders, so you must set up moderation for these objects using PowerShell. For example, this command enables moderation for a mailbox and sets up three moderators. We also select a distribution list whose members bypass moderation.

```
Set-Mailbox -Identity "CEO Mailbox" -ModerationEnabled $True -ModeratedBy "Steve Smith", "Bill Jones", "CEO Assistant" -BypassModerationFromSendersOrMembers "Executive Committee"
```

Similar properties to enable moderation can be set through the *Set-DistributionGroup*, *Set-DynamicDistributionGroup*, *Set-MailContact*, and *Set-MailUser* cmdlets. When an object is enabled for moderation, Exchange Online creates an automatic MailTip displayed to users to inform them that a message will be moderated and might be delayed when they address a message to the object.

Moderation for nested distribution lists: Distribution lists (but not dynamic distribution lists) support the *BypassNestedModerationEnabled* parameter. If set to *\$True*, any nested distribution lists that also need moderation are governed by the decision of the moderator of the distribution list to which a message is addressed. If a moderator approves a message, it will be delivered to the members of all the nested distribution lists too. The default value of the flag is *\$False*, meaning that delivery to each moderated distribution list must be approved, but in most cases, it's reasonable to set the flag to *\$True* and allow the first moderator to control approval.

Blocking Basic Authentication

Microsoft blocks email connection protocols from using basic authentication (username and password) when signing into Exchange Online. For this reason, authentication policies are no longer applicable, and this section now focuses exclusively on SMTP client connections.

SMTP AUTH Client Submissions

Many apps and SMTP-enabled devices like printers and scanners submit messages to Exchange Online using [SMTP AUTH client submission](#) (SMTP AUTH). These connections do not support modern authentication methods such as multi-factor authentication or certificate-based authentication, which means that any account using SMTP AUTH might become a target for password spray attacks.

If you don't need to use SMTP AUTH, you should disable these connections at either a tenant or mailbox level. To disable at the tenant level, run this command to update the Exchange transport configuration:

```
Set-TransportConfig -SmtpClientAuthenticationDisabled $True
```

If SMTP AUTH is enabled in the transport configuration, you can disable the feature selectively at the mailbox level. To find out what mailboxes are enabled, run the command:

```
Get-CasMailbox | Where-Object {$_._SmtpClientAuthenticationDisabled -eq $Null -or  
$_._SmtpClientAuthenticationDisabled -eq $False } | Format-Table DisplayName
```

To disable the feature, change the command to:

```
Get-CasMailbox | Where-Object {$_._SmtpClientAuthenticationDisabled -eq $Null -or  
$_._SmtpClientAuthenticationDisabled -eq $False } | Set-CasMailbox -SmtpClientAuthenticationDisabled  
$True
```

When a mailbox is blocked from SMTP AUTH, it cannot submit messages to Exchange Online with the PowerShell *Send-MailMessage* cmdlet. Many PowerShell scripts use *Send-MailMessage* to send emails for different purposes from welcoming new users to a tenant to reporting the results of a background job.

In April 2024, Microsoft announced the [deprecation of basic authentication for SMTP client connections to Exchange Online](#). The plan of record is to remove SMTP AUTH in September 2025. Before this happens, administrators can check the SMTP AUTH Clients report in the Exchange admin center to identify the usage of SMTP submission within the tenant. Microsoft will also publish message center notifications to tenants that continue to use SMTP AUTH to warn about the deprecation 30 days in advance. The alternatives are:

- For LOB applications and devices that cannot utilize Basic Authentication in combination with predominantly internal recipients, consider using the High Volume E-Mail (HVE) feature, described in Chapter 6. For LOB applications sending messages to external recipients, check if it can use Azure Communication Services for Email (ECS).
- For scripts and tools, use the Microsoft Graph API (including Microsoft Graph PowerShell SDK cmdlets), which likely requires [code changes](#). See the discussion in the PowerShell book.
- Update the [SMTP connection to use OAuth](#).

Updating apps is straightforward. Updating hardware devices to use modern authentication might not be as easy. For this reason, it's a good idea to contact vendors early to ask about their plans for an upgrade.

Chapter 6: Mail Flow

Michel de Rooij

This chapter focuses on mail flow and managing the features available in Exchange Online, Exchange Online Protection, and Microsoft Defender for Office 365 to ensure that messages transit securely and reliably from senders to recipients. Managing mail flow covers much more than providing the successful delivery of messages. It is also about keeping you safe from malware, targeted phishing attacks, spoofing, spam, and (accidental) data loss.

Administrators execute the tasks discussed here primarily through the [Exchange admin center](#) (EAC), the Microsoft 365 Defender portal, and PowerShell cmdlets. PowerShell usage is emphasized due to its efficiency and stability in updating settings and its resilience to changes compared to GUI-based tools. The chapter begins with a focus on configuring mail flow.

Configuring Mail Flow

Before Exchange Online can accept messages for a domain, the domain must be associated with a tenant. Microsoft's documentation details the process of adding domains to a tenant. Once a domain is added, the next step is to configure the domain's MX records to point to Exchange Online Protection (EOP). This ensures that other organizations know how to route email to the domain.

The wizard automatically returns the information to set up the necessary DNS records for your domain(s) when you add the domain(s) to the tenant. Only the MX and SPF records are initially relevant for mail flow purposes. Additional DNS records might be required when configuring extra protection features, like DKIM (explained later).

Real-world: If you do not add your custom domains to your tenant, Exchange Online only accepts messages for the tenant's default service domain, *tenantname.onmicrosoft.com*. This is not very useful if you want your tenant to process email for all your domains, but it allows you to set up a test tenant to verify certain features without registering a new domain.

IPV6 Support

To use IPv6 for mail flow, you must submit a support ticket to ask Microsoft to enable IPv6 for specific domains. Starting October 16, 2024, Microsoft will gradually enable IPv6 for all tenants for Accepted Domains which have their inbound mail (MX) pointing to Exchange Online. Organizations that have configured allow-lists with IPv4 addresses only must extend these with the IPv6 addresses. For organizations that wish to remain using IPv4-only for a longer time or need more time to accommodate [anonymous mail requirements for IPv6](#), Microsoft will publish more information regarding an IPv4-only opt-out option for accepted domains in September 2024.

Mail Exchanger (MX)

When you configure your domain to use EOP, the MX record for that domain points to a hostname as *domain-tld.mail.protection.outlook.com* rather than an IP address. The following example illustrates how to resolve an MX record for a domain configured in EOP:

```
Resolve-DnsName office365itpros.com -Type MX
```

Name	Type	TTL	Section	NameExchange	Preference
---	---	---	-----	-----	-----

office365itpros.com MX 3572 Answer office365itpros-com.mail.protection.outlook.com 0

When a sending server queries the MX record for the domain office365itpros.com, the A record *office365itpros-com.mail.protection.outlook.com* is returned. Next, the sending server will try to translate that hostname into an IP address, for which it needs to perform an extra DNS query. Before responding to the query, Microsoft's servers perform an internal lookup to check the region the tenant belongs to. Once the region is known, the service responds with the IP addresses of the EOP systems within the same region of the tenant.

Note: Microsoft started moving the hostname for MX records from <vanity domain-tld>.mail.protection.outlook.com to <vanity domain-tld>.<random string>.mx.microsoft. This is part of Microsoft moving workload endpoints to a single top-level domain, *microsoft*. The new hostname will support DNSSEC and SMTP DANE security measures on inbound SMTP traffic. The <random string> is needed to avoid DNSSEC limits by grouping hostnames using the standard <random string>.mx.microsoft to satisfy DNSSEC requests. More on SMTP DANE later in this chapter. The old hostname for organizations not requiring SMTP DANE with DNSSEC will keep functioning indefinitely.

Real-world: When you add a new domain to your tenant, you are asked to configure various DNS records, including the MX record for your domain. In a greenfield deployment, it is probably okay to configure the MX record to point to EOP. However, reconfiguring the MX record for an existing domain will break your mail flow.

Switching from your current solution to EOP should be done at a suitable moment. It strictly depends on your migration approach. Typically, you reconfigure your MX record once your pilot for Exchange Online is complete or wait until most of your users have been migrated to Exchange Online. The time for changing your MX record is when you have ensured your configuration is ready to accept messages from EOP for on-premises recipients. For more information, see [this Microsoft article](#).

Sharing SMTP Namespaces

Note: Microsoft was running a private preview program for native domain sharing for email. The feature has been on the roadmap since mid-2020 under Feature ID 67161. Unfortunately, the preview status is unknown at this moment, and the related feature has been removed from the published roadmap.

Many organizations use one or more unique SMTP domain names (for example, office365itpros.com). Those organizations sometimes need to share a common SMTP domain name across multiple environments to present a single domain name to the outside world.

Sharing an SMTP namespace with another tenant is impossible because you cannot register a domain name in multiple tenants. Because of this, it is technically impossible to share a common email domain without an elaborate scheme. Because address rewriting is impossible with Exchange Online, we will not discuss sharing an address namespace between multiple tenants. However, we will cover how to share a namespace across a tenant and one or more on-premises Exchange organizations.

Sharing a domain name across an on-premises organization and Microsoft 365 is more straightforward than sharing a namespace across multiple tenants. There are several ways to accomplish this:

- **Use a third-party or custom broker service** to "catch" all incoming emails and route those messages to the backend system hosting the recipient mailboxes. For the broker service to determine what host to direct a message to, you must synchronize the recipient information from all connected systems to a specific location where the broker service can access it; sometimes, this is a directory of the broker service itself. Mimecast is an example of such a service that is capable of handling routing

- for various backend systems. The downside of this approach is that it introduces another component in the mail flow process, increasing your solution's complexity and cost.
- **Reconfigure domains in Exchange from Authoritative to Internal Relay.** By default, verified domains in Office 365 are added as authoritative in Exchange Online. This means Exchange Online will accept and handle mail flow for the domain if a recipient exists in the tenant directory. Exchange Online generates a Non-Delivery Report (NDR) if a recipient's email address does not exist. When reconfiguring a domain as an Internal Relay domain, Exchange Online tries to deliver the message locally. The message can be forwarded to another mail system through a connector if no matching recipient is found. If no connector is found to match the address, Exchange performs an MX lookup to decide how to route the message.
 - **Setup routing domains** and configure each environment to forward messages to specific recipients using the configured forwarding address (based on the particular routing domain). This approach is used in a hybrid deployment.

It can be tricky to manage this solution with multiple environments: the first environment (Exchange Online) must forward messages to the second environment. The second environment forwards messages to the third, and so on. The last environment in which to receive messages must then reject unknown recipients. You will introduce a mail loop if you accept unknown recipients and forward the emails to any previous environments. Mail loops occur when messages go to recipients that do not exist in any environment.

Sender Policy Framework (SPF)

The Sender Policy Framework (SPF) record is part of the [SPF validation system](#), created to protect from the receipt of spoofed messages. The receiving server evaluates the purported sender's domain SPF record. The receiving email system will use the information on the SPF record to determine whether the email was received from a messaging system authorized to send emails from that domain.

When a message is received from an external system, the receiving system examines the IP address of the prior server in the mail flow chain. It then looks for an SPF record for the sender's domain. Then, one of two things can happen:

1. If an SPF record is found, the IP address is verified against the values specified in the SPF record. Depending on how the record is configured, this will either generate a neutral result or a "soft" or "hard failure."
2. If no record is found, the SPF lookup is considered a "soft failure."

The suggested SPF record for Exchange Online looks like the example below. The record specifies that only the servers specified in the SPF record for *spf.protection.outlook.com* can send messages on behalf of this domain:

```
v=spf1 include:spf.protection.outlook.com -all
```

If another server not listed on the SPF record for *spf.protection.outlook.com* tries to send messages for this domain, a hard failure should be generated because the "-all" parameter is specified.

The syntax of the SPF record controls how the receiving system should treat a failure:

- **-all.** The minus sign shows that any SPF failure should be considered a hard failure. Whether the hard failure results in the message being rejected depends on how it is configured in the receiving server's anti-spam solution.
- **~all.** The tilde shows that any SPF failure should be treated as a soft fail; the message will be accepted unless the receiving system rejects soft fails.

- **?all.** The question mark indicates that the domain owner is neutral towards using SPF records. A failure will not generate a soft or hard failure. Instead, it will generate a neutral result. The message should be accepted regardless of the outcome.

If EOP is the only system that will send messages for your domain(s), the suggested SPF record will suffice. However, if other systems also send emails for your domain(s), you must manually tweak the suggested SPF record to include those systems. For instance, if a marketing platform sends an email from an address belonging to one of your custom domains, the SPF record should be modified to include that system. In the example below, we add the required entry for the marketing platform to our SPF record, which is *include:servers.office365itpros.org*:

```
v=spf1 include:spf.protection.outlook.com include:servers.office365itpros.org -all
```

When an on-premises organization uses EOP to protect outbound email, you should include the public IP address for the on-premises Exchange server in the SPF record. In this example, 1.2.3.4 is the public IP of the on-premises Exchange Server(s) that are sending emails to EOP:

```
v=spf1 include:spf.protection.outlook.com ip4:1.2.3.4 -all
```

Note: Like the examples above, some SPF records use the *include* statement to point to another SPF record. This tells the recipient to trust everything in your SPF record and everything in the SPF record identified by the *include* statement. The challenge is that this SPF record might also contain an *include* statement(s), which in turn points to additional SPF record(s), which might also contain another layer of *include* statements. This has the potential to cascade into many SPF records. Every time a hostname or pointer to another record is added to an SPF record (such as the *include* statement), a new DNS lookup is triggered to try and resolve the hostname to an IP address. The total number of lookups must not exceed ten, as this will cause the SPF check to fail. Therefore, when you add an *include* statement, reviewing what the target SPF record permits on your domain's behalf is prudent. It is also worth noting that the SPF record behind the *include* statement can change anytime. A single SPF record is also limited to 255 characters.

Creating and updating SPF records is not trivial, mainly because most email administrators do not need to do it often. However, various tools on the internet can help. For instance, [this site](#) generates the SPF record to configure in your external DNS and can help you check that you do not exceed the maximum of ten DNS lookups.

Real-world: Although not all organizations check for a sender's SPF records, it is essential to configure the records for the domain to reduce the risk of encountering email delivery issues elsewhere. Organizations do not always know what other mail systems send messages on behalf of their domain. For instance, a company's marketing department might periodically send messages through a third-party solution. In such cases, you should change your domain's SPF record to include the third-party solution.

If you cannot obtain that information, the best practice is to use a different domain for the marketing department, such as `marketing.office365itpros.com`. Ensure the namespace uses a different public IP address and SPF record than your corporate main SMTP namespace. That way, if the domain `marketing.office365itpros.com` (or the underlying public IP) gets blocked, it will not affect email delivery for the main corporate namespace.

Adding SPF records for all your internet domains, even those that do not send mail, is recommended. Bad actors will use your domain regardless of whether you do. For domains that do not send mail, you can protect them with an SPF record that hard fails all senders. For example, "`v=spf1 -all`".

While SPF records have long been a critical component of email security, they are no longer the only DNS records you must implement to maintain a modern email system.

Domain Keys Identified Mail (DKIM)

Domain Keys Identified Mail (DKIM) allows an organization to add a cryptographic signature to outgoing emails. Based on the message's headers and body, this signature is added in a DKIM-specific header called *DKIM-Signature*. The purpose of DKIM-signing a message is to allow a remote organization to verify whether the message originated from a platform authorized to send messages from a given domain. A DKIM signature does not encrypt the message body's contents or any attachments. DKIM should be a part of the baseline configuration for your email message flow.

Figure 6-1 illustrates how DKIM works: The sending server signs the message with a DKIM signature (1). The DKIM signature contains both a selector name and domain name (2), which the receiving server uses to perform a DNS lookup against the sender's DNS zone (3). The returned DNS record contains the matching public key (4), which the receiving server uses to match the DKIM header in the email. The receiving server adds the DKIM result (pass or fail) to the message header (5). The message is then queued for delivery (6). DKIM confirms the email's origin and that no one has tampered with the message during transit.

DKIM supports multiple keys per domain. This is useful in situations where an organization operates numerous email platforms, wants to delegate control of DKIM signatures to individual departments within the organization, uses a third-party service to send messages on behalf of one of the organization's domains, or when administrators want to update one of the keys without affecting current mail flow. A "selector" is prepended to the domain name and recorded as part of the DKIM-Signature header to support multiple keys. For instance: "selector._domainkey.domain.com." With the selectors in place, each system (or third-party solution) can use a different selector and still generate valid DKIM signatures.

By default, Exchange Online verifies incoming DKIM signatures and signs outbound messages – even when you have not configured DKIM records. Exchange Online uses the "selector1" and "selector2" selectors.

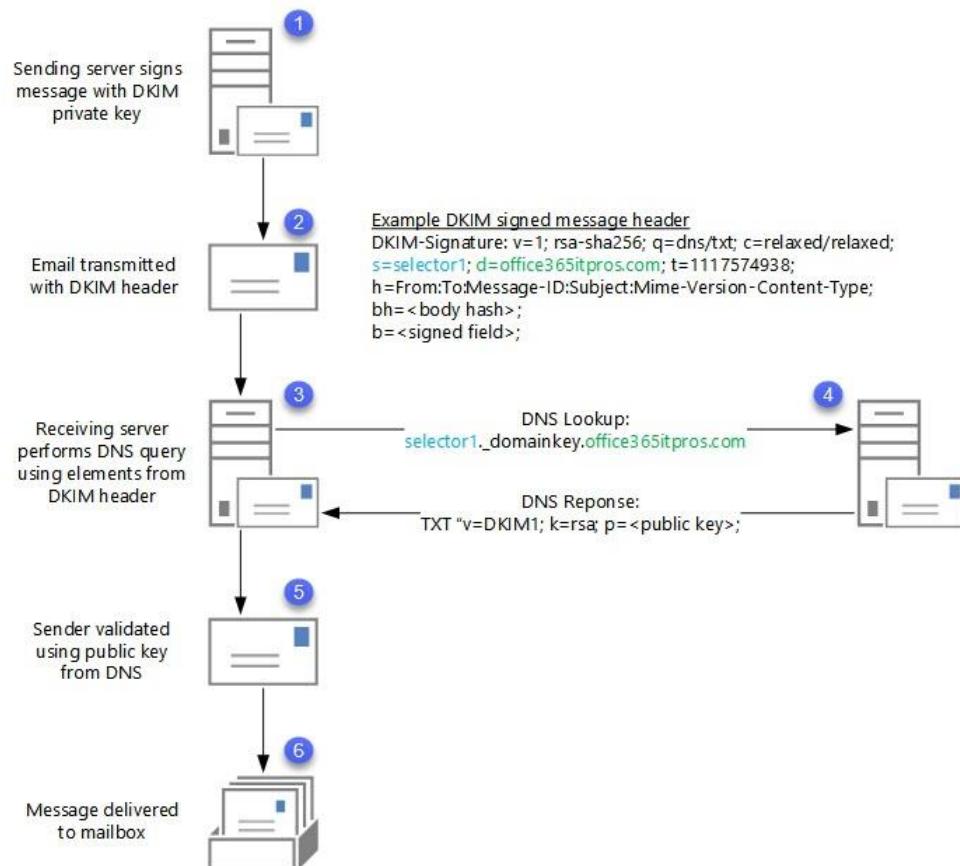


Figure 6-1: How EOP performs a DKIM lookup on incoming mail

DKIM Verification

After an inbound message is processed, the result of the DKIM verification process is written to the *Authentication-Results* header of the message. Depending on the outcome of the test, the header will show either *dkim=pass*, *dkim=none*, or *dkim=fail*, followed by a more human-readable explanation of the result in parentheses. For instance, the following *Authentication-Results* header reveals that the sender did not sign the outgoing message:

```
authentication-results: office365itpros.com; dkim=none (message not signed) header.d=None;
```

However, if the message was signed and the DKIM signature is successfully verified, the header will look similar to this:

```
authentication-results: office365itpros.com; dkim=pass (signature was verified)  
header.d=office365itpros.com;
```

Configuring DKIM Signing

Typically, several steps are necessary to enable the signing of outbound messages. However, as described below, you do not necessarily have to perform these steps if you only use Exchange Online as a mail service. This is because Microsoft enables DKIM signing by default and uses a clever workaround to ensure that signatures are valid.

Suppose you manually configure DKIM for your domain to associate signatures with vanity domains assigned to the tenant and not just the default service domain (*tenantname.onmicrosoft.com*). In that case, you must publish two DNS records for the vanity domain name you want to enable DKIM signing. Each record points to a specific target based on a combination of your domain and tenant name. For example, imagine you have a vanity domain called "office365itpros.com" and a tenant named "mycompany.onmicrosoft.com." The value of the CNAME records would then be the following:

```
selector1._domainkey.office365itpros.com CNAME  
selector1-office365itpros-com._domainkey.mycompany.onmicrosoft.com
```

and

```
selector2._domainkey.office365itpros.com CNAME  
selector2-office365itpros-com._domainkey.mycompany.onmicrosoft.com
```

The target of the CNAME record always starts with either *selector1* or *selector2*, followed by a hyphen and the domain MX key. The domain MX key is the first part of the MX record for your domain from the domains information page. The last part of the CNAME target is your tenant domain name. This is the default domain automatically created when you sign up for a Microsoft 365 tenant and is in the form of *<name>.onmicrosoft.com*. After publishing the DNS records, the easiest way to enable DKIM signing is through the Defender portal (security.microsoft.com) under **Policies & Rules > Threat Policies > Email Authentication Settings**. First, select the domain you want to enable DKIM and toggle the Sign messages for this domain with DKIM signatures slider to **Enabled**.

You can also enable DKIM when registering a domain name for your tenant. In the Microsoft 365 admin center, during the step where you are presented with DNS records to configure for the newly added domain, you will find an option to check **DomainKeys Identified Mail**. You can also toggle the switch on the Email authentication settings page, which shows an overview of domains and DomainKeys Identified mail status.

Alternatively, you can enable DKIM signing with PowerShell:

```
New-DkimSigningConfig -DomainName office365itpros.com -Enabled $true
```

Domain	Enabled
-----	-----

```
office365itpros.com      True
```

If the CNAME records are unavailable or if the records were created incorrectly, the above command will emit the following warning:

```
WARNING: Config is created but cannot be enabled since CNAME records are not published. Please
enable this policy using Set-DkimSigningConfig once CNAME records are published.
```

If you have recently updated your DNS records and set the CNAME record, you might need to wait for DNS caches to update. After sufficient time has passed, you can attempt to enable the configuration again using the following command:

```
Set-DkimSigningConfig -Identity office365itpros.com -Enabled $true
```

If you continue receiving the warning message, compare the CNAME records you created with the values EOP expects. To retrieve the correct selector CNAME values, run the following command:

```
Get-DkimSigningConfig | fl *CNAME*
```

```
Selector1CNAME: selector1-office365itpros-com._domainkey.mycompany.onmicrosoft.com
Selector2CNAME: selector2-office365itpros-com._domainkey.mycompany.onmicrosoft.com
```

It can take up to one hour after you configure DKIM before the changes have successfully replicated to all EOP servers. Once the new DKIM settings are replicated, all messages are automatically signed as the vanity domain rather than the tenant domain. For example, the following output is from a test message sent to an external recipient when the source tenant has enabled DKIM signing. Note the *dkim=pass* reference:

```
Authentication-Results: spf=pass (sender IP is 1.2.3.4) smtp.mailfrom=office365itpros.com; dkim=pass
(signature was verified) header.d=office365itpros.com; dmarc=bestguesspass action=none
header.from=office365itpros.com; compauth=pass reason=109

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=office365itpros.com;
s=selector1; h=From:To:Date:Subject:Message-ID:Content-Type:MIME-Version;
bh=WeG072W2hUk4jdiG4YKREVBP5fA4PaMBqox2yZKnVYI=;

b=mSTzijcUsZiaJizFSwmWOEpaNYBjUFXDoFQNaAgFwpbDhCcun5P5W+MYPxRRx5//KAnWT8hsV559VEU/E6PCENAQbRUnJ/Cgb
QRcoh6+X5+vtdsdXenC7gncoTOXWDak1sqh46mzW3Ls1vGVH4xdzFV6i7spZRoMif2cd/qtmU=
```

Along with the signature (shown prepended by *b=*), the DKIM header includes additional information, represented as tags used during the DKIM verification process. For instance, it indicates which selector was used (*s=selector1*) and a list of headers used during the signing process (*h=*). Trying to decipher the headers can be highly tedious and is usually unnecessary. To learn more about the details of the DKIM header and its various tags, read [RFC6367](#).

Default DKIM Signing

DKIM is a vital tool for fighting spoofed messages. As such, Microsoft automatically signs all outbound email traffic, even when the customer has not set up DKIM or configured any specific DKIM DNS records. You might wonder how Microsoft can do that, especially because they do not control the DNS zone for your domains. Microsoft controls one DNS zone directly linked to your tenant: the default tenant service domain *<tenantname>.onmicrosoft.com*. This allows them to create a DKIM signature based on the tenant domain and correctly represent your organization. The following example shows a *regular* DKIM signature, as you would expect when you have configured DKIM and the appropriate DNS records:

```
From: sender@office365itpros.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=office365itpros.com; s=selector1;
h=From:To:Date:Subject:Message-ID:Content-Type:MIME-Version;
bh=<body hash>;
b=<signed field>;
```

Look at the following example of a DKIM signature when you have not explicitly configured DKIM. Notice the selector (*s*=) and domain (*d*=) fields:

```
From: sender@office365itpros.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=o365itpros.onmicrosoft.com; s=selector1-o365itpros-com;
h=From:To:Subject:Message-ID:Content-Type:MIME-Version;
bh=<body hash>;
b=<signed field>;
```

Based on the above information, you can reconstruct the DNS records referenced to the following value:
selector1-o365itpros-com._domainkey.o365itpros.onmicrosoft.com.

Using the *Resolve-DnsName* cmdlet, you can then verify that the record exists:

```
Resolve-DnsName selector1-o365itpros-com._domainkey.mycompany.onmicrosoft.com -Type TXT

v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCkHq3ztGIm1R8a1D+7oZiaG5mTUtF01pKRBZCPFG4sugV1EFF5F6Jpwb
JDzZmyI1qYfTgUkmY0vbHsoYvW7rddLKVTTh+vE1S5P9coIHrw759hXbpPDSQ9JNP8aN+Bfrg6YMEWnOGA+PL+ZpyvswcB0jz9M6
yMvowOxChv5QIDAQAB; n=1024,1435867504,1
```

The target system uses the key returned by the record to verify the DKIM signature and does not differ from the record otherwise used when manually configuring DKIM. After all, when setting up explicit DKIM signing for Exchange Online, you do not create a TXT record with the key; you create a CNAME record pointing to the same TXT record in Microsoft's DNS zone for your tenant illustrated in the example.

DKIM Key Rotation

Microsoft uses two different keys for DKIM signing. As mentioned earlier, several reasons exist for using two keys, the most important one being that it allows Microsoft (or the tenant admin) to rotate the keys without affecting the DKIM verification process.

Here's how this works: messages are signed using one of the two selector keys at any given time—for instance, *selector1*. When Microsoft or a tenant admin wants to update the key behind *selector1*, they do not just update it. If they were to do that, messages signed by the old key still in transit would be invalidated.

To overcome this problem, the tenant admin first rotates to the key value behind the second selector (*selector2*). Any new message sent by Exchange Online is signed with this new key. When remote systems process those messages, they query the key value for *selector2* instead of *selector1*. Messages still signed by the first selector key can be verified because the key value is publicly available in DNS. This process avoids invalidating messages that are still in transit and potential delays in DNS propagation when publishing new keys.

Run the following command to check the last time a DKIM key was rotated or its bit level.

```
Get-DkimSigningConfig | fl Domain, Selector1KeySize, Selector2KeySize, SelectorBeforeRotateOnDate,
RotateOnDate, SelectorAfterRotateOnDate

Domain : office365itpros.com
Selector1KeySize : 1024
Selector2KeySize : 1024
SelectorBeforeRotateOnDate : selector2
RotateOnDate : 11/5/2019 7:00:00 PM
SelectorAfterRotateOnDate : selector1
```

Our example above shows that the last key rotation was in 2019. The *SelectorAfterRotateOnDate* indicates which selector has been in use since the previous rotation. In our example, Exchange Online has been using *selector1* since 11/5/2019. We also see that both keys use a 1,024-bit key length. Let's upgrade that by

rotating our key. We can specify the following command using a key size of 2,048 bits (current maximum) to do this.

```
Rotate-DkimSigningConfig -Identity office365itpros.com -KeySize 2048
```

The command above does not provide an output, so let's reissue the `Get-DkimSigningConfig` command.

```
Get-DkimSigningConfig | fl Domain, Selector1KeySize, Selector2KeySize, SelectorBeforeRotateOnDate, RotateOnDate, SelectorAfterRotateOnDate
```

```
Domain : office365itpros.com
Selector1KeySize : 1024
Selector2KeySize : 2048
SelectorBeforeRotateOnDate : selector1
RotateOnDate : 10/3/2022 7:00:00 PM
SelectorAfterRotateOnDate : selector2
```

From the output, we can see that only one of the keys has been upgraded to 2,048 bits, and Exchange Online will rotate to that key on 10/3/2022 at 7:00 PM. Microsoft always sets the rotation four days in the future. This allows the new key to propagate in DNS before fully being put into production. After four days, Exchange Online will switch to selector2, which has a 2,048-bit key length.

Exchange Online will not allow you to rotate again until the `RotateOnDate` has been exceeded. This prevents an admin from accidentally rotating both keys simultaneously and potentially invalidating any messages in transit.

DKIM With Third-Party Email Filters

If you route outbound emails via a third-party filtering or email hygiene service, you should ensure that this service does not invalidate Microsoft's DKIM signature on outbound messages. Suppose the third-party service rewrites the email or adds new content to the message body. In that case, the DKIM signature will be invalid, and your recipients will see DKIM failure errors (probably just in the headers, but they might reject your email because it fails). Therefore, it is often essential to ensure that the last sending system is the system that applies the DKIM signing, remembering that this might not be EOP.

Domain-based Message Authentication, Reporting, and Conformance (DMARC)

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a method for authenticating messages that build upon SPF and DKIM. It proves particularly useful in preventing phishing attacks. This is when an attacker spoofs a legitimate domain to trick the recipients into visiting a malicious website and possibly revealing personal information such as passwords. Spoofing a message means that the spammer places a value in the RFC5322 *From* field that is not their domain and uses a value from another domain to pretend that the email is from that organization instead. The RFC5322 *From* header is the one that is shown in clients such as Outlook. Because of this, spoofed messages are hard to differentiate from legitimate emails for end-users.

DMARC specifies what action the receiving server should take if SPF or DKIM validation fails for an email received from your domain. Without DMARC informing the receiving system of the intent of the sending system (concerning quarantine or rejection), the receiver may still decide not to reject messages if either SPF or DKIM validation fails.

Similar to SPF and DKIM, DMARC requires a DNS TXT record that the receiving party can query. A typical DMARC record looks like the following:

```
v=DMARC1; p=reject; pct=50; rua=mailto:postmaster@office365itpros.com;
ruf=mailto:dmarcfailures@office365itpros.com; fo=1
```

- **V** specifies the DMARC protocol version.
- **P** recommends the action the receiving system should take if SPF and DKIM validation fail. Possible actions are:
 - **Reject**
 - **Quarantine**
 - **None** (monitor mode)
- **PCT** gives the percentage of messages subjected to the DMARC policy. The default is 100.
- **RUA** (*or reporting URI for aggregate reports*) contains the email address(es) to which aggregate reports should be sent.
- **RUF** (*or reporting URI for forensic reports*) contains the email address(es) to which forensic reports should be sent.
- **FO** (*or forensic options*) can have a value of 0 or 1. 0 is implied if the *fo* field is absent from the DNS record.
 - 1 = Send forensic reports when either DKIM or SPF fails.
 - 0 = Send forensic reports when both DKIM and SPF fail.
- **SP** (*for sub-domain policy*) is not shown in the above example. If this field is absent from the DNS record, all subdomains inherit the policy from the parent domain (defined with *p=*). If you want a policy different from the parent policy for all subdomains, include *sp=*. For example, if you know you have no subdomains, add *sp=reject*. This will automatically reject all subdomains as you do not send emails from them. If you have specific subdomains, add a DMARC record for that domain with its policy to override the parent policy.

Aggregate reports are sent daily from the recipient domain to the sender email address specified in the “*rua*” field. These reports contain information such as how many emails have been received and if these messages passed SPF and DKIM tests. Microsoft only sends aggregate reports to the sender if the recipient points their MX record directly to Exchange Online. For example, Microsoft will send an aggregate report to senders for emails sent to *office365itpros.com* because its MX record is *office365itpro-com.mail.protection.outlook.com*. Microsoft does not generate aggregate reports for domains where the MX record points somewhere else, such as a third-party message hygiene service in front of Exchange Online. In this instance, the third-party message hygiene service will be responsible for sending aggregate reports to the sender.

Forensic reports are better known as failure reports and are sent to the recipients specified in the “*ruf*” field each time DMARC fails. These reports are handy for figuring out why messages fail DMARC processing. Note that most large email providers, such as Exchange Online, Gmail, and Yahoo, do not send forensic reports, regardless of whether you request them in your DMARC record. The reason is that forensic reports might contain Person Identifiable Information (PII), creating a potential privacy issue.

How DMARC Works

The following steps outline how DMARC processes a message:

1. A user receives a message. For example, from *emails@office365itpros.com*.
2. The receiving server will verify if *office365itpros.com* has a DMARC policy (DNS record).
3. Does the message pass SPF/DKIM validation?
 - a. For SPF, does the header of the RFC5322 *From* field and the envelope sender (RFC5321 *MailFrom* or RFC5321 EHLO domain) match?
 - b. For DKIM, does the RFC5322 *From* match the DKIM signing domain (*d=header*).
4. If the SPF or DKIM alignment checks fail, the message fails DMARC processing, and the action specified in the DMARC policy is executed.

If we apply this logic to the DMARC example policy from above, this means that a spoofed message (which would fail SPF or DKIM) would be *rejected*, and a failure report would be sent to dmarcfailures@office365itpros.com:

```
v=DMARC1; p=reject; pct=50; rua=mailto:postmaster@office365itpros.com;
ruf=mailto:dmarcfailures@office365itpros.com; fo=1
```

If you create a DMARC record for your domain, it is best to configure DMARC in *monitor mode* first. This allows you to sift through the failure reports to understand better why any messages from your domain fail DMARC processing. DMARC processing does not always fail because a message is spoofed. Sometimes messages come from a legitimate server not included in the SPF record or do not do DKIM signing. The more messages your environment processes, the more failure reports you will receive. For large organizations, going through failure reports can be very time-consuming. Luckily, third-party services exist, which you can specify in the DMARC policy. These services will then process the failure reports for you and provide you with a summary of the failures and the reasons.

Real-world: If your domain is a target for many spoofed messages, which is often the case for more prominent and well-known organizations, enabling DMARC might decrease the amount of phishing and spoofed email messages your organization receives. However, if you are a smaller organization, the risk from spoofed emails is likely just as high, as many organizations are getting business compromise attack emails, and the end-users are responding and revealing passwords or transferring money, etc. Therefore, we recommend that each domain starts with a "none" policy; this allows time to monitor and remediate any legitimate mail failing DMARC. Once all legitimate messages have been remediated, these domains should be transitioned to a "quarantine" policy and, finally, a "reject."

DMARC Processing on Inbound Messages

Exchange Online performs DMARC processing on inbound messages if a DMARC policy exists for the sender's domain. Just like SPF and DKIM processing, the result of the DMARC test is written to the *Authentication-Results* header:

```
authentication-results: spf=pass (sender IP is 1.2.3.4) smtp.mailfrom=phishing.com; dkim=none
(message not signed) header.d=office365itpros.com; dmarc=fail action=quarantine
header.from=office365itpros.com; compauth=fail reason=000
```

In this example, the DMARC test failed because the alignment between the RFC5322 *From* address and the envelope sender did not match (phishing.com does not equal office365itpros.com). Therefore, the composite authentication result of SPF, DKIM, and DMARC together (the *comauth* value) shows a failure, and the reason code means the message failed explicit DMARC authentication.

If the SPF domain in the *mailfrom* header does not match the *From* header on a message entering Exchange Online, the message is marked as junk. This is because the *mailfrom* header could match a valid SPF record but be unrelated to the domain that appears in the client application (the *From* header). This scenario results in spoofed emails being marked as valid in terms of SPF. Therefore, EOP requires that the *mailfrom* and *from* header values match to stop EOP considering the message a spoofed email.

Because many organizations employ complex routing instead of just EOP (third-party vendors or on-premises routing, for example), Microsoft cannot always guarantee that a DMARC failure constitutes an actual failure. For this reason, Microsoft will not reject the message even when the DMARC policy is configured with a *reject* action. Instead, EOP will add the "action=reject" value to the *authentication-results* header (or "quarantine" as another lesser seen example), which mail flow rules can use to override the verdict for such messages. Most emails in this category are rejected before reaching the end user's mailbox, but messages can also be rescued from the spam filter by a mail flow rule or allow lists.

Configuring DMARC

DMARC looks easy to set up, and to an extent, it is – you just add a valid TXT record in public DNS, and the aggregate emails appear within 48 hours in the mailbox identified in the “rua” value of the TXT record. However, the processing of these aggregate emails is more complex. Several services on the internet, such as Dmarcian and DMarcAnalyzer, will take these aggregate emails and produce the analytics for you.

Once you have the analytics for your domain, you can tweak your SPF and DKIM configuration to ensure that all your legitimate senders are within scope. Spoofing senders would be outside the scope of your SPF or DKIM records – you would then increase your DMARC policy to *p=quarantine* and then eventually *p=reject*.

Getting there is the hard part. To help customers with this, Microsoft partners with Valimail to [offer Valimail Monitor](#) as a free service for Microsoft 365 customers to get started with DMARC. This will help you monitor your mail flow and help you work towards enforcing compliance.

MTA Strict Transport Security (MTA-STS)

MTA Strict Transport Security (MTA-STS) is a security technology developed by the Messaging, Malware, and Mobile Anti-Abuse Working Group (M3AAWG). MTA-STS combats the same problem as DANE: how to secure mail flow from man-in-the-middle and downgrade attacks? The main differences are that MTA-STS does not require DNSSEC and uses TXT records instead of TLSA records.

The benefit of MTA-STS is that it is easier to deploy. For example, if your external DNS provider does not support DNSSEC or TLSA records, you cannot use DANE. However, all DNS providers should support TXT records, the only DNS requirement for MTA-STS.

When checking MTA-STS, the sending server looks for a TXT record in the recipient domain with a value of *_mta-sts*. Using office365itpros.com as an example, the TXT record is *_mta-sts.office365itpros.com*. The example below illustrates what an MTA-STS TXT record might look like for the office365itpros.com domain.

```
_mta-sts.office365itpros.com. 3600 IN TXT v=STSp1; id=20240727000000Z;
```

v=STSp1 identifies the version of MTA-STS used by the recipient domain. In the example above, version 1 is the only supported version tag of MTA-STS. The **ID** value identifies the current version of the MTA-STS policy. If the ID value changes, the sender retrieves the latest policy from *https://mta-sts.<domain name>/well-known/mta-sts.txt*. If the ID value is the same, the sender uses a previously cached copy of the recipient's policy file. This helps eliminate unnecessary HTTPS requests to the server hosting the policy file.

Note: Each time you publish a new MTA-STS policy, you should update the ID published in DNS. This alerts senders that your policy has changed and that they need to retrieve a new policy file. An ID specifying a date and time format is recommended, but this ID could be whatever you desire.

One can argue that the lack of DNSSEC means that retrieving the TXT record could be subject to man-in-the-middle attacks. However, even if a bad actor changed the ID's value before returning it to the sender, it would merely instruct the sender to download a new policy file from a known location that the recipient owns. The best a bad actor could do is return that no MTA-STS TXT record exists.

The known location used by MTA-STS is always *https://mta-sts.<domain>/well-known/mta-sts.txt*. This path, file name, and file extension are mandatory for MTA-STS. In addition, the policy file is only retrieved over HTTPS. The webserver hosting the policy file must have a valid third-party certificate. Using office365itpros.com as an example, the certificate must contain a subject name (or subject alternate name) of *mta-sts.office365itpros.com*. Alternatively, a wildcard certificate could also be used.

The example below illustrates what the contents of this policy file could contain:

```
Version: STSp1
```

```
mode: enforce
mx: office365itpros-com.mail.protection.outlook.com
max_age: 604800
```

Version identifies the version of MTA-STS in use. In our example, this is version 1.

The mode has three possible values: "enforce," "testing," and "none."

- **Enforce** instructs a sender not to transmit messages to any host that fails certificate validation. Or if the host does not support STARTTLS or TLS 1.2 (and greater).
- **Testing** instructs a sender to transmit messages (including to hosts that fail certificate validation) and provide reports to the recipient of any failures. This mode helps administrators identify and remediate any misconfigured legitimate mail exchangers before enforcing the policy.
- **None** instructs the sender to transmit all messages and treat the recipient domain as if it had no MTA-STS policy.

MX defines all MX records served by this policy. This could be a single MX record, like in our example above, or multiple MX records, each entered onto a separate line. Wildcards are also permitted. In the example above, we define Office 365 as a valid MX record for office365itpros.com. MTA-STS requires that the hosts defined in the MX records support TLS 1.2 or greater.

Max age defines how long (in seconds) a sender should cache this policy. In our example above, 604,800 is 7 days in seconds. This instructs the sender to discard the policy file after 7 days.

Figure 6-2 illustrates how MTA-STS works when in enforce mode: the sending server queries the external DNS of the recipient domain for their MX records (1), which are returned (2). The sending server then queries the external DNS of the recipient domain to see if a _mta-sts TXT record exists (3). If the _mta-sts TXT record exists (4), the sender checks the ID to see if it has changed since the last time it retrieved the _mta-sts record (5). If the ID has changed, the sender performs an HTTPS request to retrieve the MTA-STS policy file from <https://mta-sts.office365itpros.com/.well-known/mta-sts.txt> (6). If the ID is the same, the sender uses a previously cached copy of the MTA-STS policy. With a policy of "Enforce," the sender then checks all MX records defined in the policy, starting with the lowest priority MX record first (7). If the host passes certificate validation, the mail is transmitted (8). If the host fails certificate validation, MTA-STS proceeds to the next MX record in the policy. Mail is not transmitted if all hosts fail certificate validation (9).

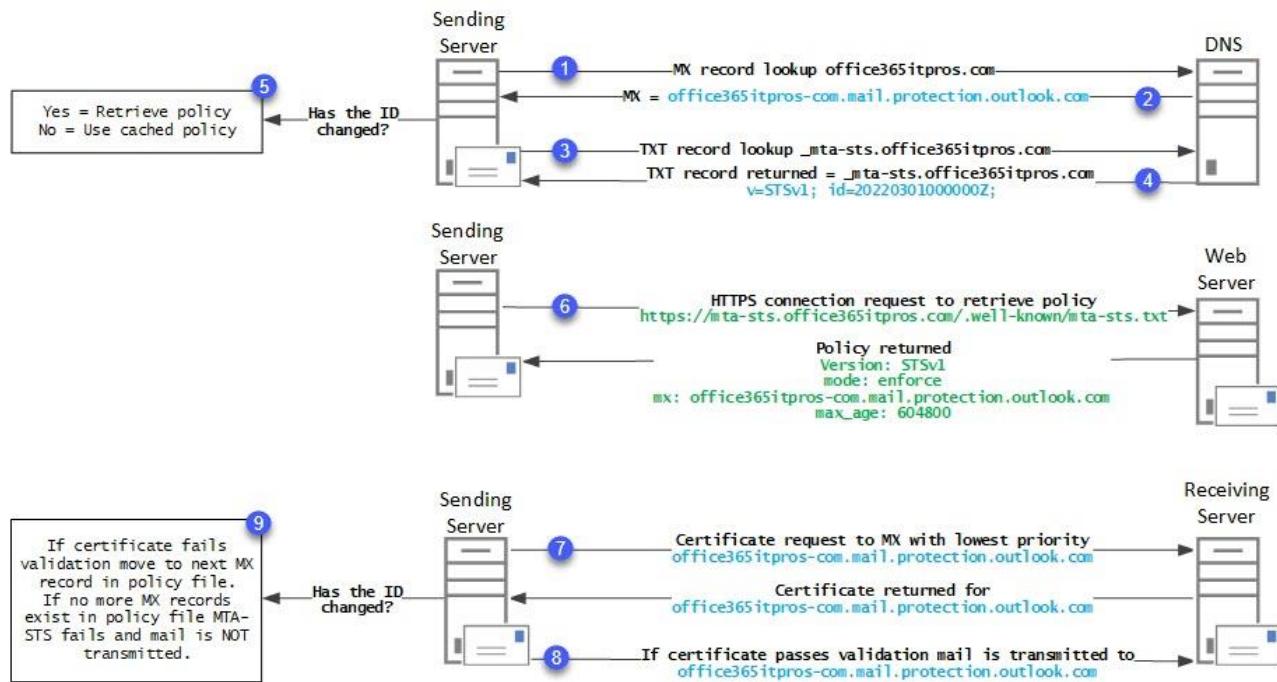


Figure 6-2: How MTA-STS prevents downgrade and man-in-the-middle attacks

SMTP DNS-based Authentication of Named Entities (SMTP-DANE)

When mail servers transfer mail, they first must agree on whether to use TLS to protect the connection and, if so, which version of TLS. During this initial handshake, these packets are unencrypted. The servers then upgrade the connection TLS after negotiating a common TLS protocol. Mail then transfers over this secure TLS connection.

The challenge is the initial unencrypted handshake. During this unencrypted state, packets are subject to man-in-the-middle and downgrade attacks. To answer this problem, the industry created a new standard called [DNS-based Authentication of Named Entities](#) (DANE).

DANE allows an organization to publish details of the TLS protocols it supports through a special DNS record in their external DNS. These DNS records are known as TLSA records. The example below illustrates what a TLSA record might look like for the `office365itpros.com` domain.

```
_25._tcp.office365itpros.com. IN TLSA 3 1 1
e1c362c8c03a15023fff83831a70d6fce33203d499a3f3d0b13243a1ac689088
```

TLSA records are not exclusive to mail flow. In the example above, the TLSA record exists for TCP 25, which is the port used by SMTP. Multiple TLSA records could exist in external DNS to serve several TCP ports. For example, an external web application that leverages HTTPS could publish TLSA records for TCP 443.

When a mail server supporting DANE wishes to send an email, it performs the steps illustrated in Figure 6-3: The sending server queries the external DNS of the recipient domain for their MX record (1), which is returned (2). The sending server then queries the external DNS of the recipient domain for a TLSA record for TCP 25 (3). If a TLSA record for TCP 25 exists, it is returned via DNSSEC (4). This returned record contains the certificate fingerprint. Next, the sending server initiates a TLS connection to the recipient server (5) using the previously retrieved MX record. The recipient server responds with its certificate fingerprint (6). Finally, the sending server matches the certificate fingerprint transmitted from the recipient server to the fingerprint received from the TLSA record (7). If the fingerprints match, the connection is established, and mail is sent (8). If the fingerprints do not match, the sending server drops the connection.

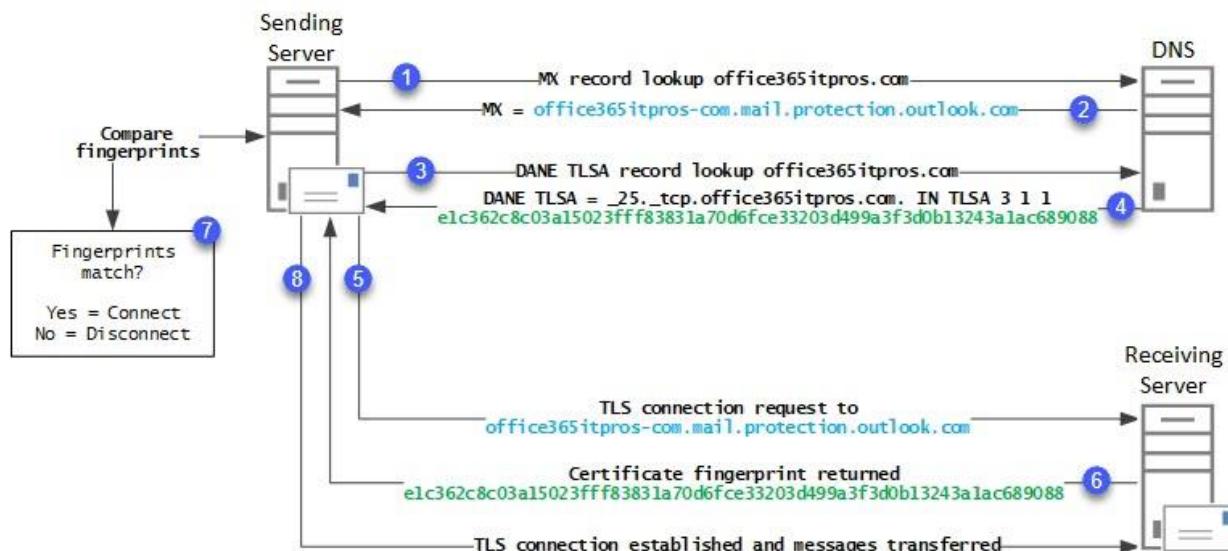


Figure 6-3: How DANE for SMTP prevents downgrade and man-in-the-middle attacks

Outbound support for SMTP DANE with DNSSEC is enabled in all tenants and does not require any tenant administrator action. You can see which receiving domains support which security mechanism in the EAC report Outbound Message in Transit Security report, tab Messages Sent. The report summarizes outbound MTA-STS, SMTP DANE with DNSSEC, SMTP DANE with DNSSEC + MTA-STS, or TLS-only usage over the selected period, as shown in Figure 6-3. On this page, you can also request a report containing more detailed information.

Outbound Message in Transit Security report

The graphs below show the volume of emails that were secured by SMTP DANE with DNSSEC, MTA-STS, TLS, or without TLS (using plain text). Microsoft will always attempt to use TLS when sending your email. [Learn more](#)

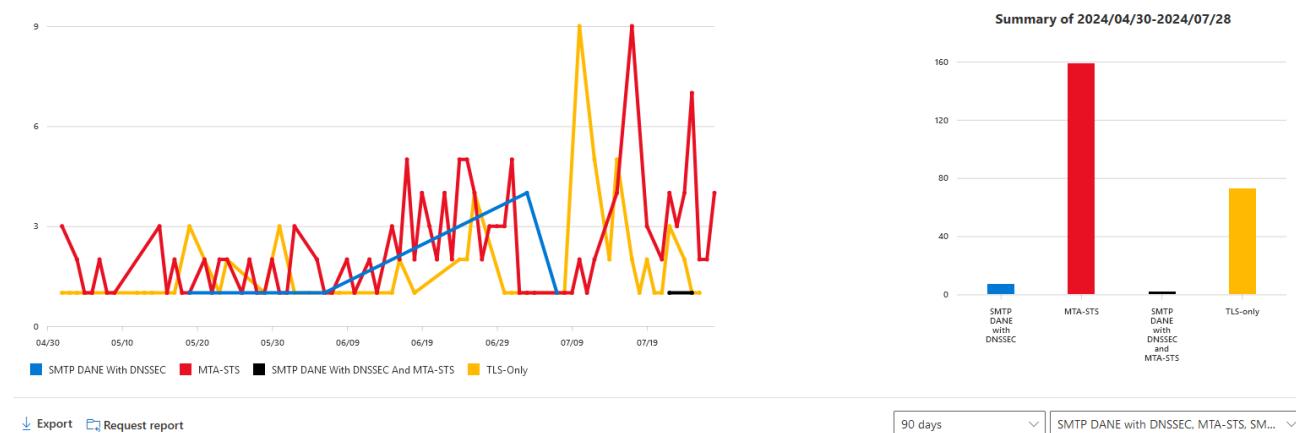


Figure 6-4: Outbound Message in Transit Security report

Inbound support for SMTP DANE with DNSSEC has been in Preview since mid-July. General Availability support has been delayed until October 2024. Setting up Inbound SMTP-DANE for a domain requires that your domain be secured by DNSSEC, offered by your provider or configured yourself. You can configure SMTP-DANE without DNSSEC, but that would not offer the protection of a DNSSEC-secured domain. Also, any smart host reference to Exchange Online will need to use `<tenant-tld>.mail.protection.outlook.com` as an

endpoint, not anything else that might have been configured from a historical perspective, e.g. mail.eo.outlook.com.

To configure inbound SMTP-DANE over DNSSEC, first, update the TTL of your MX record to the lowest value allowed by your provider. This is to minimize the waiting period between changes. After you waited for the previous TTL period for changes to propagate, first set the MTA-STS policy to *testing* when you are using MTA-STS. so changes we are going to make to accepting hosts are allowed. Also, do not forget to adjust the *id* value in the MTA-STS *_mta.sts.<domain>* policy record in DNS, to inform parties your policy file changed. Your policy file might look something like this:

```
version: STSv1
mode: testing
mx: office365itpros-com.m-v1.mx.microsoft
mx: office365itpros-com.mail.protection.outlook.com
max_age: 604800
```

Next, using the Exchange Online management module v3.5.1 or later, enable DNSSEC for your domain:

Enable-DnsSecForVerifiedDomain -DomainName office365itpros.com		
DnssecMxValue	Result	ErrorData
-----	-----	-----
office365itpros-com.m-v1.mx.microsoft	Success	

The DnsSecMxValue returned is the MX record you need to configure for domains you want to protect with SMTP-DANE, in this case, *office365itpros-com.m-v1.mx. Microsoft*. The value ends in mx.microsoft.com, which is part of Microsoft new endpoint structure for Microsoft 365-related services. In your ISP portal, configure this as an MX record with a priority higher than your current MX record, and set the TTL to a low value, e.g.

```
office365itpros.com. 300 IN MX office365itpros-com.m-v1.mx.microsoft 20
```

Next, you can verify the mx.microsoft inbound mail route is working using the Inbound SMTP test from the [Remote Connectivity Analyzer](#). When this is shown as successful, you increase the priority of the old MX record to anything higher than the mx.microsoft priority, e.g. 30. This is also the time to set the TTL value of mx.microsoft to the MX original value, e.g. 3600 seconds. Ultimately, you can remove the previous mail.protection.outlook.com MX record. When you are using MTA-STS, do not forget to remove the previous MX host from the MTA-STS policy file, set the policy back to enforce, and in DNS update the policy id tag to inform partners using MTA-STS of the change.

When these steps are completed, you can enable SMTP DANE for inbound messages for the domain:

Enable-SmtpDaneInbound -DomainName office365itpros.com		
Result	ErrorData	
-----	-----	-----
Success		

Finally, you can verify the TLSA record for your domain has propagated and everything has been set up correctly using the DNSSEC and DANE Validation Test from the [Remote Connectivity Analyzer](#):



Figure 6-5: DNSSEC and DANE Validation Test

Alternative sites to test your SMTP-DANE and DNSSEC setup can be found [here](#) and [here](#). Also, SMTP-DANE has some limitations, which you can read about [here](#).

Note: You can configure both MTA-STS and SMTP-DANE for your domains. This allows you to cover more senders who may only support one of the technologies. For example, Google and Yahoo currently support only MTA-STS, while other parties might support SMTP-DANE, which might then be the preferred authentication mechanism.

Currently, there is no report for inbound mail security, to complement the Outbound Message in Transit Security report in EAC.

Authenticated Receive Chain (ARC)

The challenge with methods used to authenticate outbound email is that they do not account for forwarding. Consider a scenario where microsoft.com sends a message to office365itpros.com, and a rule at office365itpros.com then forwards that message to contoso.com. When contoso.com queries the headers of the forwarded microsoft.com email, it will attribute the sender of the email as office365itpros.com. This will fail both SPF and DMARC because office365itpros.com is not a valid Microsoft sender.

Authenticated Receive Chain (ARC) combats this by adding a series of email headers that encrypt and store the original SPF and DMARC results to forwarded messages. The receiving system can then make decisions based not just on the SPF and DMARC information it calculates (for example, SPF might fail if the message was forwarded) but on the SPF and DMARC decisions of the original receiving system.

ARC works by utilizing three new headers. First, the *ARC-Authentication-Results* header contains the original SPF and DMARC results. The *ARC-Message-Signature* header stores information about the state of the headers as created by the forwarding system (so that the final receiver can trust what was recorded). Lastly, the *ARC-Seal* header snapshots the *ARC-Authentication-Results* and *ARC-Message-Signature* headers so that the receiver knows if they have been tampered with.

When the email arrives at the receiving server, the system reads the *ARC-Authentication-Results* header. If the forwarding system is trusted, the server can base its decision to classify the email as junk or deliver the email on what the original receiver determined (i.e., did the message pass SPF and DMARC on original delivery even though it will fail, on either or both tests, upon forwarding). The *ARC-Message-Signature* and *ARC-Seal* headers are used to prove the validity of the *ARC-Authentication-Results* header. For example, the *ARC-Message-Signature* hashes some headers from the message (listed in the *h* tag) and stores that hash in the *bh* tag. Changes to the message headers or body that invalidate the ARC headers are easily detected.

Each forwarding of the message creates a new ARC header set starting with an incrementing number (*i=2*; *i=3* etc.). Within the *ARC-Authentication-Results*, you will see that *spf=pass*, *dmarc=pass*, and *dkim=pass* for alignment purposes. An example of what the ARC headers look like in a message header is shown in Table 6-1:

<i>ARC-Authentication-Results</i>	<i>i=1; mx.microsoft.com 1; spf=pass smtp.mailfrom=office365itpros.com; dmarc=pass action=none header.from=office365itpros.com; dkim=pass header.d=office365itpros.com; arc=none</i>
<i>ARC-Message-Signature</i>	<i>i=1; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com; s=arcselector9901; h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck; bh=message-body-hash; b=hash-of-headers-in-h--tag</i>
<i>ARC-Seal</i>	<i>i=1; a=rsa-sha256; s=arcselector9901; d=microsoft.com; cv=none; b=hash</i>

TABLE 6-1: ARC SEAL HEADERS

The keys used to sign the hashes are in public DNS under the existing DKIM headers. In the above example, the selector (*s=*) is *arcselector9901*. The public key for this selector can be found in a TXT record called *arcselector9901._domainkey.microsoft.com*.

Microsoft 365 tenants trust each other. This means forwarding between tenants results in ARC headers, and the final receiving tenant can use the original receiver's SPF and DMARC results.

Adding Trusted Forwarders (ARC Sealers)

You may need to add your own trusted forwarders (ARC sealers) to your tenant. This could occur if Office 365 does not trust a forwarder that you need to trust or if you use a third-party message hygiene service in front of EOP that supports ARC sealing.

Using the Defender portal, you can add a list of trusted forwarders (ARC sealers). From the **Defender portal**, navigate to **Policies and rules > Threat Policies > Email authentication settings**. From the **Email Authentication Settings** page, select the **ARC** tab. Click the **Add** button to add a trusted sealer. If you have previously added a trusted sealer and need to add more, click the **Edit** button to update the list of trusted sealers. You can also use the **Edit** button to remove trusted sealers from the tenant.

Check [this article](#) for more information on ARC and adding trusted sealers to your tenant.

Sender Rewrite Scheme (SRS)

Authentication of your email messages with DMARC, DKIM, and SPF improves the reputation of your domain and brand by reducing spoofing and increasing the likelihood of detection of spoof attacks against the domain. However, some problems exist with these techniques. The primary issue is that SPF lists the IP addresses used for outbound emails. If your messages are delivered to another service that forwards them on again (using mail flow rules, distribution lists with external members, or inbox rules, for example), then the SPF information published for your domain makes the forwarding service appear to be a generator of spoofed email.

The Sender Rewrite Scheme (SRS) changes the P1 (or envelope from address) of auto-forwarded (or redirected) messages so that the receiving next-hop sees that the sender is the forwarding service and not the original sender. The goal is to try and avoid an SPF failure. SRS does this by changing the P1 header from the original sender's address and domain to an address that encapsulates the original sender's address but is really the forwarding service. Note, though, that this means that NDRs sent to these newly rewritten addresses will no longer return to the original sender but to the forwarding service, which in this case is Exchange Online. Exchange Online then unwraps the SRS rewritten header and sends the NDR back to the original sender. NDRs that cannot be unwrapped will go to a *bounces@<default-accepted-domain>* mailbox, which you need to create. The P2, or the *From* address the user sees in the email client, will not be changed. For example, before SRS is implemented, the P1 address is: *kim.akers@office365itpros.com*. After SRS is implemented and the initial receiving tenant forwards messages from the original sender, the P1 address might be something like this:

```
sales+SRS=f2ss=IX=office365itpros.com=kim.akers@itpros.com
```

This is best explained as:

```
<Forwarding Mailbox Username>+SRS=<Hash>=<Timestamp>=<Original Sender Domain>=<Original Sender Username>@<Forwarding Mailbox Domain>
```

Now that the forwarded email comes from the forwarding tenant, not the original system, it should not fail SPF. More details on the implementation of SRS are available on the [Exchange Blog](#).

Managing Connectors

EOP uses connectors to control inbound and outbound mail flow. By default, Exchange Online uses hidden connectors to allow messages to be sent between the tenant and the internet. However, there are many scenarios where you will need to configure additional connectors. For example, you will need a connector to

configure hybrid mail flow with an on-premises Exchange organization, deliver mail to or from a third-party message hygiene service, or force TLS with another party.

By default, EOP will always try to negotiate TLS with the receiving server. This is called opportunistic TLS. When TLS cannot be used, the sending server (EOP in this case) will revert to an unencrypted connection. However, if the recipient's message system supports TLS, EOP uses TLS for the connection.

Exceptions to this rule can exist. For example, a tenant admin could create a connector requiring TLS for a specific domain. In this scenario, the sender dictates that forced TLS must be used when sending to a particular recipient. Of course, the tenant admin should confirm that the recipient can indeed accept messages over TLS before building this connector. Setting up a dedicated connector that forces TLS might be helpful if you often communicate with a business partner or send highly confidential information.

Keep in mind that forced TLS is only good between two mail exchangers. Once the message is received by the recipient, it can then be forwarded in plain text. It is always best to leverage Office 365 Message Encryption (or Office 365 Advanced Message Encryption) for sensitive data. Ensuring the connection forces TLS is a bonus.

You may also create a connector to route messages to a specific smart host. This is often required if you use a third-party mail filtering, encryption, or data loss prevention solution in conjunction with Exchange Online. If you use a mail filtering solution in front of Exchange Online, be sure to check the section on Enhanced Filtering later in this chapter.

By default, messages in a hybrid deployment are always secured with TLS and require a valid, trusted digital certificate. The hybrid configuration wizard (HCW) configures these connectors, both on-premises and in the tenant, for you. The hybrid wizard configures these connectors with the "on-premises" type, which establishes that mail from your on-premises Exchange environment should be trusted. Messages that pass through a connector type of "on-premises" are stamped with additional headers, allowing messages from on-premises to bypass some Exchange Online Protection and Microsoft Defender checks.

Note: The first time you enable a connector type of "on-premises" in your tenant, it is disabled on creation. This is true whether the connector was created by the Hybrid Configuration Wizard or manually. To enable this connector, you must [open a case with Microsoft support](#) and provide a business justification.

Microsoft may block a connector if it detects suspicious activity. Suspicious activity could come in many forms, including a mismatch of P1 and P2 headers in outbound mail, mail sent from domains not registered in your tenant, or a sudden increase in outbound mail. You can determine if and how an inbound connector is compromised by using Threat Explorer in the Defender portal. We cover Threat Explorer later in this chapter. Once you have investigated and remediated the suspicious activity, you can unblock your connector by navigating to **Review > Restricted Entities** in the **Defender portal**. For more information on how to safely investigate and restore a connector, [see this page](#).

Real-world: Microsoft [announced a plan](#) to start throttling and blocking unsupported and non-compliant versions of Exchange Server that use the connector type of "on-premises" to send email to Exchange Online.

- Unsupported versions of Exchange, which at the time of writing are Exchange 2007, Exchange 2010, and Exchange 2013, will be initially throttled and later blocked from sending mail to Exchange Online.
- Supported versions of Exchange, which at the time of writing are Exchange 2016 and Exchange 2019, must remain up to date on cumulative and security updates to remain compliant. Non-compliant versions of Exchange 2016 and Exchange 2019 will be throttled after 30 days and blocked after 90 days of noncompliance.

The key takeaway is that if you send mail from Exchange on-premises servers to Exchange Online, you must upgrade or patch Exchange Server to a supported version. For more information, check <https://aka.ms/BlockUnsafeExchange>.

RFC5322 Support

From December 1, 2024, Microsoft will begin to require messages to comply with RFC 5322. This RFC mandates that email messages with multiple from entries in the P2 header also need to have a Sender header present. The Sender header can only contain a single address. Microsoft will send a notice to organizations where noncompliant messages are detected by October 15, 2024. This notice will include message IDs to assist administrators in tracking down the non-compliant messages to remediate the root cause. After the requirement becomes active, Exchange Online will drop messages that do not comply with RFC5322.

Creating a Connector

You can use the *New-InboundConnector* and *New-OutboundConnector* cmdlets to create connectors via PowerShell. However, the EAC wizard is much easier to work with. You do not have to specify what type of connector you want to create (inbound/outbound). Instead, you specify the source and target systems, and the wizard will automatically create the right connector. To open the wizard, open the EAC and navigate to **Mail flow > Connectors > Add a connector**.

For example, suppose we need to route mail to a specific domain through a smart host (rather than delivering to its MX record). For this, we can create an outbound partner connector. To do this, launch the connector wizard from **Mail Flow > Connectors > Add a connector**. Select Office 365 as the source and Partner Organization as the destination. Click **Next**. Give the connector a **Name** and **Description**. On this page, you can also choose whether to enable the connector as part of the wizard. You may wish to uncheck **Turn it on** if you want to enable this connector later manually. Click **Next**. On the *Use of connector* page, add your target domains in the **Only when email messages are sent to these domains** field. Click **Next**. On the *Routing* page, check **Route email through these smart hosts** and enter a fully qualified domain name (FQDN) or IP. Click **Next**. On the *Security Restrictions* page, specify whether to require TLS and the requirements for the certificate. Click **Next**. Validate the connector and click **Next**. Click **Create connector**.

According to Microsoft, many reported mail flow problems are caused by incorrectly configured connectors. To reduce the number of problems due to misconfiguration, when creating an outbound connector (from Office 365 to somewhere else), the wizard tries to validate the connector is functional before creating it. Then, an attempt is made to send a test message to a recipient you specify. The test is successful if the wizard can connect and deliver the message to the remote environment. If the validation fails, you can select to override the failure in the wizard and create the connector.

Using our example above, we can create this connector with PowerShell using the *New-OutboundConnector* cmdlet. We specify the scope of this connector with the *RecipientDomains* parameter and the delivery target with the *UseMXRecord* and *Smarthosts* parameters. The *TlsSettings* and *TlsDomains* parameters specify the TLS security when transferring mail over the connector.

```
New-OutboundConnector -Name "Contoso Outbound Connector" -ConnectorType Partner -RecipientDomains contoso.com -TlsSettings DomainValidation -TlsDomain *.contoso.com -UseMXRecord $false -Smarthosts mail.contoso.com
```

To review the properties of the connector (whether created in the EAC or PowerShell), you can use the *Get-InboundConnector* or *Get-OutboundConnector* cmdlet. In the example below, we retrieve the properties of the *Contoso Outbound Connector*.

```
Get-OutboundConnector "Contoso Outbound Connector" | Format-List
```

```

Enabled : True
UseMXRecord : False
Comment :
ConnectorType : Partner
ConnectorSource : Default
RecipientDomains : {contoso.com}
SmartHosts : {mail.contoso.com}
TlsDomain : *.contoso.com
TlsSettings : DomainValidation
IsTransportRuleScoped : False
RouteAllMessagesViaOnPremises : False
CloudServicesMailEnabled : False
AllAcceptedDomains : False
SenderRewritingEnabled : False
TestMode : False
LinkForModifiedConnector : 00000000-0000-0000-0000-000000000000
ValidationRecipients :
IsValidated : False
LastValidationTimestamp :
Name : Contoso Outbound Connector

```

For more information on creating connectors with PowerShell, check the [New-InboundConnector](#) and [New-OutboundConnector](#) Microsoft articles.

Mail Flow Rules

Email servers must be able to handle the various requirements an organization might have. It is no longer enough for a server to send messages from point A to point B. As an organization evolves, its messaging system must offer the right feature set to support the changing requirements of that organization.

One could compare the changing behavior of interacting with a messaging system to how people interact with the post office. Where before it was good enough to deliver a written letter to its recipient, today the post office offers many additional services. For instance, when you move to a new house, you can request the postal service to automatically forward mail addressed to your old location to your new home. This not only gives you the time to inform all users about the address change, but more importantly, it prevents mail from being returned to the sender or, worse: delivered to the wrong address.

The general idea behind mail flow rules is very like the above example. It provides Exchange Online with a way to dynamically handle incoming or outgoing messages based on one or more criteria. The way mail flow rules work in Exchange Online is very similar to how they operate in on-premises Exchange, with the main exception that Exchange Online mail flow rules have more conditions and actions to choose from. As a result, an organization can create up to 300 different mail flow rules.

Mail Flow Rule Conditions

Conditions (also known as predicates) define when a mail flow rule should be triggered. For instance, a condition can be used to check for a specific value in the sender's email address, or it can look for the existence of an attachment. The easiest way to build a new mail flow rule is to use the EAC, as you can select conditions from a drop-down list.

A rule can contain multiple conditions, in which case the message must match all individual conditions before any actions are triggered (logical "AND" configuration). You must create separate mail flow rules if you need to match several conditions in a logical "OR" configuration. If a single rule must apply for different values of the same condition, then add multiple values to a given condition. If multiple values are specified, the message must match one of the values assigned to the condition (logical "OR" configuration).

Note: It is also possible to create a "catch-all" rule. If you do not specify a condition (or you select *Apply to all messages*), the mail flow rule will be applied to every message that flows through the organization.

Mail Flow Rule Exceptions

Exceptions are, just like conditions, used to scope the applicability of mail flow rules. Exceptions are used in conjunction with 'regular' conditions to exclude matches against (one of) the primary condition(s). Each condition has a matching exception.

Multiple exceptions can be configured for a given rule, in which case a single match is needed for the rule to be skipped (logical "OR" configuration). Similarly, you can specify multiple values for a given exception, and the rule will be skipped if any of the values are encountered.

Note: Any predicate can be used if messages are unencrypted when they are processed. S/MIME encrypted messages (not to be confused with messages protected with sensitivity labels or Office 365 Message Encryption) cannot be processed by mail flow rules based on conditions that inspect the contents of the message. In any other case, mail flow rules with conditions based on a message's envelope header will still work correctly.

For a comprehensive list of mail flow predicates and exceptions, check this [Microsoft article](#).

Mail Flow Rule Actions

Actions ultimately carry out a task on the message. Each action uniquely affects the message, either by changing some of the message's properties or altering the routing behavior of the message. Amongst other actions, you can, for instance, re-route, reject, mark as spam, or silently redirect a message.

A mail flow rule can include multiple actions. Each rule has a priority number, and the transport service processes applicable rules in ascending order of priority. This means that if you want to execute actions in multiple rules on a message, you must plan the rules so that the desired actions run in the correct order. In determining the priority order for rules, you should consider the possibility that a rule might cause all further processing to stop after it completes because it includes the *Stop processing more rules* option. Rules also stop processing if a rule's action is to drop (delete) a message, as the next rule will not have a message to process. Something similar happens if the action is set to moderate the message (sent for approval): Exchange won't process higher priority rules until a moderator approves the message. After approval, the transport service evaluates the remaining rules against the message.

Note: Over the years since the introduction of EOP, the options for spam and malware filtering have expanded. This means fewer reasons to use mail flow rules for spam/malware filtering. For example, the malware filter includes attachment protection settings, thus avoiding the need to look for attachments by file extension name in a mail flow rule.

For a complete list of all actions available for a mail flow rule, check [this article](#).

Mail Flow Rule Properties

Apart from the building blocks detailed above, each mail flow rule also has properties that control various aspects of its processing. These include:

- **Priority** determines the order in which rules are processed. By default, Exchange Online orders mail flow rules by creation date, but you can override the processing order by adjusting the value of the priority property. Rules are processed from the lowest to the highest value.
- **Severity** allows you to "tag" a rule as either *Low*, *Medium*, *High*, *Not Audit*, or *Not specified* severity, making it easier to filter or group the data in the mail flow rule reports.
- **Rule mode** gives you the option to test a rule before turning it on (explained below).

- Optionally, you can toggle the **Activate this rule on** and/or **Deactivate this rule on** checkboxes to "schedule" the rule to be active only during a given time.
- The **Stop processing more rules** setting effectively stops mail flow rule processing after the given rule has executed its actions. Any mail flow rule with lower priority will not be affected.
- Turning on the **Defer the message if rule processing doesn't complete** option will cause the message to be resubmitted for reprocessing in the event of a failure to process the given mail flow rule.
- The selection under the **Match sender address in message** dropdown allows you to specify whether matches against any conditions or exceptions, including the sender address, are performed against the header value, the envelope value, or both.
- Lastly, the **Comments** field is available to store additional information about the rule, such as its creation date, the reason for a given modification, etc.

Apart from all the properties listed above, you can also toggle a mail flow rule On or Off by selecting the corresponding checkbox in the list of rules presented in the EAC or via the *Enable-TransportRule* or *Disable-TransportRule* cmdlets.

Creating a New Mail Flow Rule

As mentioned earlier, the easiest way to create a new mail flow rule is to use the wizard in the EAC, as it allows you to select conditions, exceptions, and actions from a drop-down list. The EAC also allows you to select a pre-configured mail flow rule from a list of templates. These templates cover common scenarios, such as allowing a specific message to bypass spam filtering. The conditions, exceptions, and actions are already pre-selected depending on the template you selected. You only need to specify a unique value(s) for any of the specified properties. For instance, if you select the **Bypass spam filtering** template, the **Set the spam confidence level (SCL)** action with a value of **-1** has already been selected, and you then select which message (condition) you want to apply this action. If you prefer to start with a blank rule, where no conditions or actions have been predefined, select **Create a new rule**.

Testing New Mail Flow Rules

Before you put a new mail flow rule into production, it is wise to verify that it does what you expect. You can verify whether a mail flow rule works by enabling it in test mode. You will have the following options to choose from when creating a new mail flow rule:

- Enforce (default).
- Test with policy tips.
- Test without policy tips.

The **Enforce** option triggers the rule if all the conditions of the rule are met. However, **Test without policy tips** will stop the rule action from running because the rule is in test mode. But how do you know the rule has worked if it does not fire? There are a couple of ways to do this.

The first is to leverage the *Test-Message* PowerShell cmdlet. This following example sends a payload, saved in the variable named \$data (the payload is in EML format) to a recipient. If the transport rule you are trying to test is looking for content in a message body or attachment be sure your EML payload contains the necessary data.

```
$data = [System.IO.File]::ReadAllBytes('C:\data\test.eml')

Test-Message -MessageFileData $data -Sender john.smith@office365itpros.com -Recipients
jane.doe@office365itpros.com -SendReportTo admin@office365itpros.com -TransportRules
-UnifiedDlpRules
```

The outcome of this test is emailed to the recipient specified by the *SendReportTo* parameter. The *TransportRules* parameter is necessary in this instance as it forces the test to pass through all transport rules. You can also specify the *UnifiedDlpRules* parameter if you also want the test to consider your DLP rules.

Alternatively, you can use the **Generate incident report and send it to** action in your rule. The **Generate incident report and send it to** action sends an email to the selected recipient with information about the message that caused the rule to trigger. In test mode (with Test without policy tips enabled), Exchange Online generates and sends the incident report email. Still, the other actions specified in the rule, such as setting a disclaimer, are not performed. The incident report action allows you to select the properties of the message you want to include in the incident report. For example, if you are working with sensitive information or local legislation prevents you from accessing the contents of a message without notifying the user, you can opt not to include the original mail and make sure that the incident report only reveals non-crucial information about the message. An example of an incident report email appears below, where we see that the disclaimer rule "Corporate Disclaimer" was triggered. Because the rule was in test mode, the actual disclaimer was not applied and, therefore, not seen by the recipient.

```
Report Id: bbc7457a-64a9-44c5-a246-1b7d35db116b
This email was automatically generated by the Generate Incident Report action.
Message Id: <VI1PR06MB1183C94FCA77A1BFB979A927C9560@VI1PR06MB1183.eurprd06.prod.outlook.com
Sender: john.smith@office365itpros.com
Subject: Incident Report Testing
Recipients: jane.doe@office365itpros.com
Severity: Low
Override: No
False Positive: No
Rule Hit: Corporate Disclaimer, Action: ApplyHtmlDisclaimer, GenerateIncidentReport
```

Incident Reports are an easy way to check the effectiveness of a mail flow rule and, at the same time, gather information about what kind of messages will trigger the rule. This will allow you to decide whether the mail flow rule meets your expectations. Once you decide that the mail flow rule is ready for production, you can edit the mail flow rule and choose to **Enforce** it. Do not forget to remove the action to send an incident report, or you will receive a report each time the rule is triggered!

Monitoring Mail Flow Rule Usage

One measurement of the effectiveness of a mail flow rule is the number of times it triggers. Of course, there might be cases where you hope a mail flow rule never triggers, such as when a mail flow rule enacts an *ethical wall* to prevent two departments from communicating with one another. This is often seen in financial institutions where regulations define that market researchers cannot communicate with brokers to avoid a conflict of interest or (in-)voluntary market manipulation.

The Exchange Admin Center includes the "Exchange Transport Rule" report dedicated to mail flow rules. The report gives you a breakdown of all the individual mail flow rule matches in either a graphical or table view. In addition, you can also group the results by the audit severity value, which we described earlier. Like many of the other Exchange-related reports, you can schedule this report to be emailed to specified recipients on a weekly or monthly basis. We will discuss this report and others later.

The *Get-MailDetailTransportRuleReport* cmdlet searches for specific transport-rule related events. For instance, it can be used to search for 'hits' within a given timeframe or to look for actions that have been performed because a mail flow rule was executed. The example shown below reports all mail flow rule hits in the past 5 days and lists the date and time, message subject, action taken, and rule that was executed:

```
Get-MailDetailTransportRuleReport -StartDate (Get-Date).AddDays(-5) -EndDate (Get-Date) | Format-List Date, Subject, Action, *Rule*
```

If you need to search for hits of a specific mail flow rule, you can use the following command:

Get-MailDetailTransportRuleReport -TransportRule "Check for sensitive data"

The cmdlet has many more parameters that allow you to refine the results further. For instance, you can look for messages from a specific sender:

```
Get-MailDetailTransportRuleReport -StartDate (Get-Date).AddDays(-5) -EndDate (Get-Date) -Sender Joe@office365itpros.com
```

The dashboard reports and the data generated by the PowerShell cmdlets come from Microsoft's reporting data warehouse. The only downside to this approach is that the information in the data warehouse isn't always up to date. It can take up to a day before these cmdlets return complete data. If you are looking for an immediate way to measure mail flow rules, adding an incident report is preferred.

Mail Flow Rule Limitations

Microsoft limits the amount of transport and journal rules each tenant can create. These limitations protect the service by limiting the amount of routing logic applied to each message. Table 6-2 list some of the rule limits.

Feature	Limit	Additional Information
Journal Rules	300	The maximum number of journal rules that can be created in a tenant
Mail Flow Rules	300	The maximum number of mail flow rules that can be created in a tenant

Table 6-2: Mail flow rule limits

Common Use Cases for Mail Flow Rules

Because of the many available conditions, mail flow rules are helpful in a myriad of scenarios. It would be impossible to list all the use cases here, but we will look at some of the more common scenarios and tasks. The examples from the scenarios described below should provide you with enough insights into the capabilities of mail flow rules so that you can produce viable solutions to any unique requirements you have.

Organization-wide Disclaimers

Sometimes legal or regulatory requirements dictate the need for an organization to add disclaimer text to outbound messages. Mail flow rules can handle this requirement because one of the actions available to a mail flow rule is the ability to prepend or append a disclaimer to a message. The content of the message can be plain text, but it can also include HTML code to make it more dynamic.

Additionally, you can include certain variables based on the attributes of a user's account to insert user-specific values in the disclaimer. For instance, by adding `%%DisplayName%%` to the disclaimer text, Exchange Online inserts the sender's display name into the text.

However, when you add a disclaimer to all outgoing messages, the user experience may not be what you expect. For example, in Figure 6-6, when you append a disclaimer to a message, the transport service adds the disclaimer text to the end of the message. Of course, this is precisely where you would expect it to be for a new message (1). However, if you reply to an email thread, you will notice that the disclaimer is added at the very bottom of the entire thread, not after the latest reply (2). This might be perfectly acceptable for a disclaimer, but it looks odd for signatures.

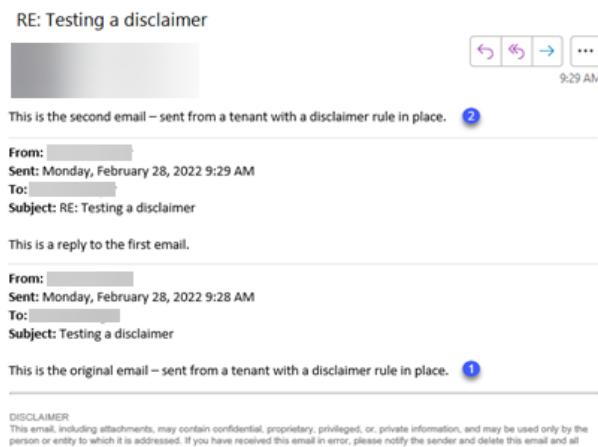


Figure 6-6: The disclaimer text added by a mail flow rule appears at the bottom of a message

Although you cannot make a mail flow rule add text at the end of the latest message, you can stop the rule by adding disclaimer text or signature if one already exists by adding an exception to the rule. This PowerShell example shows how:

```
New-TransportRule -Name "CompanyDisclaimer" -Enabled $True -SentToScope "NotInOrganization" -ApplyHtmlDisclaimerLocation "Append" -ApplyHtmlDisclaimerText <br><hr><font face='Arial' color='Gray' size='1'><br>DISCLAIMER<br>This email, including attachments, may contain confidential, proprietary, privileged, or, private information, and may be used only by the person or entity to which it is addressed. If you have received this email in error, please notify the sender and delete this email and all attachments. <br></font>" -ExceptIfSubjectOrBodyContainsWords "This email, including attachments, may contain confidential, proprietary, privileged, or, private information, and may be used"
```

The first time the message is processed, the rule runs and adds the disclaimer because it's improbable that the phrase used by the exception is present in the body or subject. However, on any subsequent occasion, the message or its replies pass through the transport service, such as when a recipient sends a further reply, the rule exception prevents the insertion of the disclaimer because the body now contains the exact words added by the same rule the first time the message was processed.

Note: One important limitation of mail flow rules is that the total size of the disclaimer cannot exceed 5,000 characters. This includes the text and any HTML tags or Cascading Style Sheet (CSS) code you might add.

To increase the range of information available for corporate disclaimers and to allow more flexibility in the number of types of disclaimers in use at any time, commercial email signature products often take a different approach when applying disclaimers to outbound email.

Bypass Spam Filtering

As discussed later, EOP automatically collects allowed and blocked sender settings from the junk mail settings managed by users through Outlook and OWA. Sometimes, an organization might want to centrally control which senders receive automatic approval and those marked as spam. For instance, this will be necessary if you introduce a new corporate communications tool that sends messages from an external system.

To achieve this goal in Exchange Online, you can use a mail flow rule to add a message header set to a specific value. In this case, the header is the "SCL" header (Spam Confidence Level) which will be set to a value of "-1". The value of the SCL header determines if a message should be sent to the user's junk email folder at the end of the processing pipeline. Table 6-3 describes the values used for the SCL header in Exchange Online:

SCL Value	Meaning
-1	The message is deemed safe because the sender is safe-listed, the sender's server is on an IP safe list, or the recipient is on the safe-recipient list. Therefore, the content filtering engine does not process the message.
0, 1	After processing by the content filtering engine, the message was deemed to be clean.
5, 6	After processing by the content filtering engine, there is reasonable confidence to mark the message as spam.
9	After processing by the content filtering engine, there is no doubt (high confidence) that the message is spam.

Table 6-3: SCL header values in Exchange Online

In the following PowerShell example, a new mail flow rule is added to create a safe list that will automatically mark messages from the office365itpros.com domain as safe:

```
New-TransportRule -Name DomainSafeList -SenderDomainIs "office365itpros.com" -SetSCL "-1"
```

Real-world: Care should be taken with setting blanket safe list rules like those shown above. If the domains or senders in question have their email address spoofed so that a message does not come from the user or organization who owns the mailbox but instead from someone acting as that sender or domain, EOP will mark the email as safe. This is because the rule checks the domain or user and not doesn't do anything to validate the reliability of the sender. Anti-phishing rules are recommended as a replacement for blanket allow lists.

Conditional Mail Routing

Conditional Mail Routing allows you to use mail flow rules to alter the default routing behavior for specific messages that match the conditions of a mail flow rule. However, if you want to control the behavior for all outbound messages, it is better to create a custom connector instead.

Consider the following scenario: You represent a large organization with multiple types of users—for instance, an educational institution with students, staff, and faculty. You use Exchange Online for both types of users but want email from staff and faculty to be routed to the internet through an on-premises appliance that offers compliance features like journaling, data loss prevention, message encryption, etc. Even though these features also exist in Exchange Online, you previously invested in the solution and do not want to lose out on those investments. If you created a regular outbound connector, all messages would be routed through the external appliance, including those from students. So instead, you create a new connector, only to be used by a mail flow rule which defines that outbound messages sent by faculty and staff mailboxes should be routed through the new connector.

This scenario is an excellent example of how conditional mail routing can help an organization meet regulatory requirements without making extensive changes to other parts of the configuration and leveraging prior investments. Although conditional mail routing adds a layer of complexity to the entire solution by splitting the message routing logic, it can be extremely valuable if carefully planned and used for the right purposes.

Real-world: The most common use of conditional mail routing is to ensure that messages sent to specific users or applications are either encrypted with TLS or sent directly to a specific system. The latter option requires the outbound connector to be configured with a smart host. As such, the MX records for the recipient's domain are ignored, and messages are delivered directly to the specified smart host. This is also done to ensure messages are sent to servers in a specific region. Often the recipient's organization does not have the infrastructure to dynamically (and geographically) route incoming messages directly to servers in the same region as the mailbox. In such a case, the sender's organization can then use conditional mail routing to accomplish the task.

Conditional mail routing relies on mail flow rules to check the properties or content of a message. The mail flow rules will redirect the message to the selected connector if a specific condition is met. Thus, before creating a mail flow rule to redirect messages to a specific connector, you must first set up a connector and configure it for conditional mail routing. To do this, create a custom outbound connector and select the option **Only when I have a transport rule set up that redirects messages to this connector** when asked, 'When do you want to use this connector?'.

In the following example, we will configure a mail flow rule to redirect all messages sent by "kim.akers@office365itpros.com" through the custom connector *Outbound to Compliance Appliance*. We will only configure the basic settings to make this rule work. Start by opening the new mail flow rule wizard from the EAC, selecting **Mail Flow**, and navigating to **Rules**. From the Rules page, select **Add a rule > Create a new rule**.

1. Specify a descriptive name for the rule. This will ensure that you can easily find the rule in the list of rules.
2. Select a condition to which the message should apply. For this example, under the **Apply this rule if** dropdowns select **The sender** and **is this person**. From the *Select Members* pane select or search for the recipient and click **Save**. For example, *kim.akers@office365itpros.com*.
3. Select the action that should be applied on the message. For this example, under the **Do the following** drop downs select **Redirect the message to** and **the following connector**. From the *Select Connector* pane select the connector and click **Save**. For example, *Outbound to Compliance Appliance*.

After saving the mail flow rule, it is enabled and will apply to any outbound message sent by *kim.akers@office365itpros.com*.

Identifying External Senders

Adding a warning message to emails from external senders is a common use case for mail flow rules. For many organizations, this warning message is a core part of end-user training to identify and report potential phishing messages. The downside to using a mail flow rule is that the warning message is often unsightly and might be included in future replies to the sender. You can enable external email tagging in Exchange Online to transition away from a mail flow rule (if you have one). Exchange Online's external email tagging functionality is available in Outlook, OWA, Outlook Mobile, and Outlook for Mac.

To enable external email tagging, run the following command:

```
Set-ExternalInOutlook -Enabled:$true
```

When Exchange Online marks a message as external, it sets the *IsExternalSender* MAPI property for the message to True. Clients check for the property and display the warning if it is True.

Some organizations don't like how Outlook marks messages as external and prefer doing the job themselves. To turn the feature off, set the value of the *Enabled* parameter to \$False. It can take a little while before Exchange Online ceases to set the *IsExternalSender* property.

You can specify external email domains that Exchange should not treat as "external." For example, you might have messages from a third-party training system that should appear to be from an internal sender. To add a domain to the list of allowed external senders by running the following command:

```
Set-ExternalInOutlook -AllowList @{Add="Office365ITPros.com"}
```

Exporting and Importing Mail Flow Rules

Although mail flow rules can be enabled in test mode, it can sometimes come in handy to experiment with a few settings in a test tenant. Once testing is complete, you can export the rule(s) from a test tenant and import them into the production tenant. To export mail flow rules from a tenant, run the following command while connected to Exchange Online PowerShell:

```
Set-Content C:\ExportTransportRules.xml -Value ((Export-TransportRuleCollection).FileData  
-Encoding Byte)
```

Next, connect to the target tenant and run the following command to import the ruleset:

```
Import-TransportRuleCollection -FileData (Get-Content -Path C:\ExportTransportRules.XML -Encoding  
Byte -ReadCount 0)
```

Confirm

Importing a rule collection will overwrite all existing rules in that collection. Do you want to
continue?

[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (default is "Y"): Y

Real-world: The *Import-TransportRuleCollection* cmdlet overwrites the existing mail flow rules in the target tenant with the content of the XML file. This command is a rip and replace. In this example, this means the mail flow rules you export from the test tenant will overwrite the rules in the production tenant. To ensure you have a rollback option, export rules from the target tenant before import.

Remote Domains

Any email domain not registered with your tenant is considered a remote domain. By default, you can deliver email to any remote domain. However, an organization might want to limit what messages get sent to remote organizations, or maybe they want to control the message format. This is where remote domain configuration settings are useful.

A remote domain allows you to control the following:

- **Out of Office replies.** Allow or deny replies to be sent to the domain. You can also control whether the internal or external out-of-office response is sent.
- **Automatic replies and forwarding.** You can control if a user-generated rule can automatically reply to or forward messages to the remote domain.
- **Message reporting.** This allows you to control whether message status notifications should be sent to the remote domain. For instance, you can prevent non-delivery reports from being sent to a remote domain or configure that meeting forward notifications are sent; by default, meeting forward notifications are only sent within the organization.
- **Format of the message.** Allows you to define if a message should be sent in rich text and what MIME character set should be used, if at all.

Note: The settings you specify for a remote domain override any user-specific settings, for instance, configured through the *Set-MailboxAutoReplyConfiguration* cmdlet. If you want to modify default settings for all other unlisted domains, you must modify the default remote domain.

You can add a new remote domain or configure an existing one by going to **Mail flow** and **Remote domains** in the EAC.

Automatic message forwarding is a common action that attackers take when they compromise a mailbox. Because this threat exists, Exchange Online does not allow automatic forwarding by default. You can amend the default policy to allow users to auto-forward email, but this is a terrible idea. Instead, if some users need

to auto-forward email from their mailboxes, you can create a custom outbound spam filter policy. The custom policy specifies the email addresses of users who can auto-forward their email outside the organization.

Fallback Domains

When you sign up for Office 365, you are asked to specify an initial domain. This domain, in the form of <custom name>.onmicrosoft.com, is the first fallback domain. The initial fallback domain is by default used for SMTP addresses and for routing email messages. Even after adding email addresses using custom domains, an address using the fallback domain is always configured, making sure messages can be routed properly when you remove the custom domain for example.

It is possible to configure additional onmicrosoft.com domains in your tenant. That is, provided the custom onmicrosoft.com domain is still available. When desired, after adding another custom onmicrosoft.com, you can promote this onmicrosoft.com domain as your new fallback domain.

Note: You can have a total of 5 onmicrosoft.com domains configured in your tenant. Additionally configured fallback domains are currently permanent. Once added, they cannot be removed, so choose your name wisely.

To add a custom onmicrosoft.com domain, from the Microsoft 365 admin center, navigate to **Settings > Domains**. There, select the current fallback domain. The admin center displays details of the fallback domain. The option to **Add onmicrosoft.com domain** is at the bottom right. Enter the name of the new custom fallback domain and click **Add domain**. Office 365 checks if the domain is already taken by another tenant. If it is, you must pick another domain. If everything checks out, Exchange Online adds the domain to the accepted domain list for the tenant.

To make the new domain your new fallback domain, select the domain you just added. In the status view that comes up, you will have the option **Make fallback domain**. Be advised that this operation will not change the SharePoint or OneDrive URLs, and only becomes the new Microsoft Online Exchange Routing Address (MOERA). This means only new provisioned mail-related objects such as mailboxes or distribution groups will get a proxy address using the new fallback domain. Existing proxy addresses using the previous fallback domain are not modified. When required, you need to make this adjustment yourself.

Device and App Mail Relay to Exchange Online

Even in the digital world, people still print many documents. Often, these documents are scanned again for digital archiving. For years, scanners could email scanned messages. Despite sending email messages, many of these devices do not support authentication and can only send plain, unauthenticated SMTP messages. Scanned messages mostly go to internal recipients anyway. However, the same is not always true for some line-of-business (LOB) applications. For example, the application might need to send a message to an external recipient when an order is updated.

This is not a problem for Exchange on-premises because you can scope your firewall to accept messages from specific device or application IP addresses. However, it's not that simple with EOP. Because EOP is publicly available on the internet, allowing unauthenticated SMTP would open the door to spammers to use EOP as an "open relay." Today, there are four possible solutions:

- If your device or application supports authentication, you configure it to use the credentials of an Exchange Online mailbox to send messages internally and externally. This method requires the device to support TLS 1.2 and send mail over port 587. Microsoft refers to this method as **SMTP Auth**.

Note: Using TLS 1.0 and TLS 1.1 with the smtp.office365.com endpoint is unsupported. Any devices or applications that require these older protocols will need to leverage the legacy endpoint of smtp-

legacy.office365.com. To activate this [legacy endpoint](#), tenant administrators must run `Set-TransportConfig -AllowLegacyTLSClients $true`.

Note: Microsoft announced that support for Basic Authentication with Client Submission (SMTP AUTH) will be removed in September 2025. To help administrators identify these authentication methods, the EAC will receive an additional report option in September 2024, identifying SMTP AUTH sent mail with Basic Auth and OAuth usage. Organizations sending mail to external recipients using SMTP AUTH will need endpoints supporting OAuth, or should consider the use of High Volume Email (HVE) or [Azure Communications Services Email](#). Hybrid Exchange organizations can continue using Exchange on-premises servers to accept messages using Basic Auth with SMTP AUTH. If you only send messages to internal recipients, you will need to start using High Volume Email, described later in this chapter.

- If the device or application either does not support authentication, does not support TLS, or can only use port 25, you can use **Direct Send**. Note that this can only be used to send mail to internal recipients in your tenant. Any external recipient will be rejected. Mail will also be heavily scrutinized and be subject to anti-spam policies and could be flagged as spam.
- If a device needs to send mail to external recipients, another option is to use a **custom connector** to identify and authenticate all on-premises devices and applications that need to send email messages. This option will likely require network configuration changes to ensure that all outbound connections from these devices and applications to Exchange Online originate from a specific set of IP addresses.

Note: If you use a custom connector to relay messages through Exchange Online there is a chance that Microsoft will send your messages through the relay pool, rather than the regular pool. If Microsoft sends messages through the relay pool, the likelihood of your messages ending up in a recipient's junk folder increases. This can happen if the sending domain is misconfigured (for example, an invalid SPF or DKIM record). To identify messages sent through the relay pool, you can use the **Top Domain Mailflow Status Report > Outbound** tab discussed later in this chapter.

- A custom or third-party SMTP relay solution is used to forward messages to Exchange Online on behalf of the SMTP device or application. For instance, the IIS SMTP service can be used to create a custom SMTP relay solution. The SMTP service will accept unauthenticated messages from devices and applications within your network and, in turn, forward the messages to Exchange Online using the credentials of an Exchange Online mailbox.

For information on configuring each of these relay methods, check this Microsoft [article](#).

Real-world: While it is possible to eliminate your last on-premises Exchange server for management tasks, many organizations maintain Exchange servers for SMTP relay for on-premises devices and apps. In those scenarios, it is easier to keep routing those emails through the existing Exchange Servers configured for secure hybrid mail flow.

The other aspect is security. Many enterprises leverage firewall rules to govern what devices and apps can send outbound mail. For security-conscious organizations want to minimize the number of outbound SMTP connections to the absolute minimum. To use an analogy, they do not want to Swiss-cheese their firewall. In this scenario, security dictates that only a handful of known and centrally managed Exchange servers (or 3rd-party relays) can send outbound mail.

High Volume Email (HVE)

For organizations that need to send bulk messages to internal recipients, Microsoft introduced the High Volume Email (HVE) for Microsoft 365 service. This service, which currently is in Preview, is specifically designed to allow organizations to end LOB and other high-volume messages to primarily internal recipients. The difference with using named accounts is that these messages are subject to different messaging limits than regular users.

During the preview, using HVE will be without cost, and messages are limited to 100,000 recipients per day per tenant, with no limit on the message rate limit. Note that this is a preview release and limitations for HVE are subject to change when the service becomes generally available. For now, HVE accounts have a higher daily recipient limit and an unlimited message rate. More on transport limits in the Transport Limits section in this chapter.

To use HVE, the tenant must create HVE accounts, which LOB applications and devices will use to authenticate. You can create up to 20 HVE accounts for this purpose. Note that addressing some external recipients is tolerated, up to 2,000 external recipients per day per account. While it is technically possible for an end user to use HVE accounts to send messages to internal (and some external) recipients, this is not what this service is intended for. When HVE is generally available, the service will likely operate on a Pay-as-You-Go basis through an Azure subscription.

Note: While the 2,000 external recipients per day per account rate limit is documented, there is also an undocumented 10 messages per minute rate limit for messages sent to external recipients. Like many throttling measures, this can be prevented by inserting a short pause between sending two messages. Alternatively, you can leverage the 20 HVE account limit to spread sending messages over multiple HVE accounts.

To configure HVE, open the EAC, go to **Mail flow**, and select the **High Volume Email (Preview)**. There, you can configure accounts using **Add an HVE account**, specifying the account's Display Name, Primary email address, alias, and the password. The email address and password are used by LOB applications or devices that use the HVE service to send email. You can also create HVE accounts with PowerShell:

```
$Pw= Read-Host 'Enter password for HVE account' -AsSecureString  
New-MailUser -LOBAppAccount -Name 'HVEAccount1' -Password $Pw -PrimarySmtpAddress  
'HVEAccount1@office365itpros.com'
```

The HVE account is a Mail-Enabled User configured as an object hidden from the Global Address List. When you inspect the properties of the Mail User object, you will see that it has a generated address in the form of *SMTP:donotedit-8c13d3ab-41a9-49ad-9884-1f9819000f32@localhost*. There is no further information available as to the purpose of this address, so don't attempt to amend the address.

The next step is to allow Basic Authentication for the HVE accounts. If this isn't done, the accounts might not be able to authenticate and send messages using SMTP. You can create an authentication policy to accomplish this, e.g.

```
New-AuthenticationPolicy -Name 'HVE Auth Policy' -AllowBasicAuthSmtp  
Set-User -Identity HVEAccount1 -AuthenticationPolicy 'HVE Auth Policy'
```

The last thing to do is reconfigure your LOB application or device to use a different SMTP endpoint. The endpoint for HVE is **smtp-hve.office365.com** (instead of smtp.office365.com or smtp-legacy.office365.com). The port to use is **587**, TLS is required (STARTTLS, with TLS 1.2 and TLS 1.3 support), and the username (email) and password are the credentials for a HVE account. HVE can only send messages, so delivery service notifications such as an NDR cannot be processed unless caught by a transport rule redirecting them to a mailbox.

An EAC report is available showing how many messages were sent by each HVE account during the reporting period. Unfortunately, there is no breakdown of internal and external recipients, or any issues encountered when sending messages. You might also request a report containing more details, but this information is at least two days old compared to the one-day age of the information in the HVE Mail summary report.

Note: Messages sent using HVE include a HVE flag in the *X-MS-Exchange-AtpMessageProperties* message header. This header shows what protections have been applied to the message, and commonly contains SA and SL for Safe Attachments and Safe Links respectively.

Exchange Online Protection (EOP)

Exchange Online Protection (EOP) is Microsoft's cloud-based email filtering service. EOP includes a set of message hygiene features to sanitize inbound and outbound mail flow and remove threats from messages. EOP protects all emails exchanged between Exchange Online (including between tenants) and external sources. Protection is in place to divert spam and malware and to guard against potential data loss. There are three configurations for EOP:

- **Exchange Online (cloud-only) deployment.** Although EOP is a separate feature, it is an integral part of and tightly integrated into Exchange Online. If you have an Exchange Online tenant, you automatically use EOP.
- **Standalone.** Organizations that do not use Exchange Online can route email traffic to EOP to use it as an email hygiene service. This can be for an on-premises Exchange environment or another email solution (hosted or on-premises).
- **Hybrid deployments.** In this scenario, EOP protects the traffic between the cloud and the on-premises servers. In a non-centralized mail flow approach, EOP can protect on-premises mailboxes as it does in a standalone deployment.

Exchange Online provides redundancy and load-balancing within a data center region. This also satisfies regulatory requirements that might need data to remain within a particular geographical area, such as the EU data processing guidelines. EOP running in country-level data centers (like Norway, France, or the United Kingdom) processes messages for tenants in those countries. EOP running in data centers in the United States (US) processes messages for US tenants. This means that it is vital to be aware of the correct namespace to use when routing messages so that you do not route to the wrong data center and have the message declined.

How EOP Processes Email

The filtering system in EOP consists of multiple layers and processes to handle inbound and outbound messages. To understand how Exchange Online processes messages, let us review the diagram shown in Figure 6-7, which shows how EOP uses inbound mail filtering to protect Exchange Online mailboxes.

The transport service routes email from source to destination unless the message triggers some component of the service that deems the message unsafe, in which case the properties of the message are changed, or the message is routed to the quarantine or rejected outright.

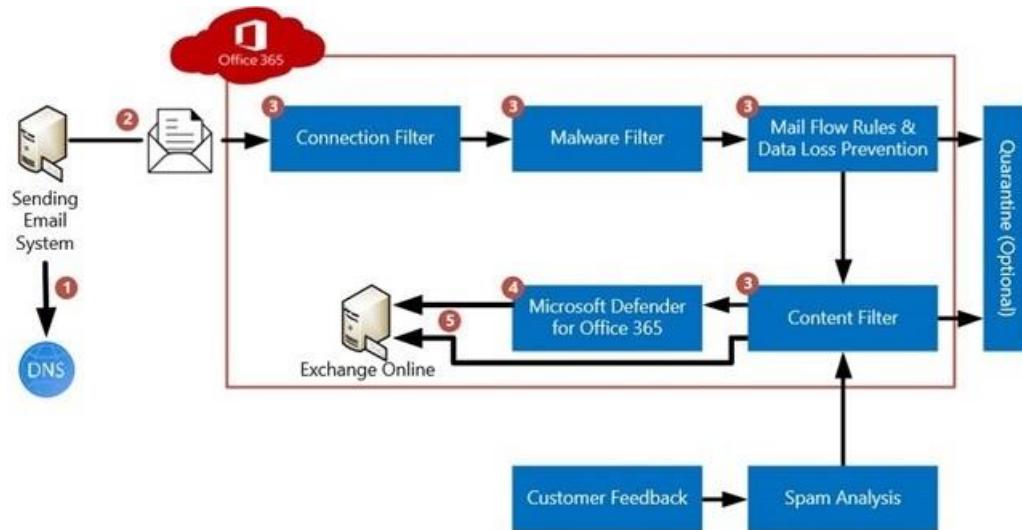


Figure 6-7: How EOP protects email

Figure 6-7 shows the route a message takes through EOP:

1. The sender's mail server looks up the domain MX record information (in our example, the MX record resolves to EOP).
2. The MX record resolves to the data centers in the primary region to which the tenant belongs. The sending mail server then tries to deliver the message to the MX endpoint retrieved earlier. To accept messages from the internet, you do not need to configure anything. The default connector in Exchange Online (which is invisible to the administrator) automatically accepts all messages.
3. Before the message is delivered to the recipient(s), it goes through several layers of filtering:
 - a. **Connection Filtering.** The connection filter is the first layer of defense. It checks several items, including the sender's reputation. In addition, an administrator can define an IP allow/block list to allow or block connections from specific IP addresses. Administrators can also opt into the safe list, a curated list of IPs Microsoft has deemed safe. By enabling this option, all safe list members bypass spam filtering.
 - b. **Malware filter.** This filter inspects the message for malware and viruses. If a message is deemed malicious, it is removed from the mail pipeline by default. However, it is not rejected at this stage because the sender does not get a notification or non-deliverable response that you might expect when a message fails to reach its target. Configuring anti-malware rules will be covered later.
 - c. **Policy Enforcement.** The policy filter checks messages against configured mail flow rules or data loss prevention (DLP) policies. If a message matches a rule or policy, the action(s) configured for that rule or policy are applied to the message.
 - d. **Content Filtering** is where the content of messages goes through checks to determine whether the message is spam or phishing based. If a message is considered spam, phishing, bulk, or high-confidence phishing, it can be deleted, sent to the user's Junk Email folder, or quarantined within EOP, depending upon the settings and rules you have configured.
4. If the tenant has Microsoft Defender for Office 365 licenses and the right policies are in place, messages will receive additional scanning before moving on to the next step.
5. If the message was not dropped, rejected, or quarantined, it is delivered to the recipient(s).

Note: Hybrid mail flow is handled slightly differently. Messages received from the on-premises organization are marked as "internal" and bypass content filtering (anti-spam). However, if the hybrid mail flow is not correctly configured, internal senders could be treated as anonymous and external to the organization. This could cause messages from internal senders to be incorrectly quarantined, moved to junk, or outright rejected.

Outbound messages are also scanned and evaluated:

1. Outbound messages first go through the **Anti-malware filter**, where they are scanned for known viruses.
2. Next, messages make their way through the **Policy Enforcement** engine. Here, messages are evaluated using configured policies such as mail flow rules, email encryption, and data loss prevention (DLP) rules. If a message matches one of the rules, the action from that rule is applied to the message.
3. The **Content Filtering** process exists to decide if sent messages are spam. A variety of techniques are used, and if a message is likely to be spam, two things can happen:
 - a. The message is routed through EOP's *High-Risk Delivery Pool*. This pool of EOP servers is used to send messages flagged as potentially being spam. This means that regular mail flow will not be affected if one of the IP addresses in the high-risk pool is blocked. Out-of-office messages are also sent via the high-risk delivery pool.
 - b. Depending on the configuration, and the characteristics of the email, it can also be quarantined.

4. If a message is considered safe, it is routed to its destination through the regular outbound pool. Unlike the high-risk pool, these servers are only used to send messages considered safe.

Real-world: Sometimes, the mail server to which EOP should deliver messages may be (temporarily) unavailable. Queuing will only happen for "transient errors," such as connection time-outs, refused connections, or other SMTP errors with 4XX error codes. Any "hard failure," such as invalid recipients, authentication mismatch, or failures shown by an SMTP 5XX error code, will generate a non-delivery report (NDR). In hybrid mail flow from on-premises, the Hybrid Wizard changes the mail flow configuration so that some 5XX error codes are downgraded to less severe 4XX error codes.

EOP will automatically try to re-deliver queued messages approximately every five minutes until it can successfully deliver the message. If the message cannot be delivered within 24 hours, the message expires, and an NDR is generated. An administrator can configure the expiration timeout using the *Set-TransportConfig* cmdlet using any value between 12 and 24 hours. Reports on messages that have been queued for over one hour are available in the Exchange admin center under **Reports > Mail Flow > Queued Messages Report**.

Zero-hour Auto Purge (ZAP)

Despite all the efforts to fight spam and malware, malicious messages can escape the scrutiny of EOP's multiple scanning engines and be delivered to user inboxes. Many reasons could result in anti-malware code not classifying a message as spam or malware. Sometimes this is because the sender (still) has a good reputation, or perhaps because the spam or malware in the email was so new that the malware signature database in EOP is unable to recognize the vulnerability exploited by the attacker.

Zero-hour Auto Purge (ZAP) retroactively deals with malware, spam, and phish that penetrates defenses by continuously monitoring EOP for signature updates.

- If a new malware signature is detected that matches a signature in a previously delivered message, ZAP retroactively removes the attachment or message from each user's mailbox.
- If a new phish or spam signature is detected that matches a signature in a previously delivered message, ZAP retroactively takes the action of the anti-spam policy, which could include moving the message to quarantine, moving the message to the user's junk email folder, deleting the message, or to take no action.
- The opposite is true for false positives: ZAP can move misidentified messages back into the user's mailbox.

ZAP is enabled by default and can be turned off through PowerShell via the *Set-HostedContentFilterPolicy* cmdlet (for phish and spam) or the *Set-MalwareFilterPolicy* cmdlets (for malware). ZAP will only work if the following conditions exist:

1. The user's junk email filtering is enabled. By default, this is true.
2. The spam filter policy is configured to apply any action except *Add X-Header*. The default is to move messages to the junk email folder.

Note that mail flow rules, end-user inbox rules and safe sender lists take precedence over ZAP. This means that if ZAP filtering classified a message as phishing, an inbox rule or safe sender definition takes precedence, resulting for instance in messages getting delivered in an inbox instead of junk email folder.

To verify if ZAP is enabled, you can use the following cmdlets:

```
Get-HostedContentFilterPolicy | Select PhishZapEnabled,SpamZapEnabled
```

```
PhishZapEnabled SpamZapEnabled
```

True	True
------	------

Although the actions are transparent to the end-user, information remains for the administrator in the message's routing information. Look for the mention of **Zero-Hour Auto Purge (ZAP)** in the details of the message trace. If the information is there, it means ZAP intervened.

Directory-based Edge Blocking (DBEB)

By default, EOP will reject any message addressed to recipients it does not recognize, that is, for which EOP cannot find a matching mail-enabled object in the directory. This feature is known as directory-based edge blocking (DBEB) and offers several benefits, especially when a domain is under a dictionary attack by a spammer. DBEB is enabled for each authoritative accepted domain within Exchange Online and blocks messages at the perimeter network.

When you register a new domain with Microsoft 365, the domain is automatically configured as *Authoritative*, designating Exchange Online as your primary (and only) mail system. All valid recipients should then be represented by an object within Exchange Online, giving the system confidence that every recipient not matched against an existing object should be considered invalid. In turn, DBEB will reject messages addressed to invalid recipients, even before the message reaches the filtering layers. For this reason, messages rejected by DBEB are not visible in the message trace logs.

In a hybrid deployment, the transport service must be able to deal with email-enabled recipients homed on-premises. The same is true in a standalone scenario where EOP protects an on-premises organization. Directory synchronization is then used to synchronize on-premises recipients to Exchange Online. However, directory synchronization does not synchronize all recipient types. For instance, dynamic distribution groups are not synchronized. As such, [without extra configuration](#), messages will be rejected. Two options exist to avoid the dropping of messages for missing recipients:

1. Create a mail contact for the missing recipients. This will ensure that a valid recipient exists in the tenant, and DBEB will accept the message, after which it is forwarded to the on-premises environment.
2. Reconfigure the domain as an *Internal Relay* domain instead of *Authoritative*.

In the latter scenario, DBEB will be disabled automatically. However, messages for recipients not found in Entra ID will be forwarded to the on-premises organization or, if you do not have a dedicated connector, to where the MX record points. Thus, you might also need to configure an outbound connector scoped to the domain name. For instance, if you have configured the domain `office365itpros.com` as an internal relay domain, you should also create an outbound connector, as illustrated in the following PowerShell example:

```
New-OutboundConnector -Name "To On-premises" -RecipientDomains "office365itpros.com" -ConnectorType "OnPremises"-SmartHosts "onpremises.office365itpros.com" -UseMXRecords $False
```

When running the `New-OutboundConnector` cmdlet, it is important to include the `OnPremises` connector type. In this example, the connector is scoped to include only the `office365itpros.com` domain. However, you might have multiple relay domains. If you want to forward all messages for all accepted domains to a specific smart host without specifying each domain individually, you can use the `-AllAcceptedDomains` switch instead. This will ensure that a single connector is used for all known accepted domains.

```
New-OutboundConnector -Name "To On-premises" -AllAcceptedDomains $True -ConnectorType "OnPremises"-SmartHosts "onpremises.office365itpros.com" -UseMXRecords $False
```

The benefit of using the `AllAcceptedDomains` parameter is that new accepted domains are automatically included in the scope of the outbound connector.

Preset Security Policies

Preset security policies allow an organization to quickly deploy their message hygiene and Microsoft Defender for Office 365 policies with a few simple clicks. Microsoft provides two predefined security policies: standard and strict. Think of these as policies Microsoft is curating and managing on your behalf. All you need to do is select which users or groups of users you want to include in the preset policies. If your organization needs a custom policy, then the preset security policies will not work.

You can deploy these policies from the **Defender portal** and by navigating to **Policies and rules > Threat Policies > Preset security policies**. Clicking the **Manage protection settings** link (under either *Standard Protection* or *Strict Protection*) launches a wizard that allows you to add users to either policy.

Available options are:

- **All Recipients** to automatically allocate everyone in the tenant to a specific preset policy.
- **Specific Recipients** allows you to define users individually, through group membership, or through their primary domain. Assigning specific users is helpful if you want to divide users between standard, strict, and custom policies (remember that users you do not allocate to any policy will default to the built-in policy).
- **None** if you wish to leverage your own custom policies or have all users default to the built-in protection policy.

Note that it is possible to assign users to multiple policies at the same time. It's probably not best to do this because it would add unnecessary complexity (best to keep things simple). Still, if a user is assigned to multiple policies, policy precedence occurs in the following order.

1. Strict protection preset security policy.
2. Standard protection preset security policy.
3. Custom security policies (by order of priority).
4. Built-in protection.

Note: Built-in protection is on by default to provide Safe Attachments and Safe Links protection for all recipients. It can only be excluded for specific recipients. Later in this chapter, we will discuss configuring built-in protection.

The wizard also allows you to add users and domains to impersonation protection (more on this topic in the Anti-Phishing section) because these policies cannot be edited once added to their respective policy pages. For example, once you complete the **Manage protection settings** wizard, Exchange Online automatically creates an Anti-Phishing policy named *Standard Preset Security Policy* or *Strict Preset Security Policy* respectively. These cannot be edited directly, only through the **Manage Protection Settings** wizard. When you turn off the standard or strict security policy, their configuration will still be visible in the Anti-phishing section. When all users, groups, or domains have been removed from the policy, their Anti-phishing configuration will be deleted.

To disable the policy, navigate to the **Preset security policies** page and toggle the switch to the left (off). If you would rather delete the policy, click the **Manage protection settings** link under the policy you wish to delete. From the wizard, set the **Apply Protection** checkboxes to **None** on the *Apply Exchange Online Protection* and *Apply Defender for Office 365* protection pages. Click **Confirm**. The policy toggle will now be greyed out and removed from all policy screens.

You can learn more about preset security policies and how their management differs from Microsoft's [documentation](#).

Permissions

To create or modify Defender for Office 365 policies, an account must be a member of the *Hygiene Management* or *Organization Management* role group in Exchange Online. When your organization enables Microsoft Defender XDR Unified RBAC (URBAC), policy management can be delegated via the *Authorization and settings* | *Security settings* | *Core security settings (manage)* permission.

To manage Tenant Allow/Block Lists, you must have the *Organization Management*, *Security Administrator*, or *Security Operator* role assigned in Exchange Online. When Unified RBAC is enabled, delegation are configurable via the permission *Authorization and settings* > *Security settings* > *Detection tuning (manage)*.

Finally, for threat detection, a more granular Unified RBAC permission is available to manage Custom Detection, Alerts Tuning or Threat Indicators of Compromise rules in Defender using the *Authorization and settings* | *Security settings* | *Detection tuning (manage)*. This removes the requirement to use the Security Settings (manage) permission which offers other capabilities that are not needed for these management tasks.

Anti-Spam Protection

[Wikipedia defines email spamming](#) as sending unsolicited, undesired, or illegal email messages. It should come as no surprise that the various anti-spam features in EOP work together to:

1. Reduce the amount of spam that is delivered to a user's inbox; and
2. Reduce the number of false positives; messages are marked as spam but are not.

When an organization uses Exchange Online, spam filtering for inbound messages is enabled by default and cannot be disabled. However, an administrator has a multitude of options to adjust the settings for the different anti-spam features, including the ability to create custom antispam policies for different groups of users.

Anti-spam Inbound Policy

Inbound spam filtering can be accessed from the **Defender portal** and navigating to **Policies and rules** > **Threat Policies** > **Anti-spam policies**. The *Anti-spam policies page* lists the default three policies (which cannot be disabled) and any custom anti-spam policies you have defined.

To create a new policy, select **Create Policy** > **Inbound**. This will launch a wizard to guide you through the policy creation. The elements of that wizard are the same as if you edit a custom policy. We will cover that next.

To customize an existing policy, select that policy, and the properties pane will be displayed. The properties pane lets you customize what constitutes spam and what actions to take on that spam.

From the policy properties pane, you can perform the following actions:

- Enable or disable the policy with the **Turn on** or **Turn off** buttons. These buttons are absent for the default policy as it is always enabled.
- Change the processing order of the policy with the **Increase Priority** or **Decrease Priority** buttons. These buttons are absent from the default policy because it always has the lowest priority.
- Delete the policy with the **Delete policy** button. The default policy cannot be deleted.
- The **Edit description** link allows you to change the name and description of the policy. The description field is a great way to document any changes you have made to the policy. Note that the default policy cannot be renamed, so the name field will be greyed out if you are editing the default policy.
- **Edit users, groups, and domains** allow you to define the scope of the policy. This section is not present on the default policy because the default policy is the catch-all for anyone not defined in a

custom policy. Custom policies have priority over the default policy and are always processed first. If you have multiple custom policies that scope the same set of users, then the policies are processed in order of priority, where the lowest number (zero) is processed first.

- **Edit bulk email threshold & spam properties** allow you to configure what constitutes spam or bulk email (we will cover this in the next section).
- **Edit actions** define what actions to take on messages marked as spam, high confidence spam, phishing, high confidence phishing, and bulk mail. These actions are as follows:
 - **Move message to Junk Email Folder** delivers the message to the user but deposits the message into the user's junk folder. This could be a helpful training tactic as it may prompt the user to scrutinize the source and content of the message.
 - **Prepend subject line with text** delivers the message to the user but modifies the subject line. This is useful if you want to provide a visual cue to the user by prepending the subject line with BULK or SPAM as an example. Like moving the message to the user's junk folder, this is also a helpful training tactic to get the user to scrutinize the message.
 - **Quarantine message** prevents delivery of the message to the user and instead delivers the message to a quarantine. A quarantine policy dictates how the user interacts with a message in the quarantine. You can define a different quarantine policy for different types of mail. For example, the quarantine policy on high confidence phish could be much more restrictive than the policy on bulk email. Quarantine policies are discussed later in this chapter.
 - **Redirect message to email address** prevents delivery of the message to the user and instead delivers the message to someone else. This option is helpful for egregious phishing that you want to redirect to a SecOps mailbox for analysis.
 - **Add X-header** adds a header to the message. This header can be targeted by mail flow or inbox rules for additional actions.
 - **Delete message** does precisely as the name implies. The message is deleted and cannot be recovered.
 - **No action** does precisely as the name prescribes. The message is forwarded to the user without modification.
 - **Intra-Organizational messages to take action on** allows an administrator to dictate what happens when internal messages sent between users in a tenant contain spam or phishing. This setting could be particularly useful to protect an organization from an insider threat or if a bad actor has compromised a mailbox. By default, actions are taken on internal high confidence phishing and spam messages. An administrator can also choose to take no action on internal messages.
 - **Retain spam in quarantine for this many days** defines how long messages are kept in quarantine if the quarantine action and a quarantine policy have been selected.
 - **Enable spam safety tips** define whether safety tips should be displayed to users in an Outlook client. This is useful if you deliver spam to the user's mailbox (e.g., prepend subject or move to junk) but want to provide additional warnings about the message.
 - **Enable zero-hour auto-purge (ZAP)** allows Exchange Online to reach into a mailbox and take retroactive action on previously delivered mail. This is useful for zero-day exploits that are only identified after the delivery of mail to a user's inbox. You can also choose whether to enable ZAP for phishing messages, spam messages, or both. It is best practice to do the latter.
- **Edit allowed and blocked senders and domains** allow an administrator to define safe and blocked senders. These can be individual senders or an entire domain (we will cover this in a later section).

Note: Not all actions are available to each spam or phishing type. For example, *No action* is only available to an email defined as bulk. On the other hand, the only actions for high confidence phish are Quarantine and Redirect messages.

Spam Thresholds and Properties

As mentioned in the previous section, an administrator can fine-tune what constitutes spam and bulk mail by clicking the **Edit spam threshold and properties** link in an Anti-spam inbound policy.

The first control is a **Bulk email threshold** slider. This slider dictates the threshold at which Exchange Online Protection acts against bulk email. The recommended value is 7 on a scale of 1 through 9. For example, setting the threshold to 7 means any bulk email with a rating between 7 and 9 is subject to the bulk email action defined in the policy. Bulk email rated between 1 and 6 is not subject to the bulk action. If you want to suppress bulk email more aggressively, you can reduce the threshold to a lower value.

The rating is also known as a Bulk Complaint Level (BCL). EOP assigns a BCL rating on every message and applies that rating in the **X-Microsoft-Antispam** header in a field called "BCL." The field can have the values described in Table 6-4.

BCL Value	Meaning
0	The message is not from a bulk email sender.
1,2,3	The message is from a known bulk sender but is unlikely to generate many complaints.
4,5,6,7	The message is from a known bulk sender and can generate many complaints.
8,9	The message is from a known bulk sender and is likely to generate a high number of complaints.

Table 6-4: BCL header values

Note: The Bulk Senders Insight tool helps to fine-tune the BCL threshold to optimize the rating between false positives and false negatives. The tool is available at <https://security.microsoft.com/senderinsights>.

The inbound spam policy lets you increase the spam score on messages if any of the following are enabled:

- Image links to a remote website (rather than using embedded images)
- URLs containing IP addresses (rather than using a registered domain name)
- URLs that redirect to another port (rather than using the standard HTTP or HTTPS ports)
- URLs that use a top-level domain of BIZ or INFO

The inbound spam policy lets you mark messages as spam if any of the following are enabled:

- Messages with no content
- HTML code with IFRAME, FORM, EMBED, or OBJECT tags
- Messages with Javascript or VBScript
- Offensive words in the subject or body (this is a curated list by Microsoft that cannot be modified)
- Senders that hardfail SPF
- Senders that hardfail sender ID
- Backscatter (we discuss Backscatter later in the chapter)
- Messages received in specific languages or from specific countries

Each of these settings can be configured as **On** or **Off**. You should consider each of these options with care. Changing a setting might increase the likelihood of a message being marked as spam which tends to have a more significant impact on the productivity of your end-users than the occasional spam message.

Some settings also have the option to be configured in **Test** mode. Configuring a setting in test mode can take additional actions, such as adding an X-Header or BCC the message to a mail recipient. Testing is a great

way to determine whether these settings are operating in the way you expect before fully enabling them. While a setting is in test mode, the original email will be delivered to the user's inbox.

Spam Allow and Block Lists

You may have a scenario where you need to allow or block a sender or domain globally for the entire organization or a group of users. To allow or block a sender or domain globally for the entire organization, you can modify the **Anti-spam inbound policy (Default)**. From the pop-out window, select **Edit allowed and blocked senders and domains**. You can add entries to the allowed senders, allowed domains, blocked senders, or blocked domains lists using the *Set-HostedContentFilterPolicy* cmdlet.

If you want to scope different allowlists or blocklists for different sets of users, you must use multiple anti-spam policies; each scoped to a different set of users (whether by individual user, group, or domain).

When building allow lists, remember that Microsoft's [Secure by Default](#) approach will disregard customer-defined entries if the message is deemed to contain malware or is classified as high confidence phish. Instead, EOP routes these messages to the quarantine regardless of their presence in an allow list or modification by a mail flow rule (e.g., changing the message header to SCL -1 to bypass filtering).

Also, you should never add your own internal domains to the allow list. In fact, if you do this, Microsoft will disregard these entries (unless they pass DMARC) to protect you from spoofing attacks. If you do need another organization (such as a marketing firm) the ability to spoof you, then you should add these entries to the Tenant Allow/Block List (TABL) instead. We cover TABL and how to add entries in a later section.

Real-world: If migrating from another filtering solution to EOP, I recommend not migrating your allow and blocklists. First, based on the age of these lists, it is questionable which entries are still valid. Second, there is no direct apples-to-apples comparison regarding filtering solutions. Each solution is different. An action taken by one solution may not have been taken by another resulting in redundant entries in your allow/blocklists. When migrating to EOP, this is a good time to start with a clean slate, or, add these entries to the Tenant Allow Block List (TABL) with an expiration date.

Connection Filter Policy

The connection filter policy allows administrators to maintain a list of allowed and blocked IP addresses. You can access this IP list from the **Defender portal** and navigating to **Policies and rules > Threat Policies > Anti-spam policies > Connection filter policy (Default)**.

It is not possible to create a custom connection filter policy. This means the IPs in the connection filter policy impact all users. Therefore, it is impossible to scope IPs to specific users, groups, or domains like you can with other policies.

To add or remove an IP address, select the **Connection filter policy (Default)**. From the pop-out window, select **Edit connection filter policy** and add the individual IP addresses or address ranges.

Selecting the **Turn on safe list** checkbox includes a list of safe IPs vetted by Microsoft to your connection filter rules.

Anti-spam Outbound Policy

To stay on top of situations where an internal recipient sends spam messages, an administrator can change the default outbound policy to generate notifications when EOP deems a message suspicious or when a user is blocked from sending messages. In the **Defender portal**, go to **Policies and rules > Threat Policies > Anti-spam policies**. Here you will find any custom policies that have been created, as well as the default policy set.

In addition to the default outbound spam filter policy, you can create custom outbound spam policies to set different notification addresses and sending limits and apply them to specific senders. To create a new outbound policy, click **Create policy** and select **Outbound** from the drop-down menu.

Another reason for custom outbound policies is to define which users or groups can automatically forward messages outside the tenant. This policy does not impact automatic forwarding to internal recipients. Automatic forwarding is any messages automatically forwarded via an inbox rule, mail flow rule, or mailbox forwarding. This is an instrumental setting for organizations concerned with data exfiltration and needs to block some or all users from automatically forwarding messages outside the organization. You can set this policy to **On – Forwarding is enabled** or **Off – Forwarding is disabled**. The default is **Automatic – System-controlled**, which is a remnant of the transition to move from an allow forwarding default to blocking forwarding. Effectively it is the same as disabling forwarding.

The outbound spam filter policy allows you to define recipient limits for Exchange Online mailboxes. The maximum number of recipients you can set is 10,000. When using the default value of 0, the tenant defaults are used instead. We cover those in the Transport Limits section later in the chapter.

- **Set an external message limit** defines the maximum number of external recipients per hour
- **Set an internal message limit** defines the maximum number of internal recipients per hour
- **Set a daily message limit** defines the maximum number of recipients a mailbox can send to per day

The **Restriction placed on users who reach the message limit** dropdown has the following actions for a user who exceeds the external, internal, or daily message limits.

- **Restrict the user from sending mail until the following day** does precisely as the name implies. A user is blocked for 24 hours. An administrator cannot override this action. An administrator can monitor who is currently restricted from the **Defender portal** by navigating to **Incidents & Alerts > View Alerts** tabs.
- **Restrict the user from sending mail** blocks the user from sending mail until an administrator intervenes. An administrator can unblock a user from the **Defender portal** and navigate to **Review > Restricted Entities**. While the previous option is automated, this option allows more administrative control. This option may be preferred so an administrator can perform an analysis before allowing the mailbox to send again. This is a good option for organizations that want to restrict mailboxes that could be compromised by a bad actor.
- **No action, alert only** sends an alert when a mailbox exceeds a limit. As the name implies, no action is taken. This is a good way for an organization to test a policy before implementing one of the previous actions.

When Exchange Online blocks a user that continuously sends emails that it classifies as spam, the user will receive NDRs for outgoing messages that provide specific information on what they need to do to unblock their account. You can also configure the outbound malware settings in the malware policy to notify administrators when internal users are blocked.

You can also unblock an account by running the *Remove-BlockedSenderAddress* cmdlet. For example:

```
Remove-BlockedSenderAddress -SenderAddress Joe.Bowers@office365itpros.com -Reason "Account OK"
```

Anti-Spam Message Headers

EOP updates the Spam Confidence Level (SCL) header to show whether it considers a given message as spam. The SCL header consists of a single digit that does not explain why a message is considered spam. To provide administrators with additional information, EOP also inserts [two extra headers](#) into each message:

- **X-Forefront-Antispam-Report** is used to provide information on the anti-spam processing of the message; and

- **X-Microsoft-Antispam** provides information specific about bulk mail and phishing results.

The **X-Forefront-Antispam-Report** header consists of many different values, each revealing more information about the message, such as where it was sent from and the result of individual anti-spam tests. The following shows what this header typically looks like:

X-Forefront-Antispam-Report:

```
CIP:199.59.150.72;IPV:NLI;CTRY:US;EFV:NLI;SFV:NSPM;SFS:(8156002)(31570200002)(2980300002)(438002)(286005)(199004)(189003)(64016003)(53416004)(2616005)(19627405001)(110436001)(956004)(476003)(126002)(733005)(18926415007)(118246002)(85226003)(53386004)(606006)(336012)(6486002)(58536013)(106002)(106466001)(2160300002)(36756003)(246002)(16586007)(36736006)(486006)(33656002)(356003)(8676002)(7696005)(26005)(1096003)(620700001)(59450400001)(966005)(551544002)(33964004)(7636002)(84326002)(6306002)(25786009)(53946003)(236005)(4290100001)(146002)(7596002)(16003)(6916009)(270700001)(579004);DIR:INB;SFP:;SCL:1;SRVR:VI1PRO301MB2318;H:spruce-goose-ac.twitter.com;FPR:;SPF:Pass;LANG:en;PTR:spruce-goose-ac.twitter.com;A:0;MX:1;
```

At first sight, it may seem hard to make some sense of the information in the header. However, if you take a closer look, you will see that the header consists of several different fields of which the following give more insight into the anti-spam decision-making process:

- **CIP** has the IP address of the server that delivered the message to EOP. This IP address should be specified when using the IP allow or block list, and the IP address should be listed in the senders' SPF record.
- **IPV** field has two values and is used to decide whether the connecting IP was found on an IP allow list or not.
 - **IPV:CAL.** The message passed anti-spam filtering because the connecting IP address was found on an IP allow list.
 - **IPV:NLI.** The IP address was not found on any IP reputation list.
- **CTRY** specifies the likely country from where the message was received. EOP uses the connecting IP address to determine the country, which may or may not be the same as the original message.
- **SFV** field specifies why a message was marked as spam or not as spam and has several values:
 - **SFV:SFE.** Filtering was skipped, and the message was let through because it was sent from an address on an individual's safe sender list.
 - **SFV:BLK.** Filtering was skipped, and the message was blocked because it was sent from an address on an individual's blocked sender list.
 - **SFV:SPM.** The message was marked as spam by the content filter.
 - **SFV:SKS.** The message was marked as spam before the content filter processed the message. This includes the scenario when a mail flow rule marks a message as spam.
 - **SFV:SKA.** The message skipped filtering and was delivered to the inbox because it matched a safe sender or safe domain list in an anti-spam policy.
 - **SFV:SKB.** The message was marked as spam because it matched an anti-spam policy's blocked sender or blocked domain list.
 - **SFV:SKN.** Before the content filter processed the message, the message was marked as not spam. This includes the scenario when a mail flow rule marks a message as safe.
 - **SFV:SKI.** The content filter skipped processing the message because it was received by the on-premises environment and thus marked as *internal*.
 - **SFV:SKQ.** The message was released from quarantine and was sent to the intended recipients.
 - **SFV:NSPM.** The message was not spam and was sent to the intended recipients.
- **SCL** gives the Spam Confidence Level of the message and denotes the likelihood of the message being spam. The higher the number, the more likely the message is spam.
- **H** specifies the HELO or EHLO string of the connecting mail server.
- **SPF** specifies information about the SPF record lookup result for the message.

- **LANG** specifies the language the message was written in.
- **PTR** identifies the PTR record of the sending IP address (also known as the reverse DNS address).
- **ARC** shows the Authenticated Received Chain headers.
- **CAT** shows the category of the protection policy applied to the message. Multiple policies process a given message, but only the value corresponding to the highest priority one will be stamped in this header, as detailed in the [documentation](#).
- **SRV:BULK** specifies that the message was marked as a bulk email message.
- **SFTY** identifies if the message is a phishing message. The "safety" header value indicates the type of phishing, such as a URL, internal phishing, domain impersonation, etc. SFTY will also indicate if the setting was overridden with a safe sender or domain setting so you can determine if an email was allowed through because of your existing overrides.

The **X-Microsoft-Antispam** header looks like this:

```
UriScan: ;BCL:1;PCL:0;RULEID:(7020095)(5600026)(4605076)(4608076)(1401150)(8001031)(1402068)(71702078)
);SRVR:VI1PR0301MB2318;
```

And this header shows the following components:

- **BCL** specifies the Bulk Complaint Level of the message on a scale of 0-9. If the value is 8 or 9, the email comes from a sender that generates many complaints.
- **PCL** specifies the Phishing Confidence Level of the message on a scale of 0-9. If the value is 0-3, the email is unlikely to be phishing. An email with a value of 4-9 is likely to be a phishing email.

Message Tracing and Anti-Spam Headers

Often message tracing is used to understand why a message was marked as spam. You must request an Extended Trace report to receive details on why the message was marked as spam. The returned CSV file holds some extra data, including the anti-spam headers explained previously.

Once the search completes, open the CSV file and look at the *custom_data* field. Note that the example below was trimmed at the end for brevity.

```
S:AMA=SUM|v=0|action=|error=|atch=0;S:AMA=EV|engine=M|v=0|sig=1.193.3192.0|name=|file=;S:AMA=EV|engine=A|v=0|sig=201503191928|name=|file=;S:AMA=EV|engine=K|v=0|sig=19.3.2015
18:28:0|name=|file=;S:CFA=AS|sfv=NotSpam|rsk=Low|sc1=0|bc1=0|score=|sfs=(601004)|sfp=0|fprx=|m1c=|m1
v=|list=1|di=|rd=mail-db3on0089.outbound.protection.outlook.com|h=eemea01-db3-...
```

The field contains helpful information regarding the various filters that processed the message. For example, the data from the anti-malware agent is displayed after **S:AMA** (Anti-Malware Agent). Similarly, the anti-spam information is displayed after the **S:SFA** (Spam-Filtering Agent). Finally, information on mail flow rules is shown after **S:TRA** (Transport Rule Agent). Once you have extracted the data, you can use the information explained in the anti-spam message headers topic to understand the decisions of the anti-spam agent.

Anti-Malware Protection

EOP automatically scans inbound messages for malware. The term malware covers a variety of malicious items, such as viruses and spyware. EOP uses a multi-layered approach to detect malware using multiple anti-malware engines to scan messages for malicious code in the message body or attachments.

Unlike anti-spam configuration options, you cannot alter how EOP processes malware. However, you can control what type of attachments EOP drops automatically and how users receive notifications when an email contains malware or a blocked attachment type. The former option is known as Common Attachment Filtering. By default, EOP maintains a list of common attachment file types often associated with malware. Among other file types, the default attachment filter will block all .exe, .vbs, and .reg files. By editing the

default anti-malware policy or creating a new one, you can add or remove file types to control whether emails containing such attachments are quarantined automatically.

Note: Outlook maintains an independent file type block list. For a list of attachments blocked by the Outlook client, check this Microsoft article, [Blocked attachments in Outlook](#).

Custom Malware Policy

The default malware policy is sufficient to suppress malware for most tenants. However, if you need a different policy for a subset of your users, you can create a new malware policy. To create a new policy, navigate to the **Defender portal > Policies and rules > Threat Policies > Anti-malware** and click **Create**.

You can scope the custom policy to a subset of users based on the following conditions:

- **Users** (select a single- or multiple recipients).
- **Groups** (select one or more groups).
- **Domains** (match recipients in these domain(s)).

Using **Exclude these users, groups and domains**, you have the same matching options to exclude recipients from the policy.

Custom policies are processed in ascending order until a policy matches a user. For example, suppose a policy with a priority of 0 is only scoped to the finance department, and our user is in the legal department. In that case, matching fails, and processing moves to the next custom policy in ascending priority. Once a match is made, processing stops, and that policy is applied to the user. If the user can't be matched to any custom policies, they receive the default policy (which is always the last in priority).

Like the default policy, the custom policy lets you define common attachment types to block. This is useful if you want to have different common attachment blocks for different groups of users. For example, you may block fewer attachment types for your IT department than your general user population. By default, a new custom policy will have 50 executable types preselected to block. But you can select more than 200 common attachment types to block. If you need to block additional attachment types not included in the common attachment type filter, you must implement the block in a mail flow rule.

The policy also allows you to define what action to take on attachments identified in the common attachment filter. Actions include:

- **Reject the message with a non-delivery report (NDR)** will reject the message and send a failure notification back to the sender. Rejection means the email and its attachment are not recoverable, and no other action or notification can be taken. With this option, the recipient will not receive a notification of the block. This is the default option.
- **Quarantine the message** redirects the email and attachment to your quarantine. You can then define which quarantine policy will apply to that email and its attachment. The flexibility of this option depends on the flexibility of your quarantine policy. For example, this is the only option that could send a notification to the recipient or allow the message to be analyzed before release. We cover quarantine policies later in the chapter.

Apart from configuring a common attachment filter, you can also configure administrator notifications and toggle the ZAP feature (although it is best to keep this enabled).

Note: To notify users of quarantined malware, you must deploy a quarantine policy. A quarantine policy allows you to define user notifications and can be attached to the anti-malware policy.

Anti-Phishing

Phishing is an attempt to steal something of value from a company. This could range from the exfiltration of sensitive information (such as credit card numbers or personally identifiable information) to encouraging someone to take action that will result in some loss for them. Phishing typically involves impersonation, where a bad actor uses an email address that mimics a vendor, partner, customer, or employee to create trust. A typical example is a bad actor using an email address that impersonates a C-level executive requesting money be wired to what will invariably be the attacker's bank account.

The Anti-Phishing policy has several measures to protect companies from these attacks. Like other EOP policies, you manage the anti-phishing policy through the Defender portal. Navigate to **Policies and rules > Threat Policies**, then select **Anti-phishing**. From there, you can view and edit the default policy or click **Create** to make a new policy. The Default policy will always apply and cannot be deleted.

When configuring a policy, you have the following options:

- **Name and Description.** As you can create multiple policies for your organization, it is a clever idea to use a clear name or at least describe the intent of the policy.
- The **Users, Groups, and Domains.** This page specifies the users the policy will be run against. This can be set to all your users or a subset of your users, like all recipients in a specific domain or members of a distribution group. You can also exclude specific users from the policy.

Once these general settings are configured, you can configure the phishing threshold and protection settings for the policy:

- **Phishing email threshold** determines how aggressive machine learning should be when determining what a phish is. Values are from 1 – Standard to 4 – Most Aggressive. The Standard preset security policy (covered earlier) uses a value of 3. It may be best to start the threshold at 1 (Standard) and gradually increase it to meet your organization's needs.
- **Enable users to protect** and **Enable domains to protect** define what email addresses or domains are scrutinized while scanning for incoming phishing attacks. Typically, it would be best to protect high-value users like your C-level executives or people with high privileges within your organization. To protect all the domains belonging to the tenant, check **Include domains I own**. You can also **Include custom domains** that allow you to add a domain not included in your tenant or that of a partner, vendor, or customer.
- To ensure trusted domains or senders, such as a partner, vendor, or customer, are never treated as impersonators, you can optionally add them to the **Manage trusted senders and domains** allow list.
- Enable/disable **Mailbox Intelligence (Recommended)** to allow the policy to use Microsoft Graph for user email signals. This helps ensure that people you have communicated with before are not treated as spoofed senders.
- Enable/disable the use of **Intelligence for impersonation protection (Recommended)** to enable enhanced impersonation. This also allows actions to be taken on emails impersonating a user.
- Enable/disable **Spoof Intelligence (Recommended)**, which allows you to define who can send mail on behalf of your domains (for example, a bulk mailing service). While the option to enable this setting is part of the anti-phish policy, the allow list is maintained through **Policies & rules > Threat policies > Tenant Allow/Block Lists > Spoofed Senders**.

Real-world: The terminology in the wizard is a little ambiguous. “Enable users to protect” and “Enable domains to protect” do not define to whom a policy applies. Instead, these are the email addresses and domains for which anti-phishing will compare the P2 header information of incoming messages. So, for example, you configure `ceo@office365itpros.com` as a user to protect and `office365itpros.com` as a domain to protect and apply the policy to all users in your organization. Then, whenever a message is received from `ceo@offfce365itpros.com` (note the look-a-like address), that message will be flagged as a phishing attempt if the person receives an email from that address for the first time.

With the phishing thresholds defined, we can now turn to the actions in our policy. An action is performed whenever a phishing threshold has been met.

Note: Some actions may be greyed out if the corresponding phishing threshold isn’t enabled on the prior page of the wizard. For example, “*If message is detected as impersonated user*” is greyed out, click the **Back** button, select **Enable users to protect**, and define a list of users to protect.

The following actions are available:

- **If message is detected as an impersonated user, impersonated domain, or if mailbox intelligence detects an impersonated user**, you can perform the following actions from the respective drop-down.
 - **Redirect message to other email addresses**. This is useful if you need to send the message to an internal security response team for analysis. The redirection will not deliver the message to the original recipient.
 - **Move message to the recipients’ Junk Email folders** does precisely as the action describes. With proper email security training, delivering the message to the junk email folder is a great way to have users pause and scrutinize the email. This ensures mail is still delivered in the case of a false positive, which could be reported by the user while instilling caution that the message ended in junk email.
 - **Quarantine the message** takes the junk folder concept one step further by keeping the message out of the user’s mailbox and off their devices. The added benefit of the quarantine is that it is out of sight and, therefore, out of mind. Generally, users only review the quarantine to look for a solicited message they have not received. As phishing emails should be unsolicited, the user will not miss the email they did not expect to receive. Depending on the quarantine policy, proper email security training is still needed, as users can release the message to their inbox.
 - **Deliver the message and add other addresses to the Bcc line** sends the suspect message as a blind carbon copy to an internal security response team and delivers it to the intended recipient. This is useful when you have an internal security team to review (mildly) suspicious messages but do not want to delay delivery to the original recipient. Note that this action delivers to the original recipient’s inbox.
 - **Delete the message before it’s delivered** deletes the message during transport. This is a definitive action, and the message is irrecoverable. Any analysis must be done using the information in message trace logs.
 - **Don’t apply any action** means that no action applies to the message.
- **Honor DMARC record policy when the message is detected as spoof** determines whether an administrator wants to honor the sender’s DMARC policy. If disabled, the sender’s DMARC policy is ignored, and the actions taken on spoofed messages are governed by the **If the message is detected as spoof** dropdown (described below). If enabled, the senders DMARC policy is considered when an explicit DMARC failure occurs, however, the failure actions can be overridden through two new dropdowns that become available.

- **If the message is detected as spoof and DMARC Policy is set as p=quarantine** allows an administrator to override the default behavior of the sender's DMARC policy. If the message fails the DMARC check and the sender's intent is to have recipient quarantine failed messages, Microsoft's default action is to quarantine the message. An administrator can override this by sending the failed message to the user's junk mail folder.
 - **If the message is detected as spoof and DMARC Policy is set as p=reject** allows an administrator to override the default behavior of the sender's DMARC policy. If the message fails the DMARC check and the sender's intent is to have the recipient reject failed messages, Microsoft's default action is to reject the message. An administrator can override this by sending the failed message to the quarantine. An administrator may prefer this action as a rejected message is purged from the tenant, whereas a quarantined message could be analyzed, and a manual action performed.
- **If the message is detected as spoof**, it only has the actions **Move message to the recipients' Junk Email folders** and **quarantine the message** from the list above. This means you must take corrective action on a spoofed message.
 - **Safety Tips and indicators** determine what the user may see in their Outlook client. Safety Tips are available across all Outlook clients, including Outlook for Windows, Outlook for Mac, Outlook on the Web, and Outlook Mobile.
 - **Show first contact safety tip (Recommended)** identifies when you receive an email from someone you know but are using a different email address than what EOP has seen before.
 - **Show user impersonation safety tip, and Show domain impersonation safety tip** informs the user whenever a user or a domain is being impersonated by the sender.
 - **Show user impersonation unusual character safety tip** informs a user when an unusual character is detected in the sender's address. An example of this is a [homoglyph attack](#). A homoglyph attack is when a bad actor swaps a character from one alphabet for a similar or identical-looking character from another. For example, a bad actor may swap out the letter "e" from the Latin alphabet for the letter "е" from the Cyrillic alphabet (Unicode 435). To the human eye, these look identical but are very different.
 - **Show (?) for unauthenticated senders** changes the picture (or initials in the absence of a picture) in the sender's profile card to a question mark. This is when Exchange Online cannot authenticate the sender via sender authentication (e.g., SPF, DKIM, & DMARC). This is explained in greater detail in the *Safety Tips* section below.
 - **Show "via" tag** shows a safety tip if the from address (displayed to the user in their email client) does not match the mailfrom attribute in the message header. An example of this safety tip could be john.smith@contoso.com on behalf of jane.doe@office365itpros.com.

Note: The first contact safety tip previously required the presence of a mail flow rule to apply *X-MS-Exchange-EnableFirstContactSafetyTip* to the email header. While Exchange Online still supports this header, it is no longer required to display a first contact safety tip.

You can also manipulate the anti-phishing policy with PowerShell using the *Set-AntiPhishPolicy* and *Set-AntiPhishRule* cmdlets. For example, run the following command to retrieve a list of all anti-phishing policies.

Get-AntiPhishPolicy

To enable mailbox intelligence for the default policy, use the following command.

```
Set-AntiPhishPolicy -EnableMailboxIntelligence $True -Identity "Office365 AntiPhish Default"
```

If you enabled an anti-phishing policy when Microsoft first released the feature, a default policy called "*Office365 AntiPhish Default*" is in your tenant. In these circumstances, it is probably best to update the default policy and remove your policy and let the default policy do the work.

Anti-Spoofing

Spoofing is when someone sends messages using your email domain through an email system other than your primary (internal) messaging system. Often a malicious attacker tries to impersonate a legitimate person's email address to convince the recipient of the message to perform actions helpful to the attacker. The concept of spoofing is not new, and over the last few years, another form called "insider spoofing" has emerged and quickly gained popularity with attackers. Insider spoofing, sometimes referred to as a spear-phishing attack, is no different from regular spoofing, except that the message appears to be coming from an internal recipient, making it much harder for the recipient to figure out if a message is invalid or not. Typically, insider-spoofing impersonates highly-ranked employees (such as a C-level executive) and targets other employees to convince them to take action, such as sending a wire transfer.

Fighting spam and phishing is an ongoing task. A newer form of insider spoofing is where user accounts are compromised (maybe due to a phishing attack), and the spoof emails are sent from compromised accounts. The malicious actor logs in as the user and sends an email from a compromised user's real mailbox. Protection against this attack includes using multi-factor authentication with appropriate password policies and protections.

Although features such as SPF records, DKIM signing, and DMARC help to detect and repel spoofing attacks, only a minority of organizations have successfully adopted some or all these features, so gaps are left for attackers to exploit.

To detect spoofed messages, Microsoft processes each incoming message, inspects the various TO and FROM headers in the message, and compares the values. For example, several checks are performed if a message is sent to someone inside your organization and the FROM field matches an internal domain. If the message was sent from inside the organization or received through a host or service that may send messages on your behalf (for example, because the host is present in the SPF record), the message is deemed legitimate. However, if the message does not pass any of these tests, or if it was received by a host with a bad reputation, the message could be considered spoofed.

When the anti-spoofing feature intervenes to mark a message as spam, the value **SFTY:9.5** is added to the **X-Microsoft-Antispam** header, which also has information about the results of other scanning engines:

X-Microsoft-Antispam: UriScan:;BCL:0;PCL:0;RULEID:(71701004)(71702002);SRVR:BY2PR12MB0565;SFTY:9.5

Besides the anti-spoofing protection described above, Microsoft offers the Spoof intelligence feature.

Spoof Intelligence

There can be legitimate reasons that justify the spoofing of your email domain(s). For instance, if you have hired an external marketing company to send electronic surveys to your customers or employees or if you have a business application that sends notification emails to your internal users. However, differentiating between legitimate and malicious attempts to spoof your domain is not easy, especially because features like SPF, DKIM, or DMARC are often not used or poorly implemented. It is also true that none of these features protect your tenant when accounts are compromised.

Spoof intelligence controls which senders can send messages on behalf of your organization. The Spoof Intelligence dashboard is located at <https://security.microsoft.com/spoofintelligence>. Alternatively, you can access the dashboard by opening the **Defender portal** and navigating to **Policies & rules > Threat Policies > Tenant Allow/Block Lists > Spoofed Senders > View Spoofing Activity**. Using the Spoof Intelligence dashboard, you can allow or revoke a specific sender's permission to spoof your domain. Additionally, when you open the dashboard, you can see a list of senders known to have sent messages on behalf of others (including your domains) in the past 7 days.

Additional details help you determine if a sender should be allowed to spoof messages. For instance, the policy tries to show who the actual sender is next to the information about which users were spoofed. EOP obtains the specific sender information by looking at the reverse DNS (PTR) record of the sending server's IP address. If no PTR record is found, the IP address is displayed in the report.

Note: Legitimate senders often have a PTR record that enables Exchange Online to look up and display the sender's hostname or domain name information. Extra caution is advised if no PTR record is found, as it is highly likely that the sender should not be allowed to spoof your domain. Unfortunately, even malicious senders can have a PTR record!

Although you cannot stop a (malicious) sender from trying to spoof your domain, the Spoof Intelligence feature controls how EOP handles incoming emails. If a sender is not explicitly allowed to spoof one or more users within your organization (domain), messages from that sender will be marked as spoofing attempts, and users will be notified of the fact.

From the Spoof Intelligence dashboard (Figure 6-8), you can change how EOP handles the spoof by selecting **Allow to spoof** or **Block from spoofing**.

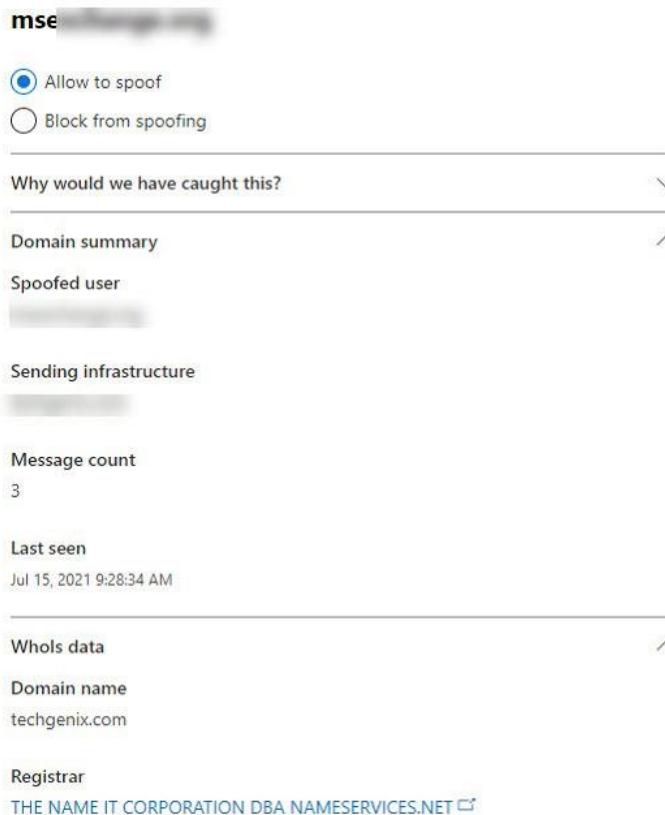


Figure 6-8: Spoof Intelligence Dashboard Action Pane

You can also control the Spoof Intelligence through PowerShell. This is done via the Tenant Allow/Block List (TABL) cmdlets. To get a list of current entries in the Tenant Allow/Block List, we leverage the `Get-TenantAllowBlockListSpoofItems` cmdlet. In the example below, we have two static entries in our list. These two entries identify that `contoso.com` and `fabrikam.com` have been allowed to spoof `office365itpros.com`.

```
Get-TenantAllowBlockListSpoofItems | Format-Table SpoofedUser, SendingInfrastructure, SpoofType, Action, Identity
```

SpoofedUser	SendingInfrastructure	SpoofType	Action	Identity
office365itpros.com	contoso.com	External	Allow	7323b926-3334-8d4a-ee09-b94e35f3467
office365itpros.com	fabrikam.com	External	Allow	24f1b37a-766e-0cc1-ca88-7e487732914b

Let's change *contoso.com* to a block rather than an allow. To change an existing entry in the Tenant Allow/Block List, we can leverage the *Set-TenantAllowBlockListSpoofItems* cmdlet. In the example below, we take the ID for *contoso.com* (retrieved from the *Get-TenantAllowBlockListSpoofItems* output above) and specify a block action against the *office365itpros.com* domain.

```
Set-TenantAllowBlockListSpoofItems -Identity office365itpros.com\Default -Action Block -Ids  
7323b926-3334-8d4a-ee09-b94e35f3467
```

After making the changes, you can use the *Get-TenantAllowBlockListSpoofItems* command again to verify that the changes were applied correctly. If you need to add a new entry rather than modify an existing entry, you leverage the *New-TenantAllowBlockListSpoofItems* cmdlet. Similarly, you can remove an entry with the *Remove-TenantAllowBlockListSpoofItems* cmdlet.

In addition to the anti-spoofing features designed to stop spoofed messages from being delivered to the user inboxes, administrators can also request the **Spoof Mail Report**. The report is accessible through the Defender portal or PowerShell. To get the report in PowerShell, use the following command:

```
Get-SpoofMailReport | Select Date, Direction, Action, SpoofedSender, TrueSender, SenderIP
```

```
Date      : 14/04/2016 0:00:00  
Direction : Inbound  
Action    : GoodMail  
SpoofedSender : Boss.Man@office365itpros.com  
TrueSender  : hubspot.com  
SenderIp   : 50.31.57.0/24  
  
Date      : 11/04/2016 0:00:00  
Direction : Inbound  
Action    : CaughtAsSpam  
SpoofedSender : CEO-of-the-company@office365itpros.com  
TrueSender  : someonlinemarketingservice.com  
SenderIp   : 1.2.3.4/24
```

The report displays information about spoofed messages, like the information in the Spoof Intelligence policy. In addition, it can show you what spoofed messages were received, whom they were impersonating, and who sent the message. In the above example, the top message was sent by an authorized service, as that message was classified as **GoodMail**.

The report serves multiple purposes. First, it helps you understand how many messages inside your organization are spoofed. More importantly, it tells you which account is being spoofed most and can reveal spear-phishing attempts. Secondly, the report enables you to generate a list of hosts sending messages on your behalf. You can then use this list to verify if authorized senders are correctly configured and whether you have represented them on your SPF records, lowering the likelihood of them being marked as spam.

Message Quarantine

By default, Exchange Online protection routes low-confidence spam and phish to the users' junk email folder and high confidence spam and phish, plus messages containing malware, to the quarantine. The quarantine is a vault where marked messages are held instead of delivered to a user's mailbox. Messages can remain in quarantine for up to 30 days, after which Exchange removes the messages permanently. Depending on your quarantine policy, end users can perform any number of actions against quarantined messages or, possibly, no actions, requiring them to ask for administrator intervention.

Quarantine Policy

Quarantine policies in Exchange Online Protection allow you to define what end users can and cannot do in the message quarantine portal. For example, you could define a policy that allows some users to release messages to their inbox and block other users from performing this action. Similarly, you could define

different quarantine policies for different threat policies. For example, you could send users quarantine notifications on messages containing spam but not send notifications on messages containing malware.

To view the default policies or create a custom policy, open the **Defender portal** and navigate to **Policies and rules > Threat Policies > Quarantine Policies**.

The default policies *DefaultFullAccessPolicy* and *AdminOnlyAccessPolicy* cannot be modified. The *DefaultFullAccessPolicy* allows users to release the message to their inbox, block the sender, delete the message, and preview the message. In contrast, the *AdminOnlyAccessPolicy* does not allow any user actions. The intention of assigning *AdminOnlyAccessPolicy* to a threat policy is to only allow administrators to act on messages. This is useful when you do not want users to release harmful messages, such as high confidence phishing messages.

To create a custom policy, select **Add custom policy** from the **Quarantine Policy** screen. Give the policy a name that describes its purpose and click **Next**. On the *Recipient Message Access* page, choose either **Limited Access** (which includes all permissions listed below except allowing recipients to release a message) or **Set Specific Access (Advanced)** to specify actions users can perform in the portal. These actions include:

- **Allow recipients to release a message from quarantine** allows the user to release the message to their inbox. This box controls whether the user sees this button in both the quarantine portal and the quarantine notification.
- **Allow recipients to request a message to be released from quarantine;** allow a user to request a message released to their inbox by an administrator. An administrator is notified based on the settings defined in the alert policy **Defender portal > Policies and rules > Alert Policy**. By default, this alert goes to quarantine administrators, security administrators, and members of the organization's management role. This box controls whether the user sees this button in both the quarantine portal and the quarantine notification.
- **Delete** allows the user to delete the message from the quarantine portal. The message is not delivered to the user's inbox. This box only controls the button in the quarantine portal.
- **Block sender** allows the user to block future messages from the sender. This box controls whether the user sees this option in the quarantine portal and the notification.
- **Allow sender** allows the user to allow future messages from the sender. This box controls whether the user sees this option in the quarantine portal and the notification.
- **Preview** allows the user to view the message from the quarantine portal without needing to release it to their inbox. This is useful if the user needs to review the message before acting.

Note: The *Allow recipients to release* actions are not honored if applied to an antimalware policy. Users will never be able to release messages with malware regardless of the quarantine policy settings.

With your actions selected, click **Next**. The quarantine notification page allows you to **Enable** whether users should receive quarantine notifications. Using our prior example, where we have a different policy for spam versus malware, we may want users to receive notifications for spam in quarantine but not for messages containing malware. Once you have picked your notification setting, select **Submit** to create the policy.

Quarantine Settings in Protection Policies

To change the quarantine policy assigned to a threat policy, navigate to the **Defender portal > Policies and rules > Threat Policies** and click on the threat policy you wish to configure. You can assign a quarantine action (and quarantine policy) to spam, high confidence spam, phishing, high confidence phishing, bulk mail, user impersonation, domain impersonation, spoofing, malware, and safe attachments. For this example, let's modify the default anti-spam policy. To do this, select **Anti-spam** from the threat policies screen and select **Anti-spam inbound policy (Default) policy**. From the pop-out screen, select **Edit actions**. Under the **Actions** section. Select **Quarantine message** from the **Spam message action** dropdown. When we pick the

quarantine action, another drop-down is displayed to allow the selection of the quarantine policy. Let's select **DefaultFullAccessPolicy** and click **Save**. This selection will allow users to perform the following actions on low confidence spam: release the message to their inbox, block the sender, delete the message, and preview the message.

Customizing Quarantine Notifications

The quarantine policies allow us to define whether users receive quarantine messages or not. If you want to change the frequency of those messages or customize the look and feel of the quarantine notification, navigate to **Policies and rules > Threat Policies > Quarantine Policies > Global Settings**.

From the *Quarantine Notification Settings* screen, you can make the following changes.

- **Sender Display Name** allows you to customize the sender shown in the message notification.
- **Specify sender address** allows an organization to configure its own internal email address as the quarantine notification sender. This is useful for organizations that want to train their user base to look for quarantine notifications from a specific sender or if the organization wants to use an established and trusted email address to send these notifications.
- **Subject** allows an organization to customize the subject of the quarantine notification. Like the sender address, an organization may customize this to an established subject line to aide user awareness and training.
- **Disclaimer** allows you to add your custom disclaimer to the bottom of the quarantine notification.
- **Choose language** allows you to customize display names and disclaimers in multiple languages. Select the required language from the drop-down and click **Add** to add it to the active set shown under **Click the language to show the previously configured settings**. This field is also where you can switch between languages to change its display name and disclaimer fields in the fields above. To remove a language, click the **X** next to its title in the active languages box.
- **Use my company logo** replaces the Microsoft logo on the quarantine notification with your company logo. You can upload your company logo via the **Microsoft 365 Admin Center** by navigating to **Settings > Org Settings > Organization Profile > Custom themes**.
- **Send end-user spam notifications** provides a drop-down where you can specify the frequency a quarantine digest is sent. Notifications can be sent as often as every 4 hours. At the other end of the scale, you can set notifications to arrive weekly. It is worth noting that this notification only occurs when new messages arrive in quarantine. Setting the notification interval to every day is a good balance for end-user experience.

Releasing Messages from Quarantine

Several ways exist to release a message from the quarantine. The fastest and easiest way for a user is to click the **Release** link for the message in the notification digest email, as shown in Figure 6-9. End users with full access to a shared mailbox will also perform quarantine actions for messages sent to the shared mailbox. If the user does not have full access permissions, they cannot perform quarantine actions. A user can also click **Review** to preview the message from the quarantine portal before releasing it. From the quarantine portal, the user can also click **Release**.

Note: The buttons in the notification email (and quarantine portal) will differ depending on the quarantine policy you have assigned to each quarantine action in your threat policies. If the quarantine policy is set to **Allow recipients to release a message from quarantine**, the **Release** button is available to end-users.

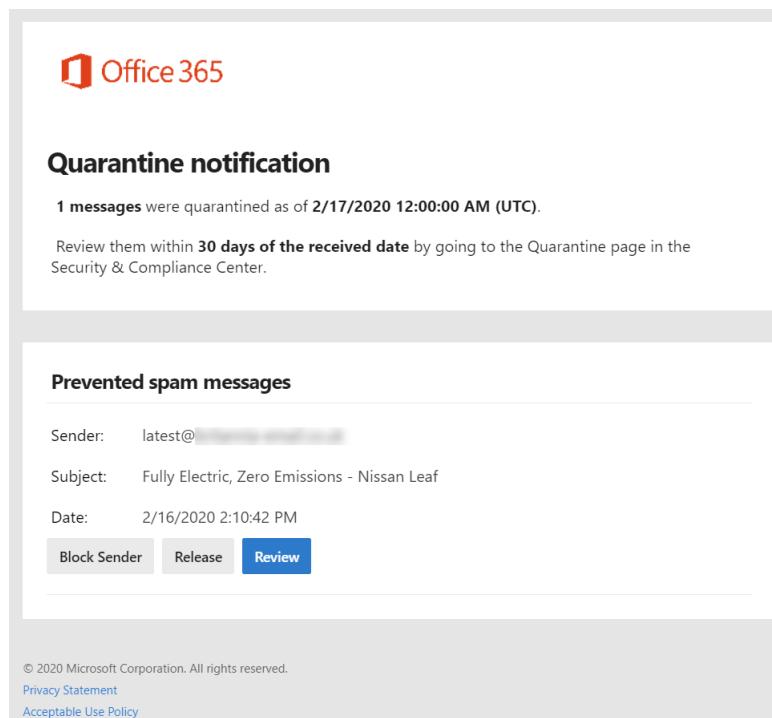


Figure 6-9: A notification that a user has potential spam to handle

Users can log in to [the quarantine portal](#) to access quarantined messages instead of waiting for Exchange Online to send notifications. To access the quarantine, launch the Defender portal and navigate to **Review > Quarantine**. To access quarantined messages held for their mailbox, the user must have a valid Microsoft 365 account and an Exchange Online or EOP license. After signing into the portal, the user sees a list of any quarantined messages waiting for resolution. This list includes quarantined messages for shared mailboxes where the user is a delegate. The user can search the list based on sender, subject, or, less likely, the message ID. In addition, filtering options such as the date and time the message was received can be applied to focus on specific messages, or the quarantine reason such as Phishing, Malware, Transport Rule, or File Type Block. Depending on the quarantine policy, the user can take the following actions on any message:

- **Release:** Exchange delivers the message to the user's inbox, and they have the option to report it as a false positive to Microsoft.
- **Request release:** Sends a message to an administrator requesting the message be released on behalf of the user.
- **View message header:** Lists the routing information and other message properties with a link to the [Microsoft Message Header Analyzer tool](#).
- **Preview message:** Displays a safe copy of the message.
- **Delete messages:** Messages are automatically removed from quarantine on their expiration date. However, a user can temporarily or permanently delete a message from the quarantine by using the delete messages button. A user may opt to do this to triage their quarantine more effectively.
- **Block sender:** Adds the sender to the user's blocked sender list. Remember that the user must sign-in to the Security Portal after clicking Block Sender to make the change. By default, blocked senders are excluded from the quarantine view. When the view is set to include displaying blocked senders, the will also be an option to remove senders from the blocked sender list after selecting a message from the blocked sender.
- **Allow sender:** The sender is added to the user's allowed sender list. For end users, this is only available if no administrator override exists. If one exists, the user can view override details.

After a message is released—either by the user, quarantine manager, or administrator—the Release by field will be set to the email address of the user or admin responsible for the release. If the message was released by the system, this will also be indicated.

Administrators can work with quarantined messages and files received for anyone in the organization. To do this, the administrator can open the **Defender portal** and navigate to **Review > Quarantine** (Figure 6-10). The interface is like the end-user interface. The difference is that an administrator can see quarantined emails or files for the entire organization and has more options to manage a message. End users may see similar interface when they manage their personal quarantine.

Administrators can take the following actions on messages:

- **Release:** Exchange delivers the message to the user's inbox. The admin can also release the message to additional users, report the email as a false positive to Microsoft, and add the sender (including any URLs or attachments) to the Tenant Allow/Block List (TABL).
- **Approve or Deny release:** Allows an admin to approve or deny a user request to release a message from quarantine (see *Request Release* in the previous list).
- **Delete messages:** Messages are automatically removed from quarantine on their expiration date. However, an admin can temporarily or permanently delete a message from the quarantine by using the delete messages button.
- **Preview message:** Displays a safe copy of the message.
- **Submit for review:** Allows an administrator to report a false positive or false negative to Microsoft. This pops out a form populated with the message ID and recipient and allows the administrator to provide the reason for the submission. The reason can be one of the following:
 - **I've confirmed it's clean** to indicate the message is a false positive. You are also given the option to allow similar messages for a certain period. For this, a time-limited entry will get added to the Tenant Allow/Block List. More on TABL later in this chapter.
 - **It appears to be clean** to indicate the message looks clean. Microsoft will perform additional analysis to decide if the message really is clean.
 - **It appears to be suspicious** to indicate the message looks suspicious. Microsoft will perform additional analysis to decide if the message really is a threat.
 - **I've confirmed it's a threat** to indicate the message is a false negative. The administrator can further classify the message as **spam**, **phish** or containing **malware**.

For false positives, the admin will also have the option to add the submitted entries to the TABL using their characteristics. These exceptions can be configured for a period of 1, 7 or 30 days, or until a specific date. An additional option for false positives is to create an exception which will expire 45 days after the exception was last used by mail flow. The latter should prevent stale exceptions littering TABL.

- **View message header:** Lists the routing information and other message properties with a link to the [Microsoft Message Header Analyzer tool](#).
- **Block sender:** The sender is added to the user's blocked sender list.
- **Share email:** Allows an administrator to forward copies of potentially malicious emails to other users. This is useful if you want to forward a specific message to your internal security team for review. Keep in mind, however, you are forwarding potentially harmful content.
- **Download message:** Allows you to download a copy of the potentially malicious email (in EML format) for offline review. Before downloading, you will be prompted to provide a reason for this action and will be required to create and confirm a password to protect the content. Keep in mind, however, you are downloading potentially harmful content.

<input type="checkbox"/> Time received	Subject	Sender	Quarantine reason	Release status	Policy type	Expires
<input checked="" type="checkbox"/> Oct 28, 2022 2:00 AM	[EXTERNAL EMAIL - USE CAUTION] Hi	wendyaranadas@sheldonsd.com	Phish	Needs review	Anti-spam policy	Nov 27, 2022 1:25:...
<input type="checkbox"/> Oct 28, 2022 1:55 AM	[EXTERNAL EMAIL - USE CAUTION] Hi	wendyaranadas@sheldonsd.com	Phish	Needs review	Anti-spam policy	Nov 27, 2022 12:52:...
<input type="checkbox"/> Oct 28, 2022 1:30 AM	[EXTERNAL EMAIL - USE CAUTION] Hi	wendyaranadas@sheldonsd.com	Phish	Needs review	Anti-spam policy	Nov 27, 2022 12:35:...
<input type="checkbox"/> Oct 27, 2022 6:00 AM	Plastic Toolmaking & Moulding Services in ...	plastic18@plasticmolds8.top	Spam	Needs review	Anti-spam policy	Nov 11, 2022 5:59:...
<input type="checkbox"/> Oct 27, 2022 12:00 PM	Re:Re: Bill of lading	vibha_garg@hotmail.com	Phish	Needs review	Anti-spam policy	Nov 25, 2022 11:42:...
<input type="checkbox"/> Oct 26, 2022 5:10 PM	RE: first feedback after having your book su...	tony.redmond@office365itpros.com	Phish	Needs review	Anti-spam policy	Nov 25, 2022 4:13:...

Figure 6-10: Viewing quarantined messages in the Microsoft 365 Defender portal

To grant administrative access to the quarantine, use the *Quarantine* role or the *Quarantine Administrator* role group within the Defender portal. In addition, members of the *Security Administrators* and *Organization Management* role groups also get access to the admin quarantine. For organizations that have enabled Unified RBAC, quarantine management can be delegated via the *Security operations* \ *Security data* \ *Email quarantine (manage)* permission.

In larger environments, the message quarantine might hold thousands of messages. Working with large quantities of messages through the Defender portal might prove challenging. PowerShell can be a better fit for such scenarios, especially when performing bulk actions on messages in the quarantine. For instance, using the *Get-QuarantineMessage* cmdlet, an administrator can look for specific messages in the quarantine. For example, this query looks for high confidence phishing messages:

```
Get-QuarantineMessage -QuarantineTypes HighConfPhish | Select ReceivedTime, SenderAddress, Subject, Expires
```

ReceivedTime	SenderAddress	Subject
07/08/2020 00:35:43	pat@casey.net	tony.redmond@ You have 3 messages
04/08/2020 09:45:38	mundobabyplaza@hotmail.com	Request For Quotation 800014
29/07/2020 18:12:09	account-update@amazon.com	#External: Amazon security alert: Sign-in from new

To release a message from the quarantine, the *Release-QuarantineMessage* cmdlet can be used. This example looks for messages addressed to a certain user that are marked as spam and releases them for delivery. It's unwise to release high confidence phishing messages unless you are certain that the messages are OK.

```
Get-QuarantineMessage -RecipientAddress James.Ryan@Office365itpros.com -QuarantineTypes Spam | Release-QuarantineMessage -ReleaseToAll
```

Configuration Analyzer

One excellent feature of Exchange Online Protection is the configuration analyzer. The analyzer makes recommendations on how to improve a tenant's email security posture, further protecting an organization from bad actors, malware, and spam. The analyzer can be accessed by navigating to **Policies and rules** > **Threat Policies** > **Configuration analyzer**.

The **Standard recommendations** tab shows how your custom policies match the *Standard Protection* preset security policy. Similarly, the **Strict recommendations** tab measures your custom policies against the *Strict Protection* preset security policy.

In Figure 6-11, the analyzer recommends changing the bulk email threshold in our *Default* policy. It shows our current value of 7, the date the value was set, and the recommended change to 6. To apply the

recommendation, we would select the checkbox on that row and click the **Apply recommendation** button. Alternatively, we could click the **View Policy** button to go to the properties of the *Default* policy.

Configuration analyzer

The Configuration analyzer can help identify issues in your current configuration and help improve your policies for better security. Want to automatically stay updated with recommendation configuration? Switch on [presets](#), [Learn more](#).

Recommendations	Policy group/setting name	Policy type	Current configuration	Last modified
<input checked="" type="checkbox"/> Move to Junk Email folder	Office365 AntiPhish Default	If email is sent by someone who's not allowed to...	Anti-phishing	Quarantine message
<input type="checkbox"/> Enable DKIM	micr...@outlook.com	DKIM signing	DKIM	false

Figure 6-11: Configuration Analyzer Recommended Changes

The **Configuration drift analysis and history** tab is an audit log of all changes to each threat management policy, whether modified via the policy or by clicking the adopt button through the recommendations screen.

Tenant Allow/Block Lists (TABL)

While Exchange Online Protection usually makes the right decision about things like spoofing, sometimes you need to explicitly allow (or block) specific senders from spoofing mail recipients or domains in your tenant. With Tenant Allow/Block Lists (TABL), you can configure up to 1,024 spoof pairs. A pair is a spoofed domain or user and the actual sending domain, user, or IP address. Currently, only IPv4 addresses are supported. Support for IPv6 addressing is rolling out and scheduled for completion at the end of October 2024.

To manage the spoofing pairs, go to **Policies and rules > Threat Policies > Tenant Allow/Block Lists** in the **Defender** portal. Click the **Spoofed Senders** tab and click **Add**. From the *Add new domain pairs pane*, add a unique spoof pair to each row, where the first entry on the row is the entity to be spoofed, and the second entry identifies the sender, domain, or IP doing the spoofing. You can then specify whether this is an **Internal** or **External** spoof and whether to **Allow** or **Block** the spoof. Click the **Add** button when you have your desired configuration.

Similarly, you may have a situation where you need to allow or block a specific file, URL, domain, or email address.

With standard Exchange Online Protection licensing, you can allow up to 500 domains or email addresses and block up to 500 domains or email addresses. These limits are increased if you are licensed for either Defender for Office 365 Plan 1 or Plan 2. Tenants with Plan 1 are granted up to 1,000 allow entries and 1,000 block entries for domains and email addresses. Tenants with Plan 2 are granted up to 5,000 allow entries and 10,000 block entries. In addition, all plans grant a block of up to 500 files and up to 500 URLs (or URL patterns).

To block a domain or email address, from **Tenant Allow/Block Lists** select the **Domains & addresses** tab and click the **Block** button. Add each email address or domain (including top-level domains) as a comma-separated list (or add one entry per row). From here, you can also specify the duration of the block (should you wish it to expire or be permanent) and a reason for the block.

To allow a domain, top-level domain, or email address, use the **Submission** feature (discussed later in this chapter) and select the **It appears clean** option. This action submits the email to Microsoft for review and allows you to add an *Allow* entry into the Tenant Allow/Block List. Like blocking a sender, you can also set an expiration and a reason for the allow entry.

Once the *Allow* entry is created, it can be managed from the Tenant Allow/Block List page. For time-limited TABL entries, the **Remove on** column on the Domains & addresses tab will show when the entry expires. For

Block entries, the **Last used date** shows the time the entry was last triggered by the filtering system, i.e. referenced in mail transport or clicking of the URL. Specific for Allow entries, you can also set the entry to expire 45 days after the Last use date.

To block URLs, you need to list a URL or a pattern. For example, you could include just office365itpros.com, or if you needed to include all the subdomains, you could specify ~office365itpros.com. It is also possible to block top-level domains. For example, if you wanted to block any URL with a top-level domain of .biz, you would enter it with the format of *.biz/*. This would then block any domain with a .biz extension.

Managing file exceptions is a little bit harder. You must provide the SHA256 hash of the file to add it to the list. Many tools can compute the hash. Microsoft's [documentation](#) for this feature shows you an easy way to compute the hash value using certutil.exe.

Identifying and reporting messages

The following sections outline how users can manage their safe sender and block lists, how users and administrators report junk and phishing messages to Microsoft, and how safety tips help users identify suspicious emails.

Informing users with Safety Tips

To increase visibility to end-users on messages containing potential threats such as spam, malware, spoofing, or phishing, Microsoft includes visual cues in messages to warn users when they encounter potentially dangerous content. Safety tips work in much the same manner as mail tips. These cues are tags inserted into messages by EOP as it processes emails before delivery to end-users. For example, whenever a message is considered suspicious, Exchange inserts a safety tip. Similarly, if a message is received from a trusted sender, the notification will make this clear. EOP supports four safety tips (red, green, yellow, and grey). Table 6-5 lists the types of safety tips supported by EOP.

Color	Safety Tip	Condition
Red	Suspicious. These messages are likely to contain phishing scams and should not be opened.	EOP detects the presence of a known phishing message or the characteristics of the message, such that EOP considers the message likely to be a scam. See this article for an explanation of why messages are assigned red safety tips.
Yellow	Unknown. The message is spam.	EOP has scanned the message, and it has failed the standard anti-spam tests.
Green	Trusted. The message is from a trusted source.	Microsoft has a list of domains owned by trusted sources (such as itself). Messages from these domains are considered trusted.
Grey	Safe. An informational tab that indicates the message has been marked safe by the tenant or user.	The message is from a domain considered to be safe by the tenant (for example, the IP address for the server is in the IP allowed list), or on the user's safe senders list, or it was put in the user's Junk Email folder and subsequently moved back to the Inbox to indicate its safe status.

Table 6-5: Types of safety tips

Safety tips can be enabled or disabled for a tenant by updating the policies used by EOP. For example, the `Set-HostedContentFilterPolicy <name> -InlineSafetyTipsEnabled` command is used to configure safety tips via PowerShell. We do not recommend that you disable Safety Tips.

Unauthenticated Sender Safety Tip

The unauthenticated senders feature works in conjunction with the analytics gathered by Exchange Online to figure out if the sender is who they say they are or if the sender is spoofing someone else. This is known as sender authentication. If the message sender fails the authentication tests (SPF, DKIM, or DMARC), Exchange

replaces the initials/photo shown next to the sender's display name with a question mark. However, a failure does not automatically result in an icon replacement because Microsoft uses extra technologies to help determine if a message is safe even though it failed authentication.

Not every message that fails to authenticate is malicious. However, you should be careful about interacting with messages that cannot authenticate if you do not recognize the sender. Or, if you recognize a sender that normally does not have a '?' in the sender image but suddenly starts seeing it, that could signify that the sender is being spoofed.

The sender authentication feature is enabled via the **Show (?) for unauthenticated senders for spoof** option in the anti-phish policy. While this feature is enabled by default, we do not recommend that you disable it.

Exchange Online will never mark senders in your safe sender list as spoofed – even if they are spoofed – and this also applies for messages marked as safe due to mail flow rules, anti-spam policies, and the safe senders specified in those policies as well. Administrators can deal with false positives caused by sender authentication by adding the sender and sending infrastructure to the anti-phishing Spoof Intelligence insight.

For more information on authenticated senders, check the following [Microsoft article](#).

How Users Mark Mail as Junk, Phish, or Safe

Exchange Online allows users to control specific junk email settings themselves. Within Outlook and OWA, a user can do the following:

- Mark a sender as safe
- Mark a sender as blocked
- Add a recipient to a safe-recipient list

When a user right-clicks a message and selects **Mark as Junk** in OWA, the message is automatically moved to the Junk Email folder, and the sender is also added to the blocked sender list. More specifically, the information is stored as part of the mailbox configuration in the following AD attributes:

- msExchSafeSenderHash
- msExchSafeRecipientHash
- msExchBlockedSenderHash

This information is accessed by EOP and taken into consideration when processing messages. Messages from safe senders are automatically marked as "not spam." In contrast, messages from blocked senders will be forwarded to the user's junk email folder or the quarantine, depending on the policy configuration. It is important to note that EOP will not honor the safe sender list if EOP considers a message to be high-confidence phishing. This is because a domain or sender that has been safe-listed might become compromised, leading to a possible compromise of the recipient's mailbox. If you need to have a sender or domain bypass this test, you can still do so with a mail flow rule that adjusts the SCL header on the message.

These attributes are synced back to the on-premises organization in a hybrid deployment. This is especially important in hybrid deployments where the MX records points to the on-premises organization instead of EOP, and these attributes are to be considered by the Exchange on-premises environment.

The write-back capability ensures that Edge Transport servers correctly process messages for cloud-based mailboxes. Note that when an on-premises mailbox is protected by EOP (or a cloud-based mailbox by Edge Transport servers), there can be a delay of at least thirty minutes between a user adding an address to one of the lists and the information being available to EOP or the Edge Transport servers. This is due to the directory synchronization interval and the worker process in Exchange Online that reads the safe and blocked sender lists and writes them to the Exchange Online directory.

In addition to the safe and blocked sender lists, users can configure client-specific settings. In Outlook Classic, the **Junk Email Options** allow you to:

- View or edit the **Safe Senders**, **Safe Recipients**, and **Blocked Senders** list.
- Toggle the setting to automatically **trust email from my contacts**.
- Adjust in-client junk email filtering through the general **Options** tab.
- Block messages from specific **countries or regions**. For instance, if a user selects to block messages from Canada (CA), all messages from a domain ending with .ca will be marked as spam.
- Block messages written in an **unfamiliar language**.

Under the **Options** tab, you will find settings that control Outlook's built-in junk email filter. The selection there should always be set to **No Automatic Filtering** for mailboxes leveraging EOP. Otherwise, you will find Outlook making decisions based on its older and less reliable junk email filter. You can also configure Outlook to remove junk email rather than move it to the Junk Email folder.

Note: EOP uses only the safe senders, safe recipients, and blocked sender lists. All other features are client-specific and will only affect messages after being delivered to the user's mailbox. However, it should be noted that EOP also provides country- and language-based protection, which can be configured separately in the anti-spam filter policy.

To access the corresponding settings in OWA, click **Settings** (cog wheel) and then **View all Outlook settings**. From there, select **Mail > Junk email**. Apart from the aforementioned lists, you will find settings to restrict message delivery to only people from your trusted lists, to consider all contacts as trusted, and to control whether messages you mark as junk are automatically reported to Microsoft.

Note: Outlook has separate tabs for Safe Senders and Safe Recipients, but OWA only shows a single list called **Safe Senders and domains**. If a user makes changes via OWA options, their Safe Recipients list is merged with the Safe Senders list, and that list is copied into both Safe Senders and Safe Recipients in Outlook. Also, any Safe Senders and Safe Recipients from an internal domain are removed automatically from these lists shortly after being added.

Lastly, administrators can review or configure junk email settings on a user's behalf via the *Get-MailboxJunkEmailConfiguration* and *Set-MailboxJunkEmailConfiguration* cmdlets. It is important to note that if you disable the junk email rule using *Set-MailboxJunkEmailConfiguration*, this only disables the user's individually defined junk email lists and junk email settings stored in their mailbox. Junk emails identified by EOP will still be processed and delivered to the user's mailbox as dictated by the anti-spam policies defined in the tenant.

How Users Report Junk and Phishing Email

Microsoft develops many of the features to combat spam and malware based on data harvested from inbound emails delivered to Exchange Online and Outlook.com. Using machine learning techniques, Microsoft distills valuable information from the data to improve the efficiency of its protection features. However, because spammers continually introduce new techniques to bypass checks, it is impossible to guarantee that every threat will be detected. As a result, sometimes messages slip past EOP. Users can report these messages (also known as false negatives) by sending them to Microsoft for analysis. If Microsoft's Spam Analysis Team confirms that the message meets the spam classification criteria, they update the EOP filtering systems to block similar messages in the future. Similarly, users can also report false positives. These are messages that EOP detected as spam but are not.

Tenant administrators can allow users to report messages to Microsoft, report messages to the tenant administrator, or both. When users believe they have received a phishing email, they can use the **Report** drop-down option in the OWA or Monarch clients to report the message to Microsoft (Figure 6-12). From this

menu, the user can either report the message as phishing or junk. Users can also report messages received by shared or delegated mailboxes as long as they have Send As or Send on Behalf permissions.

When you use **Report Junk**, Exchange copies the message to Microsoft and moves the original email to the user's *Junk Email* folder. If you accidentally report the message, you can undo the action by finding the message in the *Junk Email* folder and selecting **Not Junk** from the **Report** drop-down menu. This will report the error to Microsoft and restore the message to the Inbox.

When you use **Report Phishing**, the message is reported to Microsoft and moved to the user's Deleted Items folder.

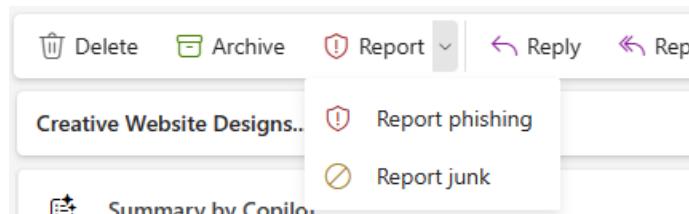


Figure 6-12: Marking a Phishing message

Note: Starting August, 2024, the report button will be available in the monthly enterprise/current channel build of Outlook Classic, followed by the other channels in their standard release timing. OWA and the New Outlook for Windows clients already include the report button. If you use an older Outlook Classic build, you must deploy the *Report Message* add-in to your users. For more information on deploying the add-in, check [Enable the Report Message or the Report Phishing add-ins](#).

Both the addin and the native report button are controlled in the **Microsoft Defender portal** by navigating to **Settings > Email & Collaboration > User reported settings**.

From this page, you can define what reporting button to use. This is useful if you want to disable the built-in Microsoft reporting button and only present a third-party reporting button to your users. Two reporting buttons can cause user confusion.

If you select the built-in Microsoft reporting button, additional options appear on the page, including who to send the phishing and junk reports to. Configure the option by selecting one of the following options from the **Send Reported Messages To** drop-down:

- **Microsoft only** – All user submissions go directly to Microsoft for analysis. This is the default option.
- **My reporting mailbox only** – All user submissions go to a mailbox of your choosing. This is useful when you want to review all user submissions internally. Note that as an administrator, it is still possible to submit these messages to Microsoft for review. This option is helpful if you are concerned about sensitive data being sent to Microsoft and want to triage user submissions first. Note that *My Reporting Mailbox Only* is the only option for government and DoD tenants. If you select this option, you will be asked to specify a destination mailbox to receive the user reports.
- **Microsoft and my reporting mailbox** – All user submissions go to both Microsoft and a mailbox of your choosing. This is useful if you want to do your own analysis in addition to allowing the user to send the message to Microsoft for review. If you select this option, you will be asked to specify a destination mailbox to receive the user reports.

Note: Messages reported by users sent to the reporting mailbox receive a prefix for the subject to indicate their status. The prefix and thus status can be "Junk:" (prefix was "1|"), "Not junk:" (was "2|") or "Phishing:" (was "3|"). Reported Teams messages are prefixed with "Security risk:".

You also have the option to **customize Email notifications**. This option controls notifications sent to the end user after they reported a message, and the admin triaged their message or it was investigated by automated investigation and response (AIR). The latter is enabled by checking **Automatically email users the results of**

the investigation. After checking, admins can provide custom body and footer for phishing, junk, and clean messages, as well as specify a custom e-mail address to use as sender, as well as have the Microsoft logo replaced with the tenant branding logo used in notification messages.

Additional options on this page define other user experience-related options, such as whether to leverage confirmation prompts, customize success notifications and emails, and allow users to submit messages directly from their quarantine portal. For more information on configuring user submission settings, check [this article](#).

How Administrators Report Junk and Phishing Emails

The **Submissions** feature, found under the **Actions & Submissions** section of the Defender portal, allows administrators to upload information to Microsoft about messages that should have been blocked or false positives. The information can be the message (in .eml or .msg format), Message ID, a URL found inside the message, or an attachment.

The administrator then decides if the message is clean, a threat, or looks like one of these classifications. This is similar to the options provided when submitting messages from the Submissions page to Microsoft for analysis, as mentioned in the Quarantine Portal section, as illustrated in Figure 6-11.

Submit to Microsoft for analysis

We will review the information and use what we've learned to improve detection. We will let you know our findings. [Learn more](#)

Select the submission type *

Add the network message ID or upload the email file *

Add the email network message ID ⓘ

e.g. 9ad939f4-30f9-4c03-ac2b-4fd107d40b78

Upload the email file (.msg or .eml)

Choose at least one recipient who had an issue * ⓘ

Why are you submitting this message to Microsoft? *

I've confirmed it's clean

It appears clean

It appears suspicious

I've confirmed it's a threat

Choose a category

Spam

Phish

Malware

Figure 6-13: Creating a new submission for a false negative email

After submitting the findings to Microsoft, you can view the analysis results. The report also provides information about any policies that have acted on the message and examines any URLs and attachments found within. For example, a common scenario is that the message was allowed by a personal exemption by the end-user or via a mail flow rule.

The page also allows you to review user-submitted messages under the **User reported messages** tab. You can also start an investigation (if your tenant has the necessary Microsoft Defender for Office 365 Plan 2 license). Additional information about the Submissions feature is available in the [online documentation](#).

Delisting Your IP Address from the Office 365 Block List

Although Microsoft does not add an IP address to the block list for no reason, sometimes this happens erroneously. Common causes for an IP address to be listed is because it was repeatedly found as the source of spam, malware, spoofed, or phishing messages. In addition, you will find yourself on the list if you have an open relay or do not pay enough attention to outbound messages.

When your IP address appears in the block list, messages sent to Exchange Online recipients fail, and a Delivery Status Notification (DSN) goes to the sender with the following information:

- 1.7.1 *Service unavailable; Client host [1.2.3.4] blocked using Blocklist 1; To request removal from this list, please forward this message to delist@microsoft.com*

Like most third-party block list providers, you can use a web form to request removal from the Block List. The form is located at <https://sender.office.com> and takes you through three simple steps:

1. You must enter your email address and the IP address to be delisted.
2. A verification email is sent to the email address.
3. If the verification succeeds, you can continue delisting the IP address.

Once the delist request has been received, the IP address is typically removed within 30 minutes.

Using a Third-Party Filtering Solution Before EOP

Organizations often consider that they can gain added protection by deploying other email filtering solutions alongside EOP. Although this approach is practical from a technical perspective, it could adversely affect some anti-spam features, including IP throttling, IP blocklists, bulk mail filtering, or anti-spoofing in EOP. This is also why Microsoft recommends against using an added filtering solution with EOP.

For instance, EOP relies on IP throttling to prevent the delivery of spam messages: when a message is received from a new IP address, EOP throttles the incoming connection by issuing an SMTP 450 error. The error indicates a transient error, which means the sending server should retry later. Legitimate servers usually retry the connection, while most spammers do not. The reason for not retrying is quite simple: the added effort to interpret the error message and then try again later is often too much trouble for spammers. Even though the feature does not stop a spammer from sending messages, it greatly reduces spam delivered to Exchange Online mailboxes. However, when a second filtering solution is used in front of EOP, all messages delivered to your organization originate from a single set of IP addresses. This renders the IP throttling feature useless.

When Exchange Online detects that your MX record does not resolve to EOP, it automatically disables some EOP anti-spam features. An example of one feature they disable is IP throttling. EOP also cannot perform IP reputation blocks, sender authentication checks such as SPF and DMARC, spam filter rules, and more.

Therefore, it is imperative to ensure that the third-party solution you choose performs all the same tests as EOP. For example, if you have a security device as your first hop that does not do anti-spam filtering, Microsoft will also not perform all the anti-spam filtering they could otherwise do.

Real-world: It is unsupported to use a third-party filtering solution in a hybrid deployment for messages sent between the on-premises organization and Exchange Online. This is because a third-party filtering solution can remove important message headers, like the *X-MS-Exchange-Organization-AuthAs* header, from the message.

When the *X-MS-Exchange-Organization-AuthAs* headers are no longer present, problems can occur. For example, messages might not be recognized as originating from within the same organization. This could lead to internal messages being treated as spam or an external out-of-office message being returned

rather than its internal counterpart. For this reason, messages must flow uninterrupted between Exchange Online and the on-premises Exchange servers.

If additional filtering is desired, or you have the requirement to terminate all inbound connections in the perimeter network, you must use a Microsoft Exchange Edge Transport server. The Edge Transport server is the only additional filtering solution that authenticates like an Exchange server in the same manner as the internal Exchange servers. You can continue using a third-party filtering solution to process all external messages entering and leaving your organization to and from the internet.

Enhanced Filtering for Connectors

If you use an email filtering solution or email gateway other than EOP, you must configure Enhanced Filtering for Connectors. The Enhanced Filtering for Connectors option allows tenants whose MX record is not resolved to Exchange Online to determine the true source of an email. It is used when messages are routed via on-premises servers or a third-party cloud filtering service, both of which make the email seem to come from that source instead of its true origin. Knowing the actual email source, you can fine-tune your spam, phishing, and mail flow rules.

Enhanced Filtering, or skip listing, is a complex routing configuration. In a hybrid scenario, the recommended solution is to route the email directly to EOP by setting the domain MX record to Exchange Online. This is not always possible, however. For example, if you are migrating to Exchange Online, your MX record will resolve to your on-premises Exchange organization until later in the migration project. During this period, or if your MX record remains configured to a third-party email filtering solution, you must ensure that EOP is aware of your internal IP addresses (if routing via on-premises) or the IP address range(s) belonging to the third-party filtering service. This includes any analysis or intermediary SMTP servers in your routing pipeline after spam, phishing, and malware filtering services.

When EOP is aware of the IP ranges belonging to other services you trust, it skips those IP address ranges in the SMTP headers to determine the true source of the email. Microsoft's Intelligent Security Graph has information about the trustworthiness and reliability of these sources based on their previous history. This information can be applied to inbound emails. When Enhanced Filtering is not configured, the information in the previous step in the received SMTP header is all that Exchange Online knows about the previous sender, which is likely to be your on-premises infrastructure or the last server in the third-party cloud infrastructure.

To enable Enhanced Filtering, open the **Defender portal**, go to **Policies and Rules > Threat Policies > Enhanced Filtering**, or use <https://security.microsoft.com/skiplisting>. Enhanced Filtering can be enabled for a subset of users for test purposes. Any email addressed to recipients outside your test user pool will not be processed through Enhanced Filtering. Therefore, if you want to test the feature and some of your pilot users receive email using multiple proxy addresses, you should include all the addresses in the Enhanced Filtering configuration. Once your pilot is complete, you can update the configuration to apply to the entire organization.

When you configure Enhanced Filtering by associating the IP addresses of trusted network ranges with the relevant connector, email domain authentication (aka DKIM, DMARC, and SPF) will improve. Now that EOP can determine the source of the email, it can check this information against anti-spoof technologies and explicitly allow, quarantine, or reject email based on the sender infrastructure.

Two SMTP headers are added to messages after Enhanced Filtering is enabled. These are:

- **X-MS-Exchange-ExternalOriginalInternetSender** shows the true source of the message. This should not be in the IP range of the on-premises servers or your third-party filter. If it is, you have not configured skip listing correctly.

- **X-MS-Exchange-SkipListedInternetSender** shows the true source of the message and is used for reporting purposes.

Enhanced Filtering replaces custom mail flow rules often used to prevent double filtering. These mail flow rules set the spam confidence level (SCL) to -1 so that messages skip EOP filtering.

Microsoft Defender for Office 365 (MDO)

Microsoft Defender for Office 365 (MDO) is a set of features designed to answer zero-day exploits or new methods built by attackers to bypass and fool protection systems such as EOP. In the current threat landscape of email, having a zero-day malware and link protection service that operates on both internal and externally sourced emails should be considered by all tenant administrators as a required purchase. By providing features such as safe attachments, safe links, safe documents, and advanced anti-phishing controls, MDO can significantly increase your organization's security posture.

Microsoft Defender for Office 365 is included in Microsoft 365 E5 and Office 365 E5 and is also available as an add-on. Like most other services available in Microsoft 365, you can enable the added protection for your entire organization or just a select group of users. However, until you buy at least one license, Microsoft Defender for Office 365 is unavailable through the Defender portal.

In hybrid deployments, messages sent between on-premises Exchange servers and Exchange Online bypass MDO scanning. This is because the connectors created in the hybrid configuration set the Spam Confidence Level (SCL) header to -1 to tell EOP to bypass any additional anti-malware or anti-spam filtering.

Built-in Protection

Built-in protection is a baseline default policy defined by Microsoft for all Microsoft Defender customers. This policy enables a base configuration for Safe Links and Safe Attachments and is applied to every user in your tenant.

This policy cannot be disabled, but users, groups, or domains can be excluded from the policy by navigating to **Policies and rules > Threat Policies > Preset security policies** and selecting **Add exclusions** under the *Built-in protection* section.

It is not recommended that users be excluded from the built-in policy. Instead, if you wish to give your users a different configuration, either create custom Safe Links and Safe Attachment policies and assign those custom policies to those users or assign those users to the strict or standard preset security policies. These policies will always take precedence over the built-in protection policy, so there should be no need to exclude users from the built-in protection.

If a user is assigned to multiple policies, policy precedence occurs in the following order.

1. Strict protection preset security policy
2. Standard protection preset security policy
3. Custom security policies (by order of priority)
4. Built-in protection policy

The built-in protection policy ensures every user has Safe Link and Safe Attachment protection in the event they are accidentally removed from all custom or preset security policies.

For a comprehensive list of built-in protection policy settings and how they differ from the standard, strict, and default custom policy settings, check the [Microsoft documentation](#).

Safe Attachments

Safe Attachments deliver extra protection against zero-day malware. EOP uses multiple anti-virus scanning engines to process incoming (and outgoing) messages. These engines use "signature" files to detect known viruses and malware. You can compare it to a database that has the essential characteristics of a virus to enable the anti-virus engine to recognize an instance of the virus when it occurs in email. The problem with this approach is that when a new virus is created, time is needed for security researchers to decipher the virus, construct its signature and update the database. During this period, messages holding the virus will likely penetrate past standard scanning and arrive in user mailboxes. When MDO is enabled, messages with attachments are rerouted to a virtual sandbox environment where the content is subjected to a "behavioral analysis" based on machine learning. During this process, the attachment is run or opened, scanned, and observed to determine whether it is malicious or not. If no suspicious activity is detected, the message is released for delivery to the user's mailbox.

Each of the MDO features works as an 'add-on' to EOP. This means that messages are only subject to additional scanning or processing if none of the other EOP features have found anything suspicious about the message. In the case of Safe Attachments, a message is only rerouted when EOP's anti-malware engine successfully processes the message and does not detect a threat. The rerouting of the message itself is fully transparent to the end user.

In addition to protecting attachments in inbound emails from external sources, Safe Attachments file protection is also available for Microsoft Teams, SharePoint Online, and OneDrive for Business. The option to enable MDO for mailboxes is driven by a policy that applies to whomever the policy is configured for. The option to enable MDO protection for OneDrive for Business, SharePoint Online, and Microsoft Teams is a global setting.

Configuring a Safe Attachments Policy

To create a policy, navigate to **Policies and rules > Threat Policies > Safe Attachments** in the Defender portal and click **Create**.

When configuring a policy, you have the following options:

- **Name and Description.** As you can create multiple policies for your organization, it is a clever idea to use a clear name or at least describe the intent of the policy.
- The **Users, Groups, and Domains.** This page specifies the users the policy will be run against. This can be set to all your users or a subset of your users, like all recipients in a specific domain or members of a distribution group. You can also exclude specific users from the policy.

Once these general settings are configured, you can configure the actions for the policy:

- **Safe Attachments unknown malware response** defines what action Safe Attachments should take when a potentially dangerous attachment is detected. The available options are *Off*, *Monitor*, *Block*, or *Dynamic Delivery*.
 - **Off** disables any action taken by safe attachments.
 - **Monitor** can be helpful when you are first enabling the feature because it allows you to assess how well Safe Attachments are performing. Although unsafe attachments are still delivered to the recipient, all the reporting features are available.
 - **Block** will quarantine both the attachment and the message.
 - **Dynamic Delivery** will ensure that the message body is delivered instantly while the attachment is being analyzed. Once the attachment has been processed, it is reattached to the original message. Should the attachment be considered malware, it will quarantine the attachment.

- **Quarantine Policy** defines which quarantine policy to use when the Block, or Dynamic Delivery actions place an attachment and message into quarantine.
- **Enable Redirect** is a great option when you want to send a copy of a malicious attachment to a security operations center (SOC) for further review. Caution is advised if you do decide to open the delivered attachment. Note that the redirect option only works when the Safe Attachments policy is set to *Monitor* mode.

To enable Safe Attachments protection for SharePoint, OneDrive, and Microsoft Teams, you need to click **Global settings** at the top of the page and toggle the switch **Turn on Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams**.

Note: It can take up to 30 minutes before a new policy, rule, or setting is fully active.

Safe Documents

Dubbed **Safe Documents for Office clients**, the feature leverages Microsoft Defender for Office 365 to scan documents before allowing users to open them outside of protected view mode in Microsoft 365 desktop applications (Version 2004, build 12730 or greater). This feature is technically not part of Microsoft Defender for Office 365 and requires a Microsoft 365 E5 or Microsoft 365 E5 Security license.

Safe Documents prevents users from opening a document received from an external source until the document can be checked against Microsoft's threat defense cloud. Since there are certain privacy considerations at play, the feature is not enabled by default. Still, it can be toggled on from the **Safe attachments > Global settings** pane by selecting **Turn on Safe Documents for Office Clients**.

Safe Links

Phishing messages often include malicious links that redirect users away from legitimate sites to sites under the attacker's control. When EOP processes these messages, a high probability exists that these links are already flagged as malicious, and the message will be caught by the anti-malware or anti-spam engine. Unfortunately, this is not always the case. Sometimes, malicious links are not known yet, or perhaps the link was not yet activated when the message was processed. The weakness in this approach to securing messages is that it only protects messages at delivery. If an attacker updates a malicious web page after it has been delivered, traditional anti-malware protection can do nothing. Usually, this is where computer-based security software kicks in, but with more users responsible for their own devices under BYOD policies, organizations do not always control what endpoints are used.

The *Safe Links* feature analyzes links at the time they are clicked. To do so, it checks the link in real-time in selected clients or rewrites any hyperlinks in email messages when EOP receives them. Safe Links will, by default, only rewrite links if the message's sender is from an anonymous source, like external senders, and if the link is in the FQDN format. For example, a link with only a server name (no dots) is not rewritten. Rewriting links for internal senders is disabled by default but can be turned on in the Safe Links policy. This protects against a scenario where a mailbox's login details are compromised. A malicious actor uses the compromised mailbox to send bad links that appear to come from a trusted sender.

For Safe Links in email, the link in the message body is rewritten during delivery in EOP. Once the email is delivered to the recipient, the underlying link looks like this:

<https://eur02.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.spamlink.contoso.com%2F&data=02%7C01%7Cgareth%40nbconsult.co%7C321a4fc34c294a14231908d754b5f730%7C69daf98459d5415ba9b1aa3b30b4a677%7C0%7C637071012816511154&sdata=eYvY4TOvBEPJIOZvilGeNclnlXIX0q0nQeFfLF9tjAc%3D&reserved=0>

Note: The base URL (*.safelinks.protection.outlook.com) will always be the same, the information that follows varies on the message and the link(s) within that message.

Outlook hides the link and shows a popup with the target URL so that users do not see the complicated nature of the rewritten link. Opening the message in a non-Microsoft client or an older Microsoft client will still show the rewritten link. When Safe Links is enabled for Office applications, the user does not see the full link. Instead, they only see the destination the link takes the user to if the target is not flagged as malicious.

Outlook also protects URLs in message subjects, URLs in nested email attachments, and URLs in S/MIME signed messages. This is achieved by processing the link at the time of the click, even if EOP did not rewrite the URL. For example, links within S/MIME-protected messages are not rewritten; therefore, the message is not rendered invalid while the link is still protected. Indeed, any text that looks like a hyperlink that is made clickable by Outlook is now protected, even though it is not seen as a link when being processed by EOP. No URL rewriting is done; the protection exists solely within the Outlook client.

When a user clicks a link in a message, the Safe Links feature checks the reputation of the remote host (website) against a set of spam lists. This usually happens within a matter of seconds and does not produce any significant delays for the user. When a website is not on one of the spam lists, the user is redirected to the requested website. However, when a match is found, the user will be stopped from accessing the remote website and receive a warning that they should not proceed.

Depending on the configuration of the Safe Links policy, the user can ignore the warning and continue to the website. By default, users are prevented from clicking through to open malicious websites. If you allow blocked links to be clicked through, the click is registered and will show up in the *URL threat protection* report in the Defender portal. We do not recommend that you allow users to access links deemed to be unsafe.

In addition to hyperlinks, Safe Links scans QR codes embedded as images in message bodies and attachments. A QR code (also known as a "Quick Response Code") is a two-dimensional barcode that returns a hyperlink when scanned by a smartphone. They are another way bad actors perform phishing attacks by hiding malicious URLs inside a QR code. When it processes messages, Microsoft Defender checks any QR code found in the content and detonates the returned hyperlink in a sandbox to determine if it is safe. For organizations without Defender for Office 365, Exchange Online Protection detects QR codes and uses various threat signals and heuristics to determine if a message (or attachment) containing a QR code should be blocked.

URL Detonation

The Safe Links feature uses a list of known malicious targets to understand if a message includes a dangerous link. This is great if a URL is known to be malicious. However, whenever an attacker creates a new malicious web page, some time will elapse between the web page being accessible and when it is first reported as malicious and, after that, blocked. The URL Detonation feature attempts to intervene during that time by actively scanning URLs in messages before allowing users to access the targets. When a link is considered malicious or points directly to executable content, and the user attempts to access the link, a warning pop-up window (colored yellow) is shown. The user is prevented from opening the target location until scanning is finished. Unlike the Safe Links feature, there is nothing to configure for the URL Detonation feature apart from enabling the option.

It is also possible to delay the email's delivery to the end-user until the links in the email are scanned (just like scanning the attachments). The option to control this behavior is turned off by default. Check the **Wait for URL scanning to complete before delivering the message** option in the Safe Links policy to turn it on. With this option set, any message containing a URL considered malicious is redirected to the user's Junk Email folder.

Configuring a Safe Links Policy

To create a Safe Links policy, open the **Defender portal** and navigate to **Policies and rules > Threat Policies > Safe Links**. Click the **Create** button.

When configuring a policy, you have the following options:

- **Name and Description.** As you can create multiple policies for your organization, it is a clever idea to use a clear name or at least describe the intent of the policy.
- The **Users, Groups, and Domains.** This page specifies the users the policy will be run against. This can be set to all your users or a subset of your users, like all recipients in a specific domain or members of a distribution group. You can also exclude specific users from the policy.

Once these general settings are configured, you can configure the actions for the policy:

- **Safe Links checks a list of known, malicious links when users click links in email**, defining that link protection is enabled for this policy and that links should be rewritten in emails.
 - **Apply Safe Links to email messages sent within the organization** also applies link protection on emails sourced from within the organization. This is particularly useful to protect against compromised mailboxes (when a bad actor has taken over a mailbox) or insider threats.
 - **Apply real-time URL scanning for suspicious links and links that point to files** defines that Defender should perform real-time scanning of all suspicious links. The option **Wait for URL scanning to complete before delivering the message** means delivery will be delayed until link scanning is complete. It is recommended that this option be enabled.
 - **Do not rewrite URLs, do checks via Safe Links API only** allows clients that support the Safe Links API to check the link at the time of clicking rather than during transport. Clients that support the Safe Links API are also not rewritten.
- **Do not rewrite the following URLs in email** is useful when you want to curate a list of trusted links that should never be rewritten. This also works well if you apply safe links to emails sent within the organization. For example, you could exclude your intranet site from being rewritten when the email is being sourced from inside your organization.
- **Safe Links checks a list of known, malicious links when users click links in Microsoft Teams** protect users from malicious links while using Teams. It is recommended to turn this on.
- **Safe Links checks a list of known, malicious links when users click links in Microsoft Office apps** protect users from malicious links while using Word, Excel, and other office products. It is recommended to turn this on.
- **Track user clicks** enable the logging of user clicks.
 - **Let users click through to the original URL** allows users to bypass the security warning and click through to the original URL. It is recommended to disable this option so users can't proceed to the malicious site. If a user believes a warning is a false positive, it is better they submit the URL for administrative review for further analysis.
 - **Display the organization branding on notification and warning pages** is an excellent way for users to identify that the source of the warning is from their own organization. This branding can then be incorporated into employee training and security awareness campaigns.
- The notification page lets you choose whether to **Use the default notification text** or specify custom text with **Use custom notification text**. Custom text is beneficial if you want to refer users to security training or an internal helpdesk.

If you need to create a custom list of URLs to block, check the earlier section in this chapter on Tenant Allow/Block Lists (TABL).

Real-world: The choice to fully block users from navigating to websites that Safe Links blocks could be very invasive. This is especially true when the protected link is accidentally blocked. To block or not block the final link is a security question, and in most cases, as the blocked site is malicious, it is best to ensure that the user cannot click through to the target site. Note that Safe Links does not stop a user from manually copying and pasting the source link into a browser to open the website from there. While the *Safe Links* feature does increase security, it is by no means a replacement for end-user training and added protection on the endpoint itself.

Testing Microsoft Defender for Office 365 features

Testing Safe Links is simple. All you need to do is send a message or write a document that includes the following URL: <http://www.spamlink.contoso.com>.

To verify whether MDO scans incoming attachments, it is enough to send a message that includes a regular (safe) attachment of a type that could include malicious code. This can be anything from an executable to a Word, PowerPoint, or PDF file. Because the regular anti-malware feature will not detect anything in the file, the message will be rerouted through MDO for additional scanning. Therefore, ensure that the attachment type is not blocked by the common attachment type filter.

If you are considering migrating to MDO from another email filtering system, you can enable MDO in evaluation mode. Evaluation mode will provide a log of threats that MDO would have protected you from that your existing email filtering system missed. You can enable evaluation mode in the Defender portal by navigating to **Policies and rules > Threat Policies** and clicking **Evaluation Mode**. It is important to note that the evaluation mode will not alert you to threats already mitigated by your existing email filtering service since those messages or attachments will never reach MDO. You can learn more about evaluation mode and how it works with third-party email gateways in Microsoft's [documentation](#).

Attack Simulation Training

Despite the best efforts of Microsoft Defender for Office 365 (or any other email security solution), it is still possible for malicious emails to reach end-user mailboxes. Therefore, a comprehensive security program will include end-user security awareness training and periodic testing of the program's efficacy. One of the tests is whether end users fall for phishing messages or open attachments to suspicious emails. If you have Microsoft Defender for Office 365 Plan 2, you can automate this testing with Attack Simulation Training.

Attack simulation training can simulate a spear-phishing attack that attempts to harvest valid credentials through phishing messages. A spear-phishing campaign will send sample phishing emails to your users that link them to a realistic webpage that attempts to collect their credentials. If a user clicks the link and enters their credentials, they will be flagged for follow-up. Attack Simulator can also send suspicious-looking emails with attachments that will be tracked if they are opened, or in the case of an attachment with a malicious link, the user will be taken to a page to try and collect their credentials.

You can also use the Attack Simulator to perform password spray attacks and password testing on users in your tenant. Attackers use these techniques to test common, weak passwords against a broad set of users in a tenant. Once the attacker identifies the password for an account, they can use it for malicious purposes. Multi-factor authentication is a crucial defense against these attacks. [Entra ID Password Protection](#) also works to prevent the use of weak passwords in hybrid environments.

To try out [Attack Simulation Training](#), access the **Defender portal** and navigate to **Email & collaboration > Attack simulation training**.

The **Overview** tab compiles the information of your attack simulation strategy into the following widgets:

- The **Recent Simulations** widget shows any recent simulations. Clicking the **View all simulations** button takes you to the *Simulations* tab. Clicking the **Launch a simulation** button launches the attack simulation wizard (covered in the next section). Note that this widget does not show any of the automated attack simulations.
- The **Recommendations** widget identifies simulated attacks you should launch or schedule for your organization.
- The **Simulation coverage** widget identifies the percentage of users who have and have not received a simulated attack. Clicking the **Launch simulation for non-simulated users** button allows you to create a simulated attack to remedy that gap.
- The **Training completion** widget identifies the percentage of users who have completed the required security awareness training. Clicking the **View training completion report** button shows how each user is progressing with their security awareness training. This report can be exported as a CSV.
- The **Repeat offenders** widget identifies users who have consecutively failed the simulated attacks. Clicking the **View repeat offenders report** button gives you a graph identifying the number of users who have failed each social engineering technique. This includes providing credentials to a fake portal, opening attachments that contain malware, and clicking malicious links. The chart below the graph identifies each user, how often they have repeated the offense, and the simulation types they have failed.
- The **Behavior impact on compromise rate** widget tries to determine the efficacy of the security awareness training and how susceptible the organization's user base is to compromise as a percentage. Clicking **View simulations and training efficacy report** expands the data surfaced by the widget into a more detailed report. This report identifies each simulation, the predicted compromise rate, the actual compromise rate (how well the organization did), the total target users, and how many of those total users fell victim to the simulated attack.

The **Simulations** tab identifies all currently configured simulations and their state (we will cover launching an attack simulation in the next section). States include simulations in draft (saved but not yet submitted), scheduled, in progress, completed, failed, and canceled.

If you select a simulation, you can review the report of that simulated attack. This includes how many users were compromised by the simulation, how many users reported the simulation as a phishing attack, which payloads were used in the simulation, recommended actions to protect users from this type of attack, and the progress of any user awareness training attached to this simulation. Other details include when the simulation was launched, when the simulation will end, how many users were targeted, and the current status of the simulation. To cancel a simulation, select the three dots on the far right of the simulation entry, and click **Cancel Simulation**. Also, using **Copy simulation** you can create a copy of a previous simulation to make adjustments or tweak it for a different audience.

The **Training** tab allows you to manage training campaigns for employees.

The **Reports** tab contains reporting options on the attack simulation coverage, training completion, repeat offenders and behavior impact on compromise rate.

The **Automations** tab allows you to automate one or more attack simulations (we will cover setting up an automated attack simulation in a later section).

The **Simulation content library** tab allows you to create your own custom payloads. Customizing the payload is helpful since you can create a phishing message or fake logon portal that is a more realistic representation of your organization using your logo, color scheme, and other convincing content.

Microsoft offers many different email payloads, including emails with the purpose of credential harvesting, delivering malware as either an attachment or a link, inserting links to websites with malicious code, or

convincing the user to grant OAuth consent. Depending on the payload selected, you can configure the sender's display name and email, the subject, phishing links, a malware attachment, language, and theme. You can also import or copy an email into the text editor. A code editor is also available to configure the email in an advanced way.

Microsoft offers several templates to create your own fake login portal, including fake portals for LinkedIn, GitHub, and Microsoft. These templates can then be customized either in the text or by code editors.

The simulation content library tab also contains the end-user notifications. End-user notifications can be customized, offering either positive reinforcement if the user submitted the simulation as phish or a failure notification if the user fell victim to the simulated attack. This could include links to additional security training and reminders for the user to complete that training.

The **Settings** tab allows you to define what is considered a repeat offender. A repeat offender is someone who has fallen victim to consecutive simulations. The default number is two, but it can be set higher.

Launching a Simulated Attack

To launch a simulation, click the **Launch a simulation** button. The *Select Technique* page (Figure 6-14Error! Reference source not found.) identifies all social engineering types, including:

- **Credential harvest** includes an email that links to a fake portal designed to trick users into inputting their credentials on a malicious website.
- **Malware attachment** includes an email with an attachment designed to run malicious code or a macro to compromise or gain access to the user's device, allowing the bad actor to launch additional attacks.
- **Link in attachment** includes an email with an attachment that has an embedded URL. The embedded URL takes the user to a fake portal to trick the user into entering credentials.
- **Link to malware** includes an email with a URL to a malicious file (for example, mimicking a well-known sharing site like SharePoint Online or Dropbox) which could contain malicious code or macros.
- **Drive-by URL** includes an email with a URL to a website that runs malicious code designed to compromise or gain access to the user's device, allowing the bad actor to launch additional attacks.
- **OAuth consent grant** uses an app created by a bad actor, prompting the user to grant permissions to the app. This could allow the app to harvest data or perform other attacks on the user.
- **How-to Guide** sends users message containing instructions on certain actions, such as how to report phishing messages.

Select a technique and click **Next**. Give the simulation a **Name** and **Description** and click **Next**.

From the *Select payloads and login page*, select the payloads sent to users. A payload can contain both an email and a login portal. You can customize the email contents, as well as select a branded login page which you can customize, or you create your own to use in the attack simulation. After selection and any customization you can also test the created payload by clicking the **Send a test** button. This test is sent to the currently logged-in user. This test is not included in the simulation reporting. When you have selected your desired payload, click **Next**.

On the *Target Users* page, you can include either specific users or groups or the entire organization. Selecting particular users is a great way to test an attack simulation on a small scale before targeting the entire organization. Then, scope the users for the automated simulation and click **Next**.

On the *Assign training* page, you can assign training to users.

- Select **No training** if you don't want to add any follow-up training to the attack simulation.

- If you want to add a custom training URL, which could be directed to an internal learning management system or security training portal, select **Redirect to custom URL** and enter the appropriate URLs.
- If you want to use security training curated by Microsoft, select **Microsoft training experience (Recommended)**. The Microsoft training experience includes a dozen videos between 3 and 7 minutes. When you select the Microsoft training experience, you can either **Assign training for me (Recommended)** or **Select training courses and modules myself**.

With the custom URL or Microsoft training experience, you can set a training due date of 7, 15, or 30 days. For phishing payloads, you can select the phish landing page to use for the learning experience as well.

On the *Select end user notification* page, pick whether to notify users about the results of their participation in the attack simulation. This is one way to provide positive reinforcement if a user correctly identified and reported a message as phish or an opportunity to provide security training and awareness to users who fell victim to the simulation. Options include:

- **Do not deliver notifications** if you do not wish to have user involvement with the simulation.
- **Microsoft default notification (recommended)** if you want to use the default Microsoft notifications. This selection allows you to define the delivery preferences for the Microsoft notifications (such as when to deliver the notification) and allows you to review the notification layout before sending.
- **Customized end-user notification** if you want to provide your own notifications. We discuss notifications in greater detail while covering the *Simulation content library* tab.

On the *Launch Details* page, select whether to execute the simulation as soon as the wizard is complete or schedule the simulation to start later. With either selection, you must also define (in days) when the simulation should end. The default is two days, ranging from 2 to 30 days. Optionally select **Enable region aware timezone** delivery to take the timezone configured on the recipient's mailbox into account when delivering the payload. With the launch schedule defined, click **Next**.

You can test the simulation before submitting it. Click the **Send a test** button to send the simulation to the currently logged-on user. If the test looks good, click the **Submit** button.

Automating a Simulated Attack

To create a new automated attack simulation, navigate to **Automations > Simulation Automations** and click the **Create Automation** button. Next, enter a **Name** and **Description**, then click **Next**.

The *Select Social Engineering Technique(s)* page (Figure 6-14) allows you to select one more attack simulation. Select the simulations you want to automate and click **Next**. From the *Select payloads and login* page, you can manually select or randomize the payloads sent to users. A payload can contain both an email and a login portal. Click **Next**.

The *Target Users*, *Assign Training*, and *Select end user notification* pages are identical to the launch simulation wizard covered in the previous section. For more details on these pages, see the previous section.

On the *Simulation Schedule* page, you can choose whether to create a **Randomized** or **Fixed** schedule to launch the attack simulation. Click **Next**.

- If you selected a fixed schedule, the *Schedule Details* page will ask for **Automation Start** and **Automation End** dates. Select a date from each date picker. You can then define how often the simulation reoccurs and whether the reoccurrence is monthly or weekly. If you select weekly, you can choose the day of the week for the occurrence. If you select monthly, you can choose the day of the month for the occurrence.

- If you selected a randomized schedule, the *Schedule Details* page will ask for **Automation Start** and **Automation End** dates. Select a date from each date picker. Then, from the *Automation Scoping* section, pick which days of the week the randomizer can send simulated attacks. For example, if your organization only works Monday through Friday, you may only wish to select weekdays. The needs of the business should also dictate this schedule. For example, if client invoicing or payroll is every Friday, you may not wish to launch simulated attacks on that day. You can also choose to randomize the delivery times of the simulation emails.

With the schedule and reoccurrence settings defined, click **Next**.

Select the social engineering technique you want to use with this simulation automation. We've curated these from the MITRE Attack framework. Depending on your selection, you will be able to use certain types of payloads.

Credential Harvest
In this type of technique, a malicious actor creates a message, with a URL in the message. When the target clicks on the URL within the message, they are taken to a web site, the website often...[View details of Credential harvest](#)

Malware Attachment
In this type of technique, a malicious actor creates a message, with an attachment added to the message. When the target opens the attachment, typically some arbitrary code such as a macro...[View details of Malware attachment](#)

Link in Attachment
In this type of technique, which is a hybrid of a Credential Harvest and Malware Attachment, a malicious actor creates a message, with a URL in an attachment, and then inserts the attachment into the message. When the target opens the attachment, they are represented with a URL in the actual attachment...[View details of Link in attachment](#)

Link to Malware
In this type of technique, a malicious actor creates a message, with an attachment added to the message. However instead of directly inserting the attachment into the message, the malicious actor will host the attachment on a well-known file sharing site, (such as SharePoint, or Dropbox) and insert the URL to the attachment file path...[View details of Link to malware](#)

Drive-by URL
In this type of technique, a malicious actor creates a message, with a URL in the message. When the target clicks on the URL within the message, they are taken to a website, the site will then try and run some background code to gather information about the target or deploy arbitrary code to their device...[View details of Drive-by URL](#)

OAuth Consent Grant
In this type of technique, a malicious actor has created an Azure Application that asks the target to grant the application permissions over some of the target's data. The application will provide...[View details of OAuth Consent Grant](#)

Figure 6-14: Automated Attack Simulator Setup Wizard showing Social Engineering Techniques

On the *Launch details* page, you can select additional options such as whether to include the same users on each simulation, whether to target repeat offenders who had fallen victim to the simulation, whether to enable region-aware delivery (so phishing messages are sent during working hours), and whether to use unique payloads for different users. Once you have your options defined, click **Next**.

Review the simulation settings and click **Submit**.

When you submit a simulation, it is saved in an inactive state. To activate the simulation, select it from the **Automations** tab and click the **Turn on** button. When enabled, the *Status* column will switch to *Active* and show the next launch time. If you wish to disable the simulation, select it from the *Automations* tab and click the **Turn off** button. The *Status* column will report *Inactive*, and the *Next launch time* column will be blank. You can also delete a simulation from this tab.

Using Third-Party Attack Simulators

Some organizations might prefer to use third-party attack simulators to send phish or impersonated emails to their end-users. Traditionally, using third-party simulators requires adding those organizations to various allow lists under several policies, so Microsoft would not act on the simulated attack.

With the advent of Microsoft's [Secure by Default](#) initiative, customer-defined entries in IP allow lists, sender allow lists, domain allow lists, and mail flow rules are not honored if the message contains malware or is classified as high confidence phish. Therefore, if you previously added your third-party vendor for email attack

simulation to any of these lists, their simulations will be blocked. Instead, you should transfer these configurations to Advanced Delivery.

Configuring Advanced Delivery

To add a third-party attack simulator, open the **Defender portal** navigate to **Policies and rules > Threat Policies > Advanced Delivery**, and select the **Phishing Simulation** tab. From this tab, click **Edit**. The *Edit Third-Party Phishing Simulation* pane (shown in Figure 6-15) lets you add all **Domains**, **Sending IPs**, and **Simulation URLs** associated with the third-party attack simulator.

It is worth noting that the *Simulation URLs* field is only used for Microsoft Teams and M365 Apps. When the URLs are added to the body of an email they are automatically allowed as long as the *Domain* and *Sending IPs* are allowed.

Edit third party phishing simulations

Phishing simulations are attacks orchestrated by your security team and used for training and learning. Simulations can help identify vulnerable users and lessen the impact of malicious attacks on your organization.

Third-party phishing simulations require at least one **Sending domain** entry [source domain or DKIM] AND at least one **Sending IP** entry to ensure message delivery. URLs present in the email message body will also be automatically allowed at time of click as a part of this phishing simulation system allow.

Note: The **Simulation URLs to allow** field is optional and available for non-email based phishing simulation campaign scenarios. Specifying URLs in this field ensures that these URLs aren't blocked at time of click for phishing simulation scenarios that use Microsoft Teams and Office apps (Word, Excel...) [Learn more](#)

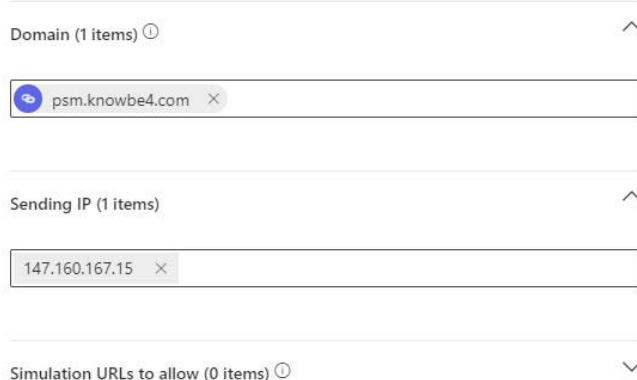


Figure 6-15: Adding third-party phishing simulations

The `New-PhishSimOverridePolicy` cmdlet creates third-party phishing simulation configurations. You can only have one policy, and its name will be `PhishSimOverridePolicy` regardless of what you specify using the mandatory `Name` parameter. After creating the new policy object, you need to create rules for domains and sender IPs using the `New-ExoPhishSimOverrideRule` cmdlet, and assign the rules to the policy by referencing its ID. The URLs that need to be exempted must be configured using the tenant allow/block lists using type `AdvancedDelivery`. The following example shows how to create a new third-party phishing simulation policy which is initially disabled, attach a domain and IP range to bypass scanning and finally enable the policy:

```

New-PhishSimOverridePolicy -Name 'Bogus' -Enabled $False
$ID = (Get-PhishSimOverridePolicy).externalIdentity
New-ExoPhishSimOverrideRule -Policy $ID -Domains 'contoso.com' -SenderIpRanges '10.1.2.3/24'
New-TenantAllowBlockListItems -ListType Url -ListSubType AdvancedDelivery -Entries *.fabrikam.com -NoExpiration
Set-PhishSimOverridePolicy -Identity 'PhishSimOverridePolicy' -Enabled $True

```

To view or modify the configuration, use `Get-ExoPhishSimOverrideRule` and `Set-ExoPhishSimOverrideRule` respectively.

Investigations

Investigations, or Automated investigation and response (AIR), are part of Microsoft Defender for Office 365 Plan 2. AIR runs a security playbook after an alert is triggered within your organization, either automatically as a response to well-known phishing/malware events or manually by an administrator. The playbook gathers additional information about the event and returns a set of actions as recommendations. However, AIR does not automatically perform remediation actions—an administrator must manually approve recommended remediations.

To access the ongoing and recently completed investigations list, open the **Defender portal** and navigate to **Investigations**. Investigations are populated in the Investigations tab from multiple sources. One such source is when an administrator reviews user-submitted messages through the Outlook reporting feature. These messages appear in the Defender portal under **Actions & Submissions > Submissions > User Reported**. From here, an administrator can select an email, select the **Submit to Microsoft for analysis** dropdown, and pick **Trigger Investigation**. Another source is when the administrator is using the *Explorer* tab in the Defender portal. Similarly, under the *Explorer* tab they can select an email, click the **Message actions** dropdown, and select **Trigger Investigation**. Essentially, anywhere you see Trigger Investigation in the Defender portal will start an investigation on that email.

By default, this dashboard is filtered to show investigations from the last 24 hours. You can expand this date range by modifying the filter. The filter also lets you scope the dashboard to a specific status or investigation type. For example, you could filter the results to focus on investigations that uncovered compromised users.

To get the properties on a specific investigation, click the **Open in new window** icon. This will launch a new page with the following tabs. Figure 6-16 shows the investigation graph of an investigation.

- **Investigation graph** gives you a visual overview of the selected item. You can click on the individual graph components to be transported to one of the other tabs. For example, the investigation graph in Figure 6-16 shows that 7 entities were analyzed (1 email, 1 file, and 5 clusters). If you click the entities analyzed icon, it transports you to the entities tab.
- **Alerts** list the alert that triggered the investigation. You can select each alert to get the details on what caused the alert. Using the example from Figure 6-16, this alert was caused due to ZAP retroactively detecting malicious content in an email. In our case, the alert identified the email (noting the recipient, subject line, sender address, sender IP, and date sent.)
- **Mailboxes** lists impacted users. You can select each user and click the **More details about user** link if you want to see all investigations that the user has been a part of in the last 7 days. This is useful to see if the user is a victim of repeated digital attacks.
- **Evidence** identifies all email items related to the investigation, including the initially reported item and any items found in the hunting phase. This could include the message body, attachments, and subject line.
- **Entities** include all the individual objects part of the investigation, such as the user, message, files, IP addresses, etc.
- **Log** gives details on the execution of different steps of the investigation.
- **Pending Actions** lists the actions Exchange Online is recommending taking. For example, the action could be to soft or hard delete the message. From here, the admin can either **Approve** or **Reject** the action. If an admin rejects the action, they must provide a reason. From the action screen, the admin can view the message headers, download the email for further analysis, or open the item in Explorer (covered in the next section).



Figure 6-16: Investigation graph

Threat Explorer

The Threat Explorer is a great way to see what actions Exchange Online takes on email. In the **Defender portal**, navigate to **Email & Collaboration > Explorer**. The top half of the dashboard displays a stack graph (Figure 6-17). The tabs along the top of the graph allow you to select either all email or focus your search to just malware, phish, campaigns, URLs, and more.

The default stack graph shows all email from the last two days and the combined delivery action, including delivered normally, delivered to junk, and blocked. By changing the default filter *Sender address* to **Delivery Action** you can change the stack graph to show different data such as **Sender Domains**, **Sender IPs**, and **Detection Technology**.

By default, the graph only shows the last two days, but this date range can be increased to the last 30 days using the date and time pickers at the top of the screen. Once you pick a new start or end date and time, click the **Refresh** button.

You can also filter results. For example, to filter all actions taken on messages from a specific sender, select **Sender** from the drop-down, type the sender's email address, and click the **Refresh** button. Note that you can filter multiple values by providing a comma-separated list in the text box. In our example, we could type multiple sender email addresses separated by a comma. There are dozens of other filters, such as looking at messages coming to or from a specific connector, actions taken, impersonated users and domains, and more.

You can also save your queries using the **Save Query** button. This is useful if you need to track a specific event over time. Saved Queries appear in the **Defender portal** on the **Threat Tracker** page.

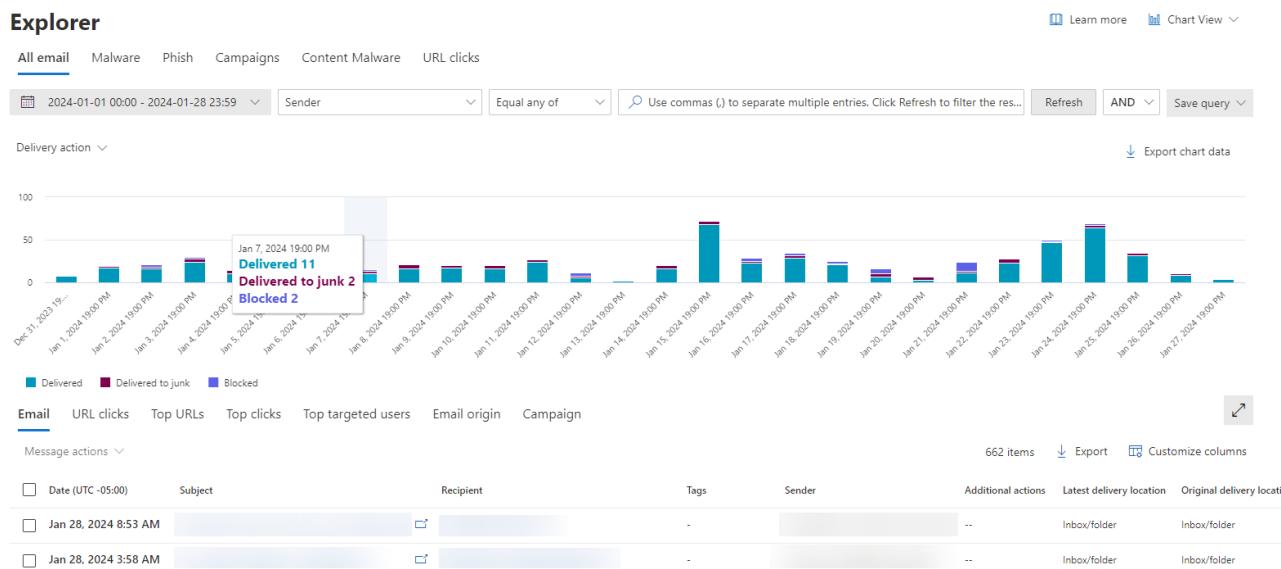


Figure 6-17: Threat Explorer showing mail delivered, delivered to junk, or blocked

The table in the lower half of the dashboard has multiple tabs allowing you to scope the table to specific results. This includes email, URL clicks, top URLs, top clicks, top targeted users, email origin, and campaigns. Each tab returns different data.

For example, the default **Email** tab identifies each email's delivery date, subject, recipient, sender, and delivery action. Selecting an email and clicking the **Open in new window** button brings up additional detail about that email. This additional detail includes a timeline through Exchange Online, a detailed analysis of the email (which includes message headers, policy actions, and more), if the email contained any attachments or URLs (and any malicious verdicts), and if the emails were related or like any other emails. For additional analysis, an admin can preview or download the email from this view.

The **Email** tab also allows you to perform message actions. By selecting an email and clicking the **Take action** button you can perform several actions including, moving the message to the users junk or deleted items, hard deleting the message, reporting the message (clean, phishing, spam, etc., similar to the dialog shown in Figure 6-13), or trigger an investigation. Selecting **Trigger investigation** launches an investigation in the *Investigations* tab we discussed in the previous section. The *Take Action* wizard can perform actions on up to 100 selected messages.

The **Top URLs** tab identifies how many emails a URL appeared. The count columns can also be sorted, allowing you to identify the top URLs found in blocked, junked, and delivered emails. Selecting a URL allows you to see which emails included the link, as well as WHOIS information on who owns the domain attached to the link. You can view more about the email that contained a URL by clicking the **Open in new window** button.

The **Top Targeted Users** is a great way to identify who is targeted by these digital attacks. Each user identified will have a corresponding number of attempts by their email address. Selecting the user will filter explorer to just that user.

Threat Tracker

Threat tracker allows you to access all your previously saved queries from Explorer. Select a query and click the **Explore** link to use a saved query. This will launch that query on the **Explorer** page. For more information, check the previous section on Explorer.

Threat Explorer allows you to modify an existing query by clicking the **Edit** button. You can also delete saved queries by clicking **Delete**.

Monitoring and Troubleshooting Mail Flow

Microsoft provides a variety of tools and reports to help you keep track of mail flow in your organization. For example, when something goes wrong, tools like message tracing let you explore precisely what happened to a message so that you can troubleshoot a problem. In addition, if you look deep into email messages, there are a plethora of diagnostic message headers that EOP and Exchange Online add to help explain precisely what happened to the message when Microsoft processed the item.

Mail Flow Dashboard

On the **Exchange Admin Center** home screen, you can find a collection of widgets and reports with associated alerts and recommendations to help you review your Exchange environment and certain aspects of it, mostly mail flow-related and recent mail-related alerts. You can customize this screen by adding or removing cards.

Figure 6-18 shows a sample Exchange Admin Center home screen. As with most other dashboards, you can customize the arrangement of the widgets to suit your needs. Most widgets link back to a mail flow report under the **Reports > Mail Flow** section in the Exchange Admin Center.

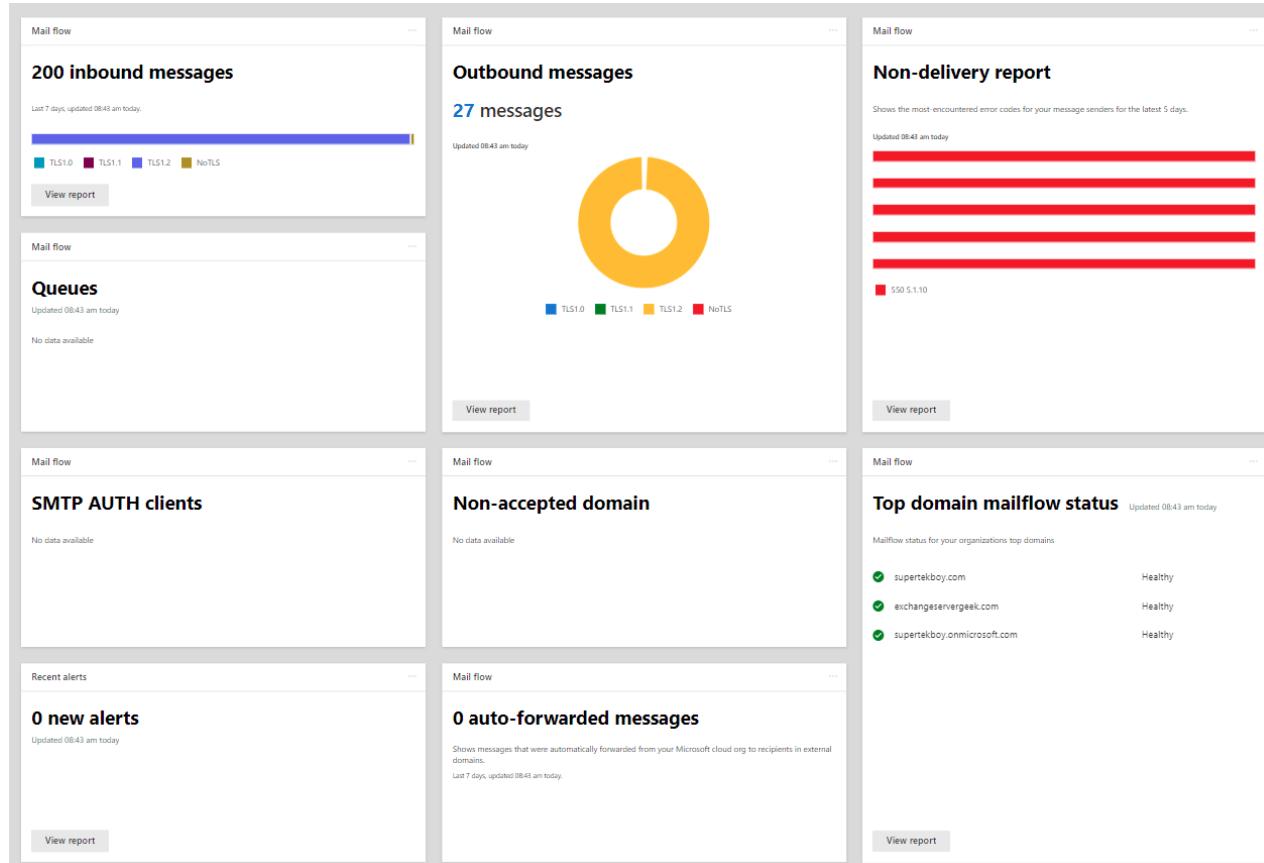


Figure 6-18: Exchange Admin Center Mail Flow cards

Inbound Messages

The inbound messages widget (Figure 6-18) displays the number of inbound messages received in the last 7 days. Below the graph, a legend identifies each TLS protocol (including messages received without TLS). You

can select each TLS protocol in the legend to focus the graph on just that protocol. Selecting the **View Report** button redirects you to the inbound messages report (under **Reports > Mail Flow**).

The inbound messages report (Figure 6-19) provides greater detail than the widget. This dedicated screen displays daily mail volume, the percentage of mail received by TLS protocol, and a detailed line item report breaking down daily mail by each connector.

The various drop-downs allow you to change the date scope between 7, 30, and 90 days (including a custom date range) or select a specific inbound connector (or all inbound connectors). You also have the option to filter the results with the **Filter > New Filter** button. To export the report to CSV, click the **Export** button. Alternatively, click the **Request Report** button to send the report directly to your email.

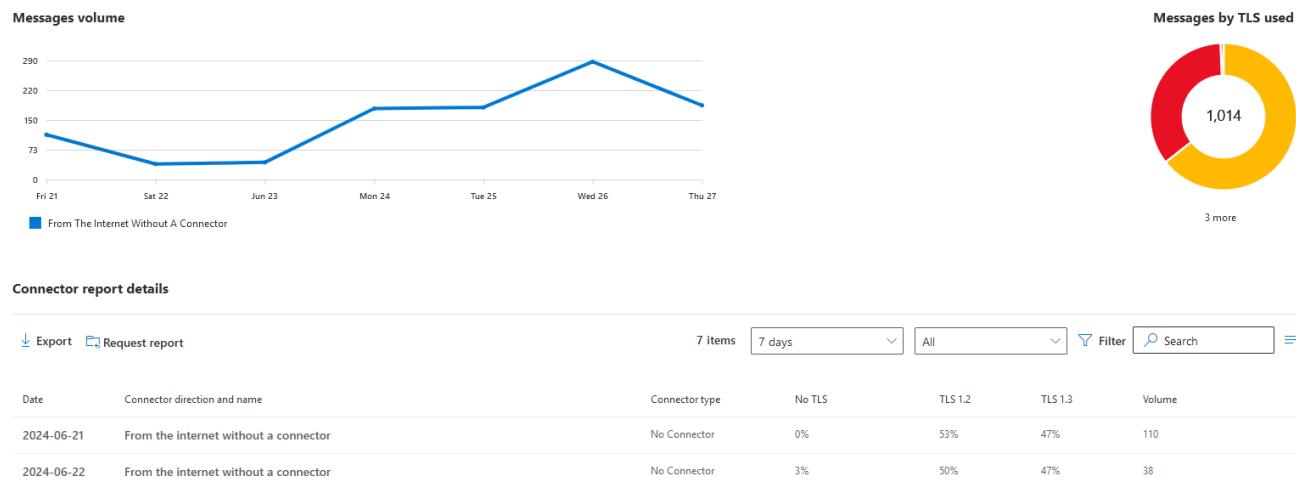


Figure 6-19: Inbound messages report

Outbound Messages

The outbound messages widget (Figure 6-18) displays the number of outbound messages sent in the last 7 days as a donut chart. Below the chart, a legend identifies each TLS protocol (including messages received without TLS). You can select each TLS protocol in the legend to focus the chart on just that protocol. Selecting the **View Report** button redirects you to the outbound messages report (under **Reports > Mail Flow**).

The outbound messages report is identical to the inbound report shown in Figure 6-19. Like the inbound report, you can see outbound mail volume by day, the percentage of mail sent by TLS protocol, and a detailed line item report breaking down daily mail by outbound connector.

The drop-downs also operate similarly to the inbound report, allowing you to change the date scope, select a specific outbound connector, or filter the results. To export the report to CSV, click the **Export** button. Alternatively, click the **Request Report** button to send the report directly to your email.

Non-Delivery Report

This widget shows the most common error codes over the last 5 days, including the number of times an error occurs on a given day. For example, Figure 6-18 shows that our only error code in the last 5 days is 550 5.1.10, which equates to "Recipient not found." A fairly innocuous error that is likely due to a mistyped email address.

The **View Report** button redirects you to the non-delivery report (located under **Reports > Mail Flow**). This report gives us a detailed overview of the volume of error codes we have received each day; selecting a key on the legend filters the graph to that specific error code. This is useful when we want to identify patterns in our errors. For example, in Figure 6-20, we primarily receive error 550 5.1.10 as identified by the widget. However, on 3/10/22 and 3/7/22, we also received error code 550 5.7.133, which means we do not have

permission to send it to a distribution list. We can then take the message IDs under the Sample Messages column and perform a message trace to investigate the failure further.

Non-delivery report

Monitor messages that aren't getting delivered to the intended recipients. When a message can't be delivered, the sender gets an emailed non-delivery report (NDR) with an error code that indicates why the message wasn't delivered. This page shows the details of the NDRs and helps you troubleshoot the issues. [Learn more](#)

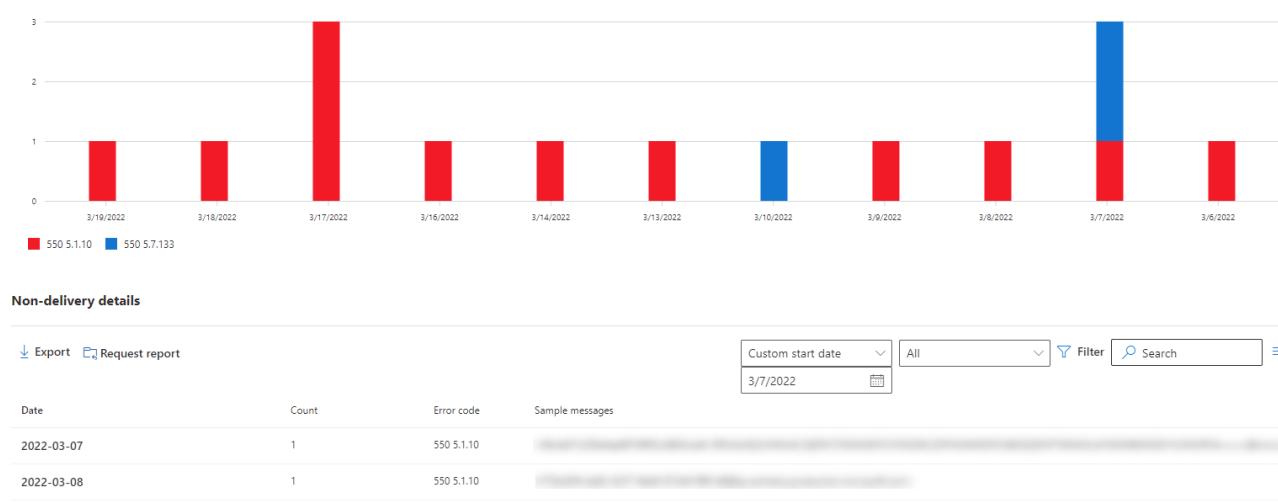


Figure 6-20: Non-delivery report

Queues

The **Queues** widget is another default part of the dashboard. The Queues widget shows you the number of messages stuck in a mail flow connector for more than one hour. If the number shown is greater than zero, you can click it to go through a series of flyout reports showing information such as the number of queued messages and the connector name (linked through to EAC, where you can fix the connector in error).

The number of queued messages can also be clicked to show a message trace report for the items stuck in the queue, showing further information on the problem. For example, a queue containing the wrong smart host might show the target host refused to allow an SMTP connection, otherwise known as a socket error.

A report is available for this widget by navigating to **Reports > Mail Flow > Queued messages report**.

SMTP AUTH Clients

Clients that connect directly to SMTP servers are known as SMTP AUTH clients. An example of an SMTP AUTH client could be a multi-function printer performing scan-to-email that relays directly to Exchange Online via `smtp.office365.com`, rather than an on-premises mail server. The TLS version used by these clients is visible in this widget. This widget will be empty if you do not leverage SMTP AUTH clients.

Understanding the TLS version used for SMTP AUTH is vital as Microsoft deprecates the use of TLS 1.0 and TLS 1.1 from their primary `smtp.office365.com` endpoint. Any client needing TLS 1.0 and TLS 1.1 must use the legacy-`smtp.office365.com` endpoint instead (see the Device and App Mail Relay to Exchange Online section).

A report is available for this widget by navigating to **Reports > Mail Flow > SMTP AUTH clients report**.

Note: To reduce your attack surface, Microsoft recommends that organizations enable SMTP AUTH only on mailboxes that require access to the protocol. See the Managing Exchange Online chapter for more information on this topic.

Non-Accepted Domain

The non-accepted domain widget identifies email relayed from your on-premises environment using a domain not registered in Office 365. For example, if an on-premises application sends mail as "app@office365itpros.co.uk" and the only domain in your tenant is "office365itpros.com," this widget will identify that issue.

Making sure to only send messages from domains registered to your tenant is incredibly important. Microsoft will reject any mail where the *From* address does not match one of the domains in your tenant. This is particularly important in tenant-to-tenant migrations, where a domain is removed from one tenant and added to another. During this transition, any on-premises relays must be updated to the new tenant.

A report is available for this widget by navigating to **Reports > Mail Flow > Non-accepted domains report**.

Top Domain Mail Flow

You must have the correct MX record published in DNS to receive emails for a domain. A change in the MX record could result in an email outage. This widget gives you a high-level overview of potential health issues for your registered domains (including the tenant domain). A green checkmark and a status of *Healthy* indicate everything is good.

Selecting the **View Report** button (Figure 6-21) redirects you to the *Top domain mail flow status report* (located under **Reports > Mail Flow**). The *Inbound* tab gives a detailed overview of each domain, its health, the previous and current MX records (if it has recently changed), and if you have received an email to that domain in the past 6 hours. The *Outbound* tab identifies any email sent or relayed through your tenant that is considered high risk, and subsequently sent through a high-risk relay pool. You can use this report to identify which messages triggered a risk and use message trace to further identify domain misconfigurations (such as an invalid SPF record) that might cause the message to be considered high risk. In message trace, any Exchange Online server with "RLY" in its name is a server associated with the high-risk relay pool.

Top domain mailflow status report					
Export		Filter		Search	≡
Domain	Domain status	Previous Mx Record	Current Mx Record	Emails received (past 6 hours)	
<input type="checkbox"/> supertekboy.com	Healthy	supertekboy-com.mail.protection.outlook.com	supertekboy-com.mail.protection.outlook.com	Yes	
<input type="checkbox"/> exchangeservergeek.com	Healthy	exchangeservergeek-com.mail.protection.outlook.c...	exchangeservergeek-com.mail.protection.outlook.com	No	
<input type="checkbox"/> supertekboy.onmicrosoft.com	Healthy	supertekboy.mail.protection.outlook.com	supertekboy.mail.protection.outlook.com	No	

Figure 6-21: Top Domain Mailflow Status Report

This report will also identify when domains have expired, which would result in the domain no longer resolving and causing mail flow and other issues.

Recent Alerts

Security is always something to review on an ongoing and consistent basis. The **Recent Alerts** widget identifies if any Exchange Online mailboxes are potentially compromised. The most common item displayed here is alerts on forwarding rules (see the next widget report). Click the **View Report** button to see a report of all alerts in the last 90 days. This report is also accessible by navigating to **Mail Flow > Alerts**.

Auto-Forwarded Messages

The auto-forwarded messages widget is designed to help you combat a common approach to data exfiltration. For example, this often happens during a business email compromise attack when the attacker

wishes to understand a victim's mail traffic patterns before they send a phishing email to try and lure someone into taking action, such as making a payment. It is recommended that you limit this behavior so that email is only forwarded outside the organization when justified by business reasons.

The widget identifies the number of forwarded items in the past week, including messages forwarded by a user via an inbox rule, their OWA forwarding options, or an administrator who has configured a mail flow rule or SMTP forwarding.

A report is available for this widget by navigating to **Reports > Mail Flow > Auto-forwarded messages report**. The **Summary** tab identifies all forwarded messages, the method used to forward those messages (inbox rules, mail flow rules, or SMTP forwarding), and the forwarding users and domains. The **New Activity** tab shows any new forwarding in the past 7 days.

It is prudent to frequently review this information and block or remove any rules that forward emails as appropriate. It is also worth noting that you can create alert policies to signal an alert when a user forwards emails from their account. Also, Microsoft Secure Score awards a higher score to tenants who do not allow email forwarding.

Other Widgets

Other widgets (not shown in Figure 6-18) include:

- **Migration Batch** identifies the success or failure of recent migration batches to or from Office 365. Selecting the View Report button takes you to the Reports > Migration tab, where you can dive into the nature of the success or failures of each batch.
- **Mailboxes** provide quick links to everyday administrative actions such as adding a shared mailbox, managing email forwarding, or hiding a mailbox from address lists.
- **Training and Guide** provide links to Exchange Online documentation and training for administrators.

Mail Flow Reports

Most widgets described in the previous section link to a report under **Reports > Mail Flow**. However, the reports tab also contains additional reports that do not have a corresponding widget. These reports are discussed below.

Mail Flow Map Report

The *Mail flow map* report provides a visualization of mail flow in Office 365. This helps to identify trends or anomalies in mail routing.

- The center of the visualization is Office 365. This shows the count of internal messages in the tenant.
- Messages coming into the tenant, including mail from the internet and any custom connectors, are shown to the left of Office 365.
- Messages leaving the tenant, including mail to the internet and any custom connectors, are shown to the right of Office 365.

The table below the visualization identifies each domain exchanging mail with your tenant in the last 90 days. You can also refine this report by clicking the **Filter** button. For example, to only see messages received by a specific domain, select **Send or receive domain** option from the *Field* drop-down, pick an operator and specify the domain. You can export these results for further analysis to CSV by clicking the **Export** button.

Mailboxes Exceeding Receiving Limits Report

The *Mailboxes exceeding receiving limits* report identifies mailboxes that could be throttled due to exceeding transport limits. When mailboxes are throttled, they experience delays in sending and receiving mail. Throttling has a clear impact on users and the business, so keeping on top of any potential throttling is vital.

This report comprises a heatmap that shows the top 10 mailboxes impacted in the last 24 hours and a table of all mailboxes that exceed transport thresholds.

For a complete list of transport limits, see the Transport Limits section.

Dynamic Distribution Group Report

The *Dynamic distribution group* report provides usage information about dynamic distribution groups. By switching the report to **Unused**, an administrator can quickly identify which dynamic distribution groups are not in use. By default, the report only shows the last 30 days, but this range can be increased to a 90-day window using the date range picker.

Reply-all Storm Protection Report

The *Reply-all storm protection report* identifies when a reply-all storm was triggered based on the thresholds configured by the tenant admin. By default, reply-all protection blocks replies to an email thread for 6 hours if it had detected more than 10 reply-all messages within 60 minutes to a thread with over 2,500 recipients. These values (aside from the 60-minute detection window) are configurable from the **Exchange Admin Center** by navigating to **Settings > Mail Flow**.

The goal of reply-all storm protection is to stop chain emails from impacting the organization. The *Reply-all storm protection report* identifies each message that triggered reply-all protection. This can be useful if you need to provide guidance or training to the message originator to prevent a reply-all storm in the future. The report attributes could also be used if you need to perform a content search to remove the offending messages.

The configurable ranges for the reply-all storm protection can be found in the Transport Limits section.

Exchange Transport Rule Report

The *Exchange transport rule* report identifies triggered mail flow rules over a given period. This data is represented by a graph (Figure 6-22), which identifies the daily volume of each triggered rule, and a donut chart, which breaks down rule volume by direction and severity. You can select a key from each chart legend to focus on a specific component. For example, you can select the outbound key to focus solely on the volume of rules triggered on outbound mail flow.

Exchange Transport Rule report

View matches for the mail flow rules that are set up for your organization. You can manage these rules in the Exchange Admin Center. [Learn more](#)

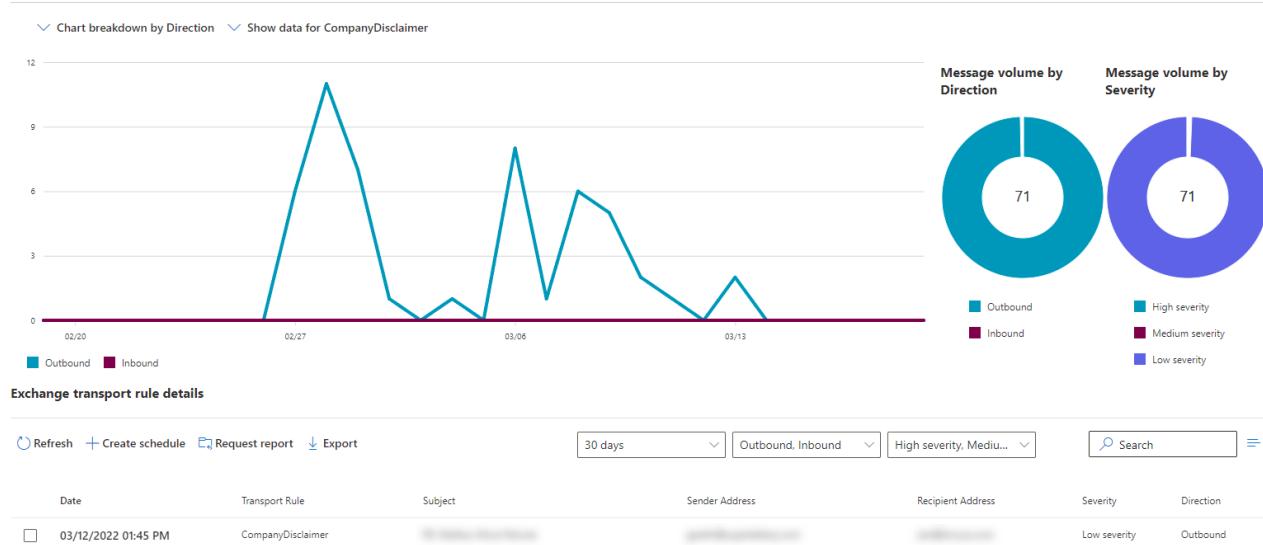


Figure 6-22: Exchange Transport Rule report

By default, this report shows the volume for the last 7 days. However, like all other reports, it is possible to change this timespan to 7, 30, or 90 days (including a custom date range). In addition, it is possible to focus the graph on a specific rule, mail flow direction, or severity using the drop-downs. This is useful to see whether a rule is triggering more in one direction than the other (e.g., inbound versus outbound) or if you are looking for rules categorized as high severity.

High Volume Email

The High Volume Email report reports on the HVE email volume. The report is currently in preview.

Outbound Message in Transit Security Report

The *Outbound message in transit security* report identifies the state of messages being secured with MTA-STS, DANE for SMTP, or opportunistic TLS.

- Messages Blocked identifies all messages that failed MTA-STS or DANE for SMTP validation and were unable to send. These errors can help admins identify and troubleshoot specific domains having problems.
- Messages Secured identifies all messages successfully delivered with MTA-STS, DANE for SMTP, or opportunistic TLS. This is useful to validate if mail can be sent to a specific domain using MTA-STS, DANE, or opportunistic TLS.

Out-of-date connecting on-premises Exchange Servers Report

In the connectors section, we discussed how unsupported and non-compliant Exchange Servers will be throttled after 30 days and blocked after 90 days. The *Out-of-date connecting on-premises Exchange servers report* identifies any currently unsupported and non-compliant servers subject to throttling and blocking. For more information, check <https://aka.ms/BlockUnsafeExchange>.

Email and Collaboration Reports

In addition to the Mail Flow Reports in the Exchange Admin Center, the Microsoft Defender portal contains additional email security reports. These can be accessed through the **Defender portal** and by navigating to **Reports > Email & collaboration reports**.

Mail Latency Report

With the extra layers of security provided by Microsoft Defender, including the ability to detonate attachments in a sandbox, administrators may be concerned about how much latency this adds to message delivery. To enable administrators to better visualize this for their entire tenant Microsoft aggregates all message trace data into the *Mail Latency* report.

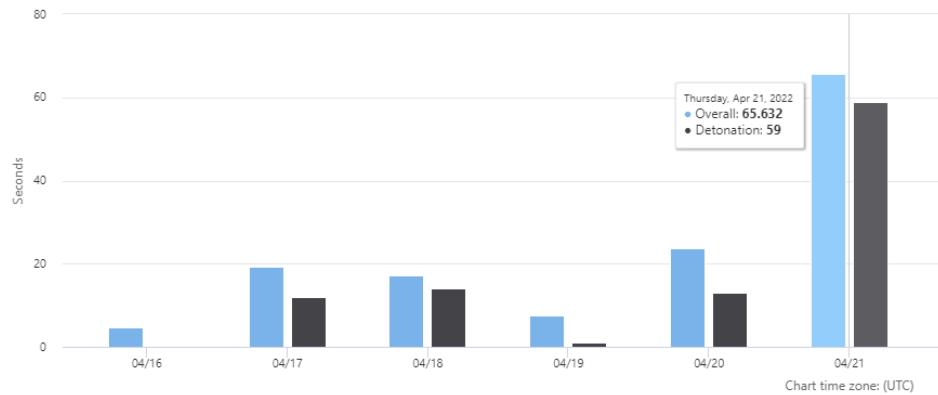
You can access this report from the **Defender portal** under **Reports > Email & collaboration**. The **Mail Latency** report (Figure 6-23) contains a bar chart and a table. The percentile tabs across the top allow you to switch the chart between the 50th, 90th, and 99th percentiles. Each bar identifies the average latency of all messages in a given day. Filters allow you to change the date range or narrow down the scope to only messages that were detonated in a sandbox.

Mail latency report

50th percentiles 90th percentiles 99th percentiles

This report shows all latency within the mail filtering and delivery pipeline. It does not include client or network latency. [Learn more about this report](#)

Filters: Date (UTC): 4/14/2022-4/26/2022 Message view: [Inline detonation](#)



Overall Detonation

[Export](#) [Refresh](#)

22 items

Date (UTC)	Latency	Message count	50th percentile	90th percentile	99th percentile
04/26/2022	Overall latency	8	46.986s	80.477s	80.477s

Figure 6-23: Mail Latency Report

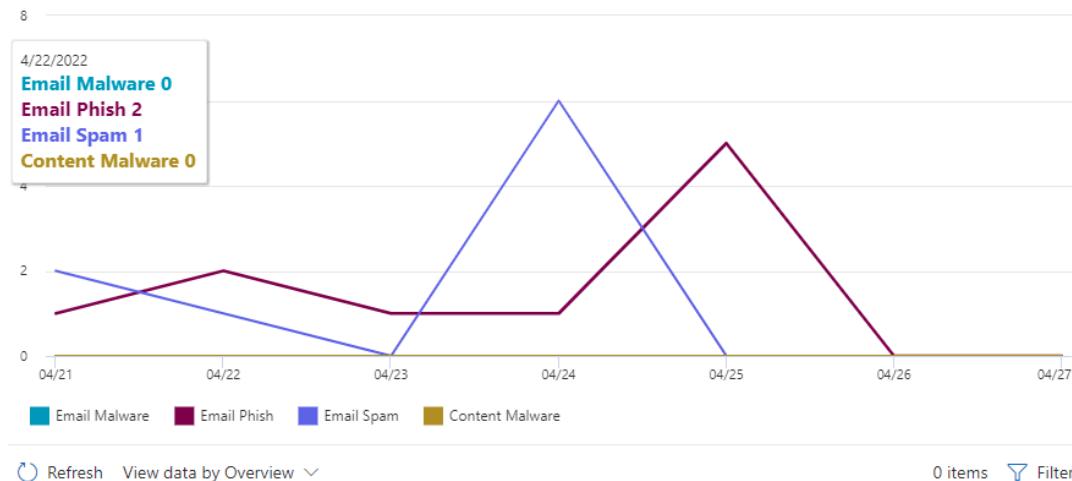
Threat Protection Status Report

In addition to the information provided by message traces, Microsoft includes several reports that give statistical information on processed messages. You can access these reports in **Defender portal** under **Reports > Email & collaboration**. The **Threat Protection Status** report shown in Figure 6-24 is an example.

Threat protection status

The Threat protection status report provides information about threats found prior to email delivery, covering relevant detection technologies, policy types, and delivery actions. [Learn more about this report](#)

Filters: Date (UTC): 4/22/2022-4/28/2022 Detection: Email Malware +3 Protected by: MDO +1 Tag: All +3 more



[Refresh](#) [View data by Overview](#) 0 items [Filter](#)

Figure 6-24: Safe Attachments reports

The reports available in the GUI are interactive and allow you to adjust the filters on the fly. For example, you can change which file types are shown or alter the date range. However, the information that fuels these reports comes from underlying message trace information. For example, suppose you specify a custom date

range that goes beyond 30 days. In that case, Exchange Online generates a historical search automatically, and you will have the ability to download the CSV report later instead of viewing it interactively on screen. More information on message traces and historical searches is in the Message Tracing section.

The reports are also available as tables showing the underlying data. To see this information and explore further (such as message ID, to and from information), click **View data by** drop-down and select something other than **Overview** (for example, *View data by Email > Phish*).

URL Threat Protection Report

Reporting on Safe Links is available in the **Defender portal** under **Reports > Email & collaboration > URL protection report** widget.

The **URL threat protection** report has two views. The default view shows the resulting action of each click. By default, this includes blocked clicks, blocked but clicked through, blocked by tenant admin, blocked by tenant admin but clicked through, clicked through during scan, and pending scan. Clicking the filter button, you can include allowed clicks, modify the date range for the report, and filter to specific domains or recipients. If your Safe Links policy has the **Do not track user clicks** option selected, this report will contain incomplete data.

Figure 6-25 illustrates the URL threat protection report, highlighting the URL click protection action view. The report shows URLs that resulted in a block page, those block pages where the user clicked through to the actual destination (if enabled in the policy), and those URLs that were the result of scanning a direct attachment as part of the URL. The actual URLs are displayed below the chart in a table.

URL threat protection

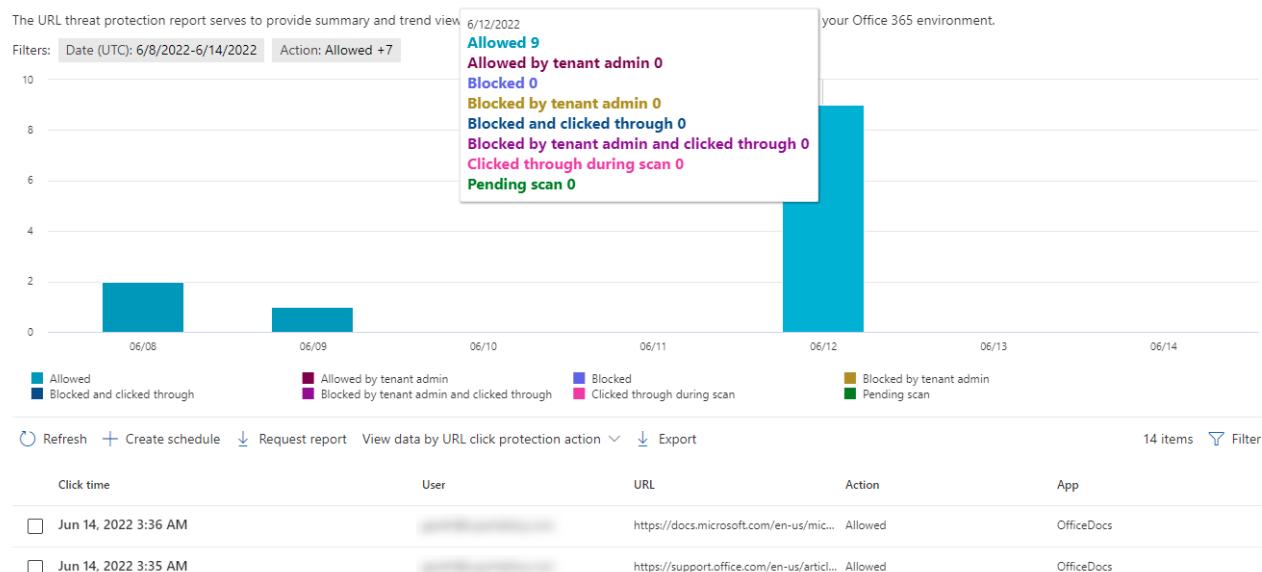


Figure 6-25: URL threat protection report, highlighting the URL click protection action view.

The second view is the **URL click by application**, which shows a breakdown across the different applications that support Safe Links. This can give insight into whether users are clicking links in email or other Microsoft 365 Apps (Word, Excel, Teams, etc.).

The basic function of the Safe Links report is to show links that were received. If enabled, the report can also detect and show what links were clicked and by whom. This makes a compelling argument for using the report because it lets you understand which users might need extra security training.

If a URL appears in your Safe Links report that you consider safe, you can add the URL or the domain to your Safe Links allow list. Always do due diligence on URLs. A reason exists for the URL to be blocked. Just because your organization might use the target website does not mean the content is safe.

Post-Delivery Activities Report

As mentioned earlier, Zero-hero auto pure (ZAP) is a feature that retroactively removes malicious content after it has been delivered to a user's mailbox. This report is particularly useful when a user reports a missing email, and you are unsure if it is due to accidental deletion or a ZAP retroactive action.

To determine if ZAP removed the email, go to the **Defender portal** and navigate to **Reports > Email & collaboration > Post-Delivery Activities** widget. From this report, you can identify each email reclassified as malicious, the original location of that email, and what action ZAP took on the malicious email. For example, ZAP moved the message to the user's deleted Items folder or quarantine.

Mail flow Status Report

The mail flow status report (Figure 6-26) visualizes how email is categorized in your tenant. With a date picker, mail direction, and additional filters, you can focus the statistics in the graph and table on the content you are concerned about. For example, if you select all filters, the graph and table will illustrate the total mail received, how much of it was considered good mail, how much was malware, phishing, and spam, and how much mail was impacted by either a transport rule or edge protection.

To locate this report, go to the **Defender portal** and navigate to **Reports > Email & collaboration > Mail flow status report** widget. Additionally, you can use the **Create Schedule** button to have Microsoft 365 email you a copy of this report daily, weekly, or monthly. Multiple users could be configured to receive this report, or a distribution group could be leveraged instead.

Mailflow status report



Figure 6-26: Mail flow Status Report identifying good and bad mail

You can also extract these statistics with PowerShell using the `Get-MailTrafficATPReport` cmdlet. For example, the following command will return all inbound and outbound traffic between two dates. Note that your start date can only go back 92 days.

```
Get-MailTrafficATPReport -StartDate 9/28/2023 -EndDate 9/29/2023 | Select Date, Direction, EventType, VerdictSource, MessageCount | Format-Table -AutoSize
```

Date	Direction	EventType	VerdictSource	MessageCount
9/29/2023 12:00:00 AM	Inbound	Message passed	NotSpam	6
9/29/2023 12:00:00 AM	Outbound	Message passed	NotSpam	1
9/28/2023 12:00:00 AM	Inbound	Advanced filter	Spam	1
9/28/2023 12:00:00 AM	Inbound	General filter	Spam	1
9/28/2023 12:00:00 AM	Inbound	Message passed	NotSpam	16
9/28/2023 12:00:00 AM	Inbound	Spoof external domain	Phish	1

9/28/2023 12:00:00 AM	Inbound	URL detonation	Phish	2
9/28/2023 12:00:00 AM	Outbound	Message passed	Allow	1

User Reported Messages

This report, which can be accessed via **Defender Portal > Reports > Email & collaboration reports and insights > User reported messages**, shows all junk, phishing, spam, or false positives reported by users over a given period. The report shows the last seven days by default, but this can increase to the last 30 days using filters. In addition to date range, you can apply filters to scope to a single submitter using their email address in the *Reported By* field. Other filters include the reason something was reported, for example, *No Threats* in the case of a false positive, or *Threats* in the case of a false negative, whether you want to include messages that were part of a Phish Simulation (see the section on Attack Simulation Training) or the Email or Teams message identifier.

The table below the chart identifies all messages within the specified filters. From this table, clicking on an individual message provides more details, such as:

- When the message was reported, by whom, and for what reason (e.g., Junk)
- The original threat, action taken, and delivery location of the message before being reported
- Sender display name, sender address, return path, sender IP, sender location, and recipients
- If the message passed or failed SPF, DKIM, DMARC, or COMPAUTH
- Any URLs in the message and if those URLs were malicious
- Any attachments in the message and if those attachments were malicious

In addition to the information above, after clicking a message to open its details, an administrator has the following options related to the message:

- **Open Email Entity** to launch the message in Threat Explorer. Threat Explorer provides even more details on this message, including a timeline of how the message progressed through the tenant to the recipient, an analysis of the message header with the calculated action, more details on any included attachments and URLs, and a preview of the message.
- **Take Action** to take an action, such as moving or deleting the message, adding a tenant level block, reporting the message to Microsoft, or starting a new case (or adding to an existing case) in automated investigation and response.
- **Submit to Microsoft for analysis** allows an admin to forward a user-submitted message to Microsoft for further investigation. This is particularly useful if users only submit messages to a tenant admin. This might be useful when an organization is concerned with potentially sensitive emails, especially those marked as *Not Junk*, being forwarded to Microsoft.
- **Mark as and notify** to record an administrative decision in the *Marked As* column. For example, an admin could mark an item as *No threats found*, *Phishing*, or *Spam* to help track progress on reported items.
- **View Alert** to view the related alert by opening it in the **Defender portal** in a separate window.

Non-Delivery Reports

Whenever a mail server cannot deliver a message because of a hard failure, it generates an NDR and sends the NDR to the message's originator. This happens so that the sender knows the message failed. Compare it to snail mail being "returned to sender" because the post office could not deliver the letter to its destination.

NDRs hold information about why the message delivery failed. The following example illustrates the typical information found in an NDR, saying that the recipient does not exist in the remote email system:

550 5.1.10 RESOLVER.ADR.RecipientNotFound; Recipient not found by SMTP address lookup

The receiving server generates the information in an NDR. Historically, the recipient's messaging system generates the NDR and sends it back to the originator. However, most modern messaging systems now generate NDRs based on the receiving server's information at the originating system, which significantly enhances the user experience, as outlined below.

Regular NDR messages are not very helpful for most users and often leave them wondering what to do next. On the other hand, NDRs typically also contain other details which are helpful for an administrator trying to figure out what happened.

When a user reports an NDR, it is normal to investigate to try to rectify the problem. However, when a remote system responds that a user is not known or that the remote mailbox is full, there is nothing that you can do except wait for the remote server to fix the problem. Microsoft has invested in the layout and text in the NDRs generated by Exchange Online to reduce support calls. These messages are more descriptive and helpful than is the norm with other SMTP-compliant email systems. In some cases, the advice helps the user resolve the problem themselves. Figure 6-27 is a good example. The problem is clear, and the steps necessary to deliver the message to the intended recipient are there for the user to take. In addition, the NDR still has information that could be helpful to the administrator, like the original message headers and SMTP error code.

Your message to [UserX@domain.com](#) couldn't be delivered.

UserX wasn't found at [domain.com](#)

michael	Office 365	
Action Required		Recipient
Unknown To address		

How to Fix It

The address may be misspelled or may not exist. Try one or more of the following:

- Send the message again following these steps: In Outlook, open this non-delivery report (**NDR**) and choose **Send Again** from the Report ribbon. In Outlook on the web, select this **NDR**, then select the link "**To send this message again, click here.**" Then delete and retype the entire recipient address. If prompted with an Auto-Complete List suggestion don't select it. After typing the complete address, click **Send**.
 - Contact the recipient (by phone, for example) to check that the address exists and is correct.
 - The recipient may have set up email forwarding to an incorrect address. Ask them to check that any forwarding they've set up is working correctly.
 - Clear the recipient Auto-Complete List in Outlook or Outlook on the web by following the steps in this article: [Fix email delivery issues for error code 5.1.10 in Office 365](#), and then send the message again. Retype the entire recipient address before selecting **Send**.

If the problem continues, forward this message to your email admin. If you're an email admin, refer to the [More Info for Email Admins](#) section below.

Figure 6-27: Layout for NDR message(s)

Backscatter Filtering

Spammers often send messages to random recipients on the internet and use someone else's email address to spoof the "From:" header. When one of these messages is sent to an invalid recipient, the receiving email server can generate an NDR, which is sent back to the spoofed email address instead of the spammer. These NDR messages are referred to as backscatter.

NDR messages are very useful. They can tell someone who sent a message that it was not successfully delivered, for instance, because the recipient's mailbox is full or maybe because the email address is invalid. However, false NDR messages are a nuisance for end-users, as anyone who has ever received one for a message they know they did not send will understand.

EOP applies a unique signature to each outgoing message to reduce backscatter. The signature is stored in an SMTP header called *x-microsoft-antispam-prvs*, as illustrated in the following example:

```
x-microsoft-antispam-prvs:  
<AM3PRO4MB4028F8BB1D18D36001E6876D9E60@AM3PRO4MB402.eurprd04.prod.outlook.com>
```

If an NDR message is generated for a legitimate message, it will include the signature header. When EOP processes the message, the header is recognized, and the NDR message is considered valid. However, if the received NDR message does not have the header, Exchange Online considers the message to be backscatter.

If you use EOP to protect on-premises mailboxes in a standalone configuration or a hybrid deployment, but EOP does not handle outbound mail flow, you should enable the NDR Backscatter feature. Go to the **Defender portal > Policies & rules > Threat policies > Anti-spam**, select the **Anti-Spam inbound policy (Default)**, and click **Edit spam threshold and properties**. Under **Mark as spam**, toggle **NDR backscatter** to **On**. In on-premises configurations where EOP protects both inbound and outbound mail flow, you do not need to enable the NDR Backscatter feature because the *x-microsoft-antispam-prvs* header is added to all outbound messages automatically.

Message Tracing

Most Exchange administrators are familiar with the following scenario: a user calls the helpdesk to report, "Person X sent me a message a few hours ago, but I still haven't received it." Sometimes messages are misaddressed, the sender has not sent the email, or they are not delivered when expected, or the message was sent but never arrived in the recipient's inbox. For instance, a mail flow rule might forward the message to a different mailbox, or the message may go into the user's junk email folder instead of the inbox.

Message tracing proves particularly helpful to troubleshoot scenarios like the ones mentioned earlier as it allows you to figure out what happened to a message, when it was delivered or why it was rejected, quarantined, or perhaps deferred. Exchange Online keeps message tracking data for 90 days. Today, you can trace message in several ways:

- Through the **Mail flow > Message trace** section of the EAC.
- Using PowerShell with the *Get-MessageTrace* and *Get-HistoricalSearch* cmdlets.

Exchange Online separates traces into recent messages (up to ten days old) and those over a longer timeframe (from ten to ninety days old). Recent message traces are done interactively, and you see the results on-screen. However, if you need to track messages older than ten days or if you need to create a report with extended information, you use a *historical search* instead. Unlike Exchange Server, message tracking information is available online for a limited period before it moves into the reporting data warehouse. Historical searches run in the background, and the results can be downloaded once the search is complete. It may take several hours for a historical search to complete.

Tracing Messages

To run message traces in the Exchange admin center, go to the **Mail flow > Message trace** section. You can create new custom traces, choose from one of the pre-defined or previously saved trace reports and view the results of finished/pending traces. The pre-defined trace options are a great way to quickly start a trace you regularly use with the same options. Most of the time, however, you will create a new (custom) trace using one of the following parameters:

- **Sender** and **Recipient** allow you to specify who sent or received the message. If you need to specify an external sender's address in the recipient picker, type it in manually and click **OK**.
- **Time range**. By default, a trace is scoped to the last 48 hours. However, you can edit the scope to span up to the last 90 days. You can also provide a custom scope with specific start and end dates and times (within the last 90 days). Searches over ten days old are performed as background searches, and the results are emailed to you once they are complete.
- **Delivery status** allows the administrator to target messages based on what action was performed. Among other things, you can specify to search for quarantined messages, filtered as spam, failed, or messages that have yet to be cataloged with getting status. If you are unsure what happened to the message, the default selection of **All** works best.
- **Message ID**. Each message has a unique message ID. You can find the ID from the message headers to scope the message trace to a single message.
- **Direction** specifies if the message was sent (outbound) or received (inbound).
- **Original client IP address** is the IP address of the sender's messaging service/server.

When executing a historical or **extended report** search, you must also specify the following:

- **Report Title**. The subject of the email that is sent to the notification email address.
- **Notification email address** of the person to whom the report should be sent.

Real-world: Exchange Online automatically decides when to start a historical search. You can quickly distinguish between a regular search from a historical search when creating a new trace. When the text on the **Search** button changes to **Next**, a historical search is created instead, and you will have to wait for the results to be available. This is true for all traces for which you request an extended report, regardless of the date range.

Viewing Trace Results

There are two ways to view trace results: interactively (when running a regular search) or through a CSV file (downloadable results from searches over more than 10 days). The format of the CSV file makes it easy to sort through the information and create custom views quickly. However, extended reports are restricted to including a sender or recipient or message ID. Standard searches can be time-based only with no other restrictions. On the other hand, the interactive results are generally more interesting for troubleshooting purposes for various reasons: they show you more information on the various events that apply to the message while in transit. In addition, you can quickly find related messages, making troubleshooting easy.

Trace results show the message status and the message events. The events include information about the message as it made its way through the various filtering mechanisms in EOP. Although you can derive the same information from the raw message events, the way results are displayed on screen makes it easy to find information about whether a message was delivered successfully and, in case it was not, why not.

In addition to the message status, each trace has extra information in a more human-readable format. For example, it might tell you how to fix a problem when a message was not delivered successfully, or it will tell you if a message was forwarded to another recipient. Figure 6-28 shows an example where a message goes to a mailbox that cannot accept the message. Note how the GUI highlights the status and cause of the problem and suggests a solution.

Message Center Major Change Update Notification

The screenshot shows a detailed message trace report. At the top, there are buttons for 'Copy report text below' and 'Prepare and email extended report'. Below this, a table shows the 'Sender' (o365mc@microsoft.com) and 'Recipient' (redacted). A progress bar indicates the message was 'Received' (green), 'Processed' (grey), and 'Not delivered' (red). A section titled 'Status' explains that Office 365 received the message but couldn't deliver it due to a recipient not found by SMTP address lookup. An 'Error: 550 5.1.10 RESOLVER.ADR.RecipientNotFound' message is shown. A note states that an NDR message was sent to o365mc@microsoft.com. Below this, a 'How to fix it' section advises asking the sender to forward the NDR for guidance. A 'Message events' section lists two entries: a 'Receive' event at 6/25/2021, 8:17 AM, and a 'Fail' event at the same time with the reason being the recipient not found.

Event	Date (UTC)	Detail
Receive	6/25/2021, 8:17 AM	Message received by: BY5...
Fail	6/25/2021, 8:17 AM	Reason: [[LED=550 5.1.10 ... Reason: [[LED=550 5.1.10 RESOLVER.ADR.RecipientNotFound: Recipient not found by SMTP address lookup];{MSG=};{FQDN=}; {IP=};{LRT=}]]

Figure 6-28: Viewing trace results in the Exchange Admin Center

Tracing Messages with PowerShell

Tracing messages in PowerShell is easy. The sole difference from the approach taken by the Exchange admin center is that you use different cmdlets to start a regular or historical search. A regular search, which can trace messages for up to ten days, is started using the `Get-MessageTrace` cmdlet. For instance, to view all messages from the past 48 hours, run the following command:

```
Get-MessageTrace -StartDate (Get-Date).AddDays(-2) -EndDate (Get-Date) | Select Received, SenderAddress, RecipientAddress, Subject
```

Received	SenderAddress	RecipientAddress
9 Oct 2018 08:16:39	michel@eightwone.com	kim.akers@office365itpros.com
9 Oct 2018 08:14:43	newsletter@bloemandwild.com	deirdre.smith@office365itpros.com
9 Oct 2018 08:13:20	michel@eightwone.com	ben.owens@office365itpros.com...

Additional parameters are available for `Get-MessageTrace` to scope trace results, such as looking for messages sent by specific mailboxes. Working examples of how to use PowerShell to extract and use message trace data can be found in these articles:

- [Report email sent to external recipients.](#)
- [Analyze email sent to internal and external destinations.](#)
- [Analyze volume of email sent outbound and received from other domains.](#)
- [Find inactive distribution lists using message trace data.](#)

Extra Detail in Message Traces

When you run a message trace in the Exchange admin center, Exchange Online automatically returns extra routing information with more details about what happened to the message while it was in transit. When

using PowerShell traces, to get the same results, pipe the results from the message trace to the *Get-MessageTraceDetails* cmdlet as shown below:

```
Get-MessageTrace -StartDate (Get-Date).AddDays(-2) -EndDate (Get-Date) | Get-MessageTraceDetail | Select MessageID, Date, Event, Detail, Data | Out-GridView
```

Historical Message Traces

The *Start-HistoricalSearch* cmdlet launches a historical search and is used similarly to *Get-MessageTrace*. For instance, to start a search for messages from a certain sender in the past 90 days and send the report to admin@office365itpros.com, you would use the following PowerShell cmdlet:

```
Start-HistoricalSearch -ReportTitle "Historical Search" -NotifyAddress "admin@office365itpros.com" -StartDate (Get-Date).AddDays(-90) -EndDate (Get-Date) -ReportType MessageTraceDetail -Sender Kim.Akers@office365itpros.com
```

JobId	SubmitDate	ReportTitle	Status	Rows
ef59-4710-81f3-f511e0bc2222	8 Oct 2018 16:14:04	Historical Search	NotStarted	0

The *ReportType* parameter controls how much detail is returned. For instance, to include the full routing details, the *ReportType* is changed to *MessageTraceDetail*. The *Get-HistoricalSearch* cmdlet checks the status of searches. When the search is complete, you can download the CSV file containing its results.

```
Get-HistoricalSearch | Where-Object {$_.Status -eq "InProgress"} | Select-Object SubmitDate, ReportTitle, Status | Format-Table -AutoSize
```

SubmitDate	ReportTitle	Status
8 Oct 2023 16:14:04	Historical Search	InProgress

A single *Get-HistoricalSearch* search is limited to 100 recipient or sender addresses. If you need to search over more recipients or senders, you must split the search over multiple searches and combine the results. A historical search can return up to 100,000 records and a tenant can run up to 25 historical search jobs daily.

An example of using the data generated by historical message trace searches to create an inbound email report for a tenant over the last 90 days is [described in this article](#). Another example is using historical message trace data to assess [whether distribution lists have been used over the last 90 days](#).

Transport Limits

Microsoft imposes several transport-related limits on its service to protect its service from those who would like to abuse Exchange Online by using it to send spam and to ensure that every tenant is treated equally. As you plan to use Exchange Online and EOP for your message routing, you should be familiar with the limits Microsoft imposes.

Without limits, a single user could, in theory, send hundreds of thousands of messages daily. As a result, the transport subsystem would consume enormous resources to process those messages and reduce its capacity to process legitimate emails. To address this, transport limits are imposed at various levels and are the same for all tenants, regardless of the license plan you subscribe to.

Table 6-6 lists the various limits imposed in Exchange Online. See [this page for the complete list of limits](#) imposed by Microsoft on other plans.

Feature	Limit	Additional Information
<i>Recipient rate limit</i>	10,000 recipients per day.	To discourage the delivery of unsolicited bulk messages, Exchange Online uses recipient limits to prevent users and applications from sending large

<i>External recipient rate limit (from January 2025)</i>	2,000 recipients per day.	volumes of email. Distribution lists count as a single recipient.
<i>HVE recipient rate limit</i>	100,000 internal recipients per day, 2,000 external.	HVE limits apply while HVE is in preview, subject to change when HVE reaches GA.
<i>Recipient limit</i>	500 recipients	The number of recipients you can add to a single message defaults to 500, but a value from 1 to 1000 can be set per mailbox or as a tenant-wide default.
<i>Message rate limit</i>	30 messages per minute	The number of messages the transport subsystem will process per minute, sometimes referred to as the throttling threshold, over SMTP client submission.
<i>HVE message rate limit</i>	Unlimited	HVE limits apply while HVE is in preview, subject to change when HVE reaches GA.
<i>Message size limit (Outlook)</i>	150 MB	The maximum size of a message when sent through Outlook.
<i>Message size limit (OWA)</i>	112 MB	The maximum size of a message when sent through OWA.
<i>Message size limit (Outlook for Mac)</i>	150 MB	The maximum size of a message when sent through Outlook for Mac.
<i>File attachments limit</i>	250 attachments	The maximum amount of attachments that can be added to a single message.
<i>Subject length limit</i>	255 characters	The maximum length of a message subject.
<i>File attachment size limit (Outlook)</i>	150 MB	The maximum size of a single attachment when sent through Outlook.
<i>File attachment size limit (OWA)</i>	112 MB	The maximum size of a single attachment when sent through Outlook.
<i>File attachment size limit (Outlook for Mac)</i>	150 MB	The maximum size of a single attachment when sent through Outlook for Mac.
<i>SMTP Authenticated Submission limit</i>	3 concurrent connections	Three concurrent connections are allowed to send email messages at the same time from the same mailbox. This limit typically impacts third-party email clients and devices, such as multi-function printers configured to log in to a single mailbox. The mailbox the client or device authenticates into allows three concurrent connections as well as storing the items it sends in the Sent Items folder.
<i>Reply All Storm Protection</i>	10 reply-all messages to over 2,500 recipients in 60 minutes (default settings)	Further replies to the conversation are blocked for six hours. An NDR is sent to people who try to respond during this time, saying that the "conversation is too busy with too many people" and educating them not to use Reply-All. The number of recipients, responses, and block duration are customizable . The 60-minute detection window is not.
<i>Scanning limits for the content of attachments</i>	1MB	The mail flow rule conditions enable you to examine the content of message attachments, but only the first 1 MB of the text extracted from an attachment is inspected. This 1 MB limit refers to the text extracted from the attachment, not the attachment's file size. For example, a 2 MB file may contain less than 1 MB of text, so all of the text would be inspected.

<i>Message Expiration</i>	1 day	If a message can't be delivered due to a temporary error, Exchange Online will attempt to resend that message until it either succeeds or the message expiration threshold is met. By default, Exchange Online will keep retrying to send a message for up to 24 hours. An administrator can customize this threshold to be any value between 12 and 24 hours using <i>Set-TransportConfig</i> . Note that this does not apply to messages which receive permanent errors. Permanent errors result in an immediate non-delivery report (NDR).
---------------------------	-------	---

Table 6-6: Transport limits for Exchange Online

Note: Beginning January 2025, Microsoft will start to enforce an external recipient rate (ERR) limit of 2000 recipients per 24 hours. The enforcement will consist of two phases: First, the limit will apply to mailboxes hosted in Exchange Online and new tenants. Between July and December 2025, the limit will be applied to mailboxes in existing tenants. The limit will be part of the overall 10,000 recipient rate limit shown in Table 6-6. This control limits senders to send messages to 2,000 external recipients per day from a total of 10,000 recipients per day. Organizations that require sending emails to higher volumes of external recipients from a single mailbox are recommended to consider using [Azure Communication Services for E-mail](#). More details in [MC787382](#).

In general, Microsoft does not grant exceptions to any of these limits. Although you can raise a support request to increase the limits, the chances of succeeding are slim. Instead, many of these limits can be worked around. A good example is the 10,000 recipients per day limit. It is common for large organizations to broadcast corporate communication messages to all users. If you have more than 10,000 users, you will not be able to send the message to everyone at once. Instead of adding individual recipients to a message, you should use a distribution group. Each distribution group can hold up to 100,000 recipients and is counted only as a single recipient.

Another example is an organization where the marketing department must send customers messages. At a rate of 30 messages per minute, 'only' 43,200 messages can be sent per day. Microsoft recommends using a third-party mass-mailing service for this purpose, such as SendGrid or MailChimp.

Real-world: The actual message size can vary from client to client and differs for messages routed outside Exchange Online. In the latter scenario, messages could grow roughly 33% because of extra encoding, effectively lowering the maximum size from 150MB to approximately 112 MB. The above limits also used to be much lower. Over time, Microsoft gradually increased the maximum supported message sizes, but they did not change the default maximum message size. As such, even a new tenant imposes a 35 MB message size limit for every user by default. An [excellent article](#) outlines how to determine a user's current configured limit and how you can modify that limit to a value within the boundaries of the supported maximum sizes described in Table 6-6.

Chapter 7: Managing SharePoint and OneDrive for Business

Juan Carlos González

SharePoint Online and OneDrive for Business are core workloads giving tenants the ability to store documents and information and build modern workplace solutions and services. This chapter focuses on describing how to manage both services (collectively referred to by Microsoft as **ODSP**) using the administrative interfaces, PowerShell, and available APIs. We also describe some basic SharePoint concepts and points to consider when migrating from SharePoint on-premises and on-premises file servers to SharePoint Online and OneDrive for Business. Finally, we cover how applications and services such as Microsoft Stream, Microsoft Lists, Microsoft Search, Microsoft Syntex, and Microsoft Viva leverage the SharePoint Online platform.

SharePoint Online

[SharePoint Online](#) is a core Microsoft 365 service used by hundreds of thousands of organizations worldwide for Intranets, Team Sites, and Content Management among other scenarios. It is also a key component for other workloads and services such as Microsoft Teams, Planner, some Microsoft Viva flavors or Microsoft Loop. At the Microsoft Ignite conference in November 2023, Microsoft said that over 300 million users add 2.3 billion new documents to SharePoint Online daily. Given that Teams has more than 320 million monthly active users, it's unsurprising that SharePoint Online has this level of activity. In May 2023, Microsoft said that tenants [generate more than 200 petabytes of SharePoint Online content monthly](#).

Much of SharePoint's success comes from a thriving developer community and the many applications they create to run on top of SharePoint. Some of those applications are available for SharePoint Online and more will come, which in turn creates further opportunities for tenants to exploit the platform.

Organizations use SharePoint Online as a standalone service to build Intranet, Extranet, or other types of portals, or to deliver content management services to other applications. Microsoft 365 Groups, Microsoft Stream, Microsoft Loop, and Microsoft Teams are examples where applications include SharePoint Online in collaborative experiences:

- **Teams:** Each team has its own SharePoint site. Each standard team channel has a folder to store messages and files shared between team members. Private and shared channels have their own SharePoint Online sites with access restricted to the channel membership.
- **Planner:** Stores attachments for tasks in the SharePoint Online site belonging to the underlying Group.

Managing documents and other files is the common thread running through SharePoint Online. The Microsoft 365 substrate together with the Graph and its growing collection of REST-based APIs is the platform; SharePoint Online contributes the ability to manage large collections of documents and metadata in that platform and offers native extensibility through elements such as the SharePoint Framework (SPFx), PnP extensibility model, Site Scripts and Site Templates, Microsoft Lists, Power Apps or Power Automate.

SharePoint Online is a critical piece of the overall story. Any deployment that seeks to move workload into the cloud must incorporate SharePoint Online into the plans to extract full value from its cloud investment.

Sites and Site Collections: In SharePoint on-premises and the early days of SharePoint Online, it was common to discuss information architectures based on creating several site collections or several subsites under a single site collection. Today, thanks to the influence of applications like Teams and Groups, most site collections consist of one site and Microsoft has moved away from talking about site collections in favor of sites. Although a site collection is the more correct term and still appears in the documentation, a site is equally valid and is, in most cases, what you deal with.

Basic SharePoint Online Concepts

Those who have not used the on-premises version of SharePoint are probably unaware of the basic concepts that underpin the operation of the application. Here is a quick guide to the major SharePoint terms and components.

Sites

A **Site** is the basic unit for SharePoint Online and is the place to keep and manage content. To enable easier administration and to group sites with a common purpose, older deployments often organize sites into **Site Collections**. Inside Microsoft 365, the rule is to use single-site collections. For example, the sites used by Groups (including those used by Teams and Viva Engage communities) are single-site collections. This book refers to site collections as sites.

Sites are the entry point to the SharePoint Online start page. SharePoint Online decides what sites appear on a user's start page based on the user's recent activity. Signals stored in the Microsoft Graph gathered from user interaction with SharePoint Online team sites and group document libraries (including those used by Teams) are the basis for suggested sites. From the home page, you can create new sites (modern team sites or communication sites) and news items posted to any site the current user can access.

Each site can have its own security, layout, theme, navigation, regional settings, and custom search settings. A site can also have processes to ensure that the information held on the site is processed in a specific manner. The latest form of sites is known as modern SharePoint Online sites, including "group-enabled" team sites, modern team sites, and communication sites. A "Group-enabled" site is associated with a Microsoft 365 Group, which is responsible for the management of the site membership. [Communication sites](#) are mobile-friendly and configured to communicate and dynamically display information. Their role is to serve up information to users drawn from different sources available to SharePoint. Finally, modern team sites are similar to "group-enabled" team sites but without an underlying Microsoft 365 Group.

Hub Sites

Communication sites present news and visually rich content, making them the best choice for sites around a single topic. The web parts available for Communication sites and the pages are mobile-friendly. They are a great solution for building real-world Intranets. Hub Sites provide the glue to group modern sites with a common purpose sharing elements such as branding or navigation.

[Hub sites](#) integrate multiple Communication and team sites to build a real Intranet or general-purpose portals such as employee portals, division portals, or department portals. For example, it is possible to have several enterprise departments, each with its own team site for collaboration, together with multiple Communication sites with news and updates, interconnected to become an information gateway, without having to create the sites as a single hierarchical collection.

Hub Site Limits: The [number of Hub Sites that can be created by](#) a tenant is currently limited to 2,000.

A Hub site can aggregate news, events, and highlighted contents from all its associated sites and fulfill some other valuable functions: it adds consistent branding across all sites and a common menu, making it easier to navigate between the sites. Each hub site includes cumulative analytics for its connected sites through the site usage page. Users can search within the complete Hub site components and can use the digest option to organize selected news stories to go out as an email summary including images and links.

Tenant Home Site

A Home site is a type of Communication site bringing together news, events, embedded video and conversations, and other resources to deliver an engaging experience that reflects your organization's voice, priorities, and brand.

You can designate a Communication site as a Home site for the tenant by running the `Set-SPOHomeSite` cmdlet, or through the [Viva Connections admin center](#). The site can be registered as a hub site but can't be associated with a hub. After executing the cmdlet, SharePoint sets the Home site to be an organizational news site and configures it for organization-wide search. By default, [only a single Home Site can be configured per tenant](#). To configure additional Home Sites, users must have a Microsoft Viva Suite or Viva Communications and Communities license.

Modern Information Architectures for SharePoint Online

Before the arrival of modern SharePoint Online sites, the typical SharePoint deployment followed a classic pattern based on a hierarchical structure of sites and subsites with inherited permissions, navigation, and common branding. On-premises deployments use this architecture, and many organizations brought the approach to SharePoint Online. While popular, architectures based on this pattern can be difficult to maintain, inflexible, and sometimes suffer performance problems. Microsoft introduced a different information architecture based on single-site collections that can be associated with a Hub site. The new approach has a flat structure that makes it easy to share navigation, branding, and other elements. It is known as a *Flat Information Architecture* and is the [de facto standard promoted by Microsoft](#) for the design of SharePoint Online deployments.

Site Limits for SharePoint Lists, Libraries, and Subsites: Microsoft recommends a maximum of 2,000 lists and libraries per site and 2,000 subsites per site. Microsoft enforces these long-standing limits for SharePoint to ensure site performance. Sites that exceed the limit will no longer be able to add new libraries or lists. Similarly, any site that exceeds the limit of 2,000 subsites will no longer be able to add new subsites.

SharePoint Search

SharePoint Online uses Microsoft Search Service to create content indexes from the files kept on sites. The Search box on the SharePoint Online home page allows users to find content using different scopes (Sites, Files, People, News, Images, and Power BI). In the case of the Files and Sites scopes, Microsoft Search returns all the sites (including OneDrive for Business sites) and files and/or folders the user has access to that contain the search term. News and people scopes provide results of any news containing the search term and any user whose user profile includes that term. Each site also has a search capability, but in this case, the scope of the search is limited to the site.

Pages

Modern pages are one of the key elements of SharePoint Online sites. They are fast, easy to author, and support rich multimedia content to make sure that they look great on any device, in a browser, or within the SharePoint mobile app. Examples of how to use modern Sites and pages include status and trip reports, guides, and frequently asked questions. SharePoint Modern pages use modern customizable Web Parts to meet business needs, supporting the addition of documents, videos, images, site activities, community feeds,

and additional items. In addition, the user experience of adding content to modern pages is different: just click the plus sign and pick a Web Part from the toolbox to start customizing a modern page. Using the [SharePoint Framework](#) (SPFx), developers can build custom Web Parts that show up directly in the toolbox. SPFx also supports the creation of SPFx extensions to customize specific areas in SharePoint modern pages such as the page footer and page header, or modern list and document libraries, by placing new actions in the list/document library command bar or the item/document menu or customizing Microsoft Search in SharePoint Online. Microsoft Viva Connections uses SPFx through the deployment of out-of-the-box Adaptive Cards Extensions (ACE) or custom ones to the Viva Connections dashboard.

Apps

Sites can include *Apps* (or Add-ins) and Web Parts to expand the functionality available through the site. If enabled, site administrators or users with full control permission can add custom apps developed by the organization or by third parties to a site using the SharePoint store.

Document libraries and *Microsoft Lists* are common examples of Add-ins used with SharePoint sites. Document libraries manage documents belonging to the site. Microsoft Lists are a great way to [create business Apps](#) to share, store, and track information of interest either for individual (personal Lists) or workgroup purposes.

On an ongoing basis, Microsoft adds new features to improve the overall user experience when working with Microsoft Lists and Document libraries. Examples include:

- Allowing users to create a new list from scratch, create a new list from an existing list or template, or create a list from an Excel table. Similarly, users can create new document libraries from existing libraries or a template (There are currently three templates available to create document libraries: Media library, Invoices, and Learning).
- Adding a new rich-text editor for text fields in lists and document libraries.
- Conditionally show or hide columns in a list or a document library form based on a value in another column.
- Being able to customize list and document library forms using JSON code.

Metadata

Document management systems depend on metadata to organize and find information. Although users do not need to add metadata to documents (apart from a title and file name) when they add them to a SharePoint document library, it is a good idea to coach people to pay attention to the titles, tags, and comments that they can add to documents, plus any other metadata considered necessary for certain types of documents. The big pay-off is that documents with accurate metadata are easier to find with Microsoft Search and eDiscovery searches.

File Versioning

Versioning is a useful feature that does not exist for documents stored on local drives or file shares. File versioning allows you to keep multiple versions of documents and revert to an earlier version if necessary. For example, a file might become corrupt because of a hardware or software problem or a cyberattack might encrypt the files in a document library. File versioning supports many SharePoint features, including:

- Users can restore a previous version of a document to become the current version with the Version history option in the SharePoint Online and OneDrive for Business browser clients. Restoration of a previous version is also possible for any file synchronized with the OneDrive sync client through the Version history option in File Explorer, macOS Finder, and OneDrive Activity Feed.
- Microsoft 365 Enterprise Apps (desktop) and Online applications (Word, Excel, and PowerPoint) use file versioning for document AutoSave. These apps can open a previous version of a document and compare its content against the current version. Apps can also restore a previous version.

- The continual synchronization of changes made to documents permits real-time updates for co-authoring of Office documents.
- SharePoint Online and OneDrive for Business can restore document libraries to a point in time within the past 30 days.

[SharePoint Online supports the concept of major and minor versions](#) while OneDrive for Business only supports major versions. No technical difference exists between a major and minor version of a document. Both represent updates to files and the difference between the two exists in how a user regards the number and importance of changes they made in a version. By default, SharePoint Online and OneDrive for Business libraries support [a minimum of one hundred major versions](#). You can't disable versioning in library settings through the versioning settings page for a given Document library and you must choose a value between 100 and 50,000 for the number of versions kept. To use versioning on lists, you must enable it first.

Keeping hundreds of versions of documents might seem excessive, but if those versions are not present, it might not be possible to recover important documents to a specific point in time. Organizations that don't want to enable minimum versioning must run *Set-SPOTenant* to disable the feature. To disable the feature, download the latest version of the PowerShell module for SharePoint Online and run the command:

```
Set-SPOTenant -EnableMinimumVersionRequirement $False
```

Site owners can set Version time limits (in preview) for Document libraries to delete file versions based on age. Three options exist:

- No time limit: Versions won't be deleted based on their age.
- Automatic: Versions are deleted over time based on activity and how long ago the file was first created.
- Manual: Versions are deleted when they exceed a specific number of days configured.

Users can view the version expiration setting applied to a file through the Expiring in column available in the file's Version history view.

AutoSave

The AutoSave feature in Microsoft 365 Apps (Word, PowerPoint, and Excel) automatically captures changes made to documents stored in SharePoint and OneDrive for Business libraries. The idea is that a user can work on a document without having to worry about saving it because any change they make is saved to the server on an ongoing basis. The feature isn't supported for files stored on local or shared drives. AutoSave uses versioning to capture edits made using the Office desktop applications and online apps. AutoSave is unsupported for non-Office files because only the Office apps can synchronize small differential changes back to SharePoint to create new versions on the server.

SharePoint Online doesn't generate a new version of a file for each change made to a document. Sets of changes are gathered by the server and are periodically committed to creating a new version. During a session, a new version might be generated every ten minutes or so, depending on the volume and type of edits in a document. For instance, pasting a large amount of text into a document usually forces Word to create a new version. If the app loses connection to the server, the server creates a new version to make sure that no data is lost.

A long editing session can easily generate 20-30 versions of a document. In some cases, SharePoint Online keeps many more versions. For instance, the chapter files for this book typically generate several hundred versions over the course of a year. The storage requirement for versions is mitigated using shredded storage in SharePoint Online to capture and store versions efficiently. The BLOBs used for document storage are broken up into "shreds" (roughly 64KB). As users update documents and create versions, SharePoint only

needs to update the affected shreds. When documents are opened, SharePoint combines the shreds and delivers the complete file.

Continuously saving documents as changes occur makes the Office co-authoring feature more seamless. Updates made to a file by one user are synchronized to the server and back to the copies opened by other users within seconds. Co-authoring is possible without AutoSave, but users must manually refresh their copies of documents to see changes.

You can [change AutoSave options in the Microsoft 365 Apps or update group policy settings](#), but you cannot affect how the cloud Office apps save document edits.

SharePoint Online Quotas and Limits

Many [SharePoint on-premises boundaries and limits](#) exist in its cloud counterpart, but there are [some specific limits](#) that only apply to SharePoint Online. For instance, a tenant can create up to two million sites and a single site can store up to 25 TB of information.

On-premises SharePoint servers use SQL databases to store site data. SharePoint Online also uses SQL (or rather Azure SQL), but the management of storage is much simplified in that Microsoft takes care of this for tenants. The storage limit for a tenant is calculated based on the Microsoft 365 licenses owned by the tenant plus any added storage the tenant buys from Microsoft. Briefly, the storage quota for a tenant is:

1 TB plus 10 GB per licensed user plus purchased storage

Thus, a tenant with 200 licensed users has a SharePoint Online storage base of 3 TB. If this is insufficient, the tenant can buy an unlimited (in practice) [amount of extra storage](#). The added monthly charge is based on the amount of additional storage. If your storage requirements decrease, you can change the amount of added storage or cut it altogether. In addition, users with a frontline worker license don't add any storage to the available pool for a tenant.

The Export option in the Active Sites section of the SharePoint admin center downloads a CSV file that includes storage information for each site. If you prefer, you can write your own version with PowerShell, perhaps using [this sample script from GitHub](#).

SharePoint Embedded

[SharePoint Embedded](#) is a cloud-based file storage management system accessible through Microsoft Graph APIs. SharePoint Embedded adds a third storage partition to a tenant to join those managed by SharePoint Online and OneDrive for Business. It is intended to be a storage platform for Microsoft and third-party applications wishing to build on the strength of SharePoint Online file storage and the surrounding Microsoft 365 ecosystem.

The basics of SharePoint Embedded are as follows:

- A new SharePoint partition (a File Storage Container) is created in the tenant when a developer installs or registers an Entra ID application to use SharePoint Embedded. This partition does not have a user interface and documents stored there can only be accessible via Graph APIs.
- After creating the partition, developers can start executing file operations (creating new files, deleting existing files, getting a list of files available, or sharing files) using Graph APIs. In Graph terms, the partition contains a single drive, similar to a document library, and the Graph requests used to manage files stored in the drive are the same as those used with a SharePoint Online document library or OneDrive for Business account.
- The application is responsible for all elements of the user interface.
- Third-party application consumption of SharePoint Embedded storage is billed through a metered consumption model paid for with an Azure Subscription.

Microsoft products such as Microsoft Loop, Edge workspaces, and Microsoft Designer use SharePoint Embedded. These are good examples of applications that you don't realize consume SharePoint storage.

SharePoint Embedded can be managed by users with the Global Administrator role or the SharePoint Embedded Administrator role. Both roles can perform the following tasks:

- Manage, configure, and maintain SharePoint Embedded containers.
- Enumerate and manage SharePoint Embedded containers.
- Enumerate and manage permissions for SharePoint Embedded containers.
- Manage storage of SharePoint Embedded containers.
- Assign security and compliance policies on SharePoint Embedded containers.
- Apply security and compliance policies to SharePoint Embedded containers.

Managing SharePoint Online

The management of SharePoint Online follows the same approach as other workloads, through a dedicated portal and PowerShell. This section describes how to manage SharePoint using both approaches. SharePoint Advanced Management and SharePoint Migration Tools are covered later in the chapter.

The SharePoint Online Admin Center

The SharePoint Online admin center is the portal for administrative access to SharePoint Online and OneDrive for Business. To access the portal, select **SharePoint** from the **Admin Centers** section in the Microsoft 365 admin center, or type the URL [https://\[tenant\]-admin.sharepoint.com](https://[tenant]-admin.sharepoint.com) into a browser. Note that the "-admin" part in the SharePoint admin center is critical as this tells SharePoint that you want to access the

The SharePoint Online admin center displays site information in a list view that allows the administrator to apply filters, add extra columns to expose information such as the sensitivity label assigned to sites, or find sites connected to Microsoft 365 Groups and/or Teams. Site management in the SharePoint admin center includes an option to export site data to a CSV file. The SharePoint admin center shares the same look and feel as other Microsoft 365 admin centers. Along with site management, the SharePoint admin center includes features such as displaying a summary of the SharePoint activities in the tenant and relevant messages from the Message Center and the Service Health status.

Classic SharePoint admin center features availability: Some classic SharePoint admin center features are still available in SharePoint Online, but Microsoft has already retired some of its components, including these pages: Site collections, Sharing, Access Control, classic Term Store and Geolocation.

Admin roles to Manage SharePoint Online

To administer SharePoint Online, several administrator roles can be assigned to users:

- The **Global Administrator** role. When Microsoft 365 provisions a new tenant, SharePoint Online creates several default sites and adds the Global admin as the primary administrator for each site.
- The **SharePoint Online Administrator** role. Accounts holding this role have access to the SharePoint Online admin center and can manage settings for SharePoint Online and OneDrive for Business.
- The **Global Reader** role gives read-only access to all the information and settings available in the SharePoint admin center.
- The **Site administrator** role is assigned to users by a SharePoint Online administrator or a global administrator to permit them to manage a specific site. A single site can have several administrators, but only one primary administrator. Group owners automatically become Site administrators for sites that are group-enabled, including those used by Teams. The SharePoint Online administrator can assign permissions to the primary site administrator when creating a site and can add more administrators for the site afterward. Site administrators do not have access to the SharePoint Online

Admin Center. A site administrator can be added to a site in three different ways: from the Active site list in the SharePoint admin center, PowerShell, and the site settings page.

Managing Active Sites and Deleted Sites

The Active sites list in the SharePoint admin center manages active (not deleted) sites. To see the details of a specific site, select it from the list and click the **Edit** action or the site name to display the site details panel with site usage statistics, properties (Domain, URL, Template, etc.), and different site settings (Membership, External file sharing, Microsoft 365 groups settings for group related sites or the sensitivity label applied to the site). Administrators can change the default All Sites list view at any point to use one of the default views (like Microsoft 365 Groups sites) or a custom view. For a selected site, the following management actions are available:

- **Edit:** Allow administrators access to the site details panel where they can update different site settings.
- **Membership:** Depending on the site type, you can change/modify Group owners and members (Group sites) for the selected site, change/modify primary site admins, and change/modify site owners, members, and visitors.
- **Hub:** You can promote the selected site to become a [Hub site](#) ("Register as hub site" option) or to join the site to an existing Hub site ("Associate with a hub site" option). If the site is already a Hub site, a SharePoint admin can change the Hub site settings (Display name and the users that can associate new sites to the Hub) or unregister the site as Hub site. Finally, if the site is already joined to a Hub site, the Hub site association can be changed using the "Change hub association" option.
- **Sharing:** This option configures the external sharing capability for the site (we describe the sharing options for SharePoint sites). It is also possible to access the global sharing settings page from the sharing settings panel.
- **Delete:** It deletes the selected site by moving it to the site recycle bin.
- **Storage:** If manual quota management is enabled, you can modify the storage quota for the site selected.

If the site selected is the root site in the tenant, a **Replace site** option is available. The organization can replace the root site with any other site in the tenant if that site is a team site or a communication site. The replacement site cannot be a hub site or connected to a Microsoft 365 group.

The **Your recent actions** option allows administrators to review the site actions he/she took since they signed into the SharePoint admin center such as changing storage quota for a site, adding new members to a site, or changing site sharing settings.

Logically, to create SharePoint sites, use the **Create** button. Currently, it's possible to create modern team sites (with or without associates Microsoft 365 groups), communication sites, a content center site for Microsoft Syntex, and (but not recommended) classic sites.

In the Active Sites section, you can execute the following bulk edit options:

- **Sharing:** Configure the same sharing option for the selected sites.
- **Hub associations:** Associate the selected sites with a Hub site in the tenant.
- **Delete:** Delete the selected sites and move them to the Sites recycle bin.

When you select a site or click a site name from the Active sites view, SharePoint opens the site details panel to display information about the site in four sections:

- **General:** Displays several modifiable site and group properties (Site name, Site address and Hub association for any site type. Group description and Group aliases for Group sites) along with some that are not (site template, domain site description, and who created the site). The admin center lists

the Group name and Group primary email for Group sites. If the site is a Hub site, you cannot edit the Hub association here. For group sites not connected to Teams, an informative banner and **Add Teams** button appear at the top of the section. For team-connected sites, an “Open in teams” option allows you to navigate to the linked Team. If the team has any channel sites (used for private and/or shared channels), the panel shows the number of channel sites. SharePoint administrators cannot access the content of a channel site unless they are a member of the private or shared channel owning the site.

- **Activity:** Displays information about recent site activity such as Last site activity, files stored for the site, the number of views in the last 30 days, the number of files viewed/edited in the last 30 days, and storage usage. The statistics displayed here are usually two or three days old.
- **Membership:** Displays information about site permissions together with lists of the membership of Owners and Members for Group sites and the default SharePoint Groups in the site (Owners, Members, and Visitors). For Group sites, additional owners and members can be added to the Group. For any kind of site, the default SharePoint Groups membership can be managed by adding/removing new users or groups (Security groups, Microsoft 365 Groups).
- **Settings:** For any site type, change the Sharing settings of the site, modify the Custom scripts option, or assign a sensitivity label to the site. Before you can assign a sensitivity label with container management settings to SharePoint sites, administrators must first create and publish the labels to users to allow them to apply the labels to sites. Custom scripts are blocked by default and although you can enable this setting, after 24 hours is automatically disabled again. For Group sites the following settings are available:
 - Email, where you can configure the normal email settings for the group:
 - Let people outside the organization email this team.
 - Send copies of teams emails and events to team members’ inboxes.
 - Don’t show team email address in Outlook.
 - Privacy, select the access type for the site (*Public* or *Private*).
 - Teams conversations, with the following options:
 - Allow members to edit sent messages.
 - Allow members to delete their sent messages.

Deleted sites are listed in the Deleted sites section in the SharePoint admin center. An administrator can select any deleted site and restore it using the “Restore” option. To permanently remove a site, just click the “Permanently delete” option.

Renaming Sites: The SharePoint admin center includes the ability to partially change the URL of a site by renaming the site. To rename a site, select it and edit its name in the site details panel. A detailed overview of the steps to rename a site [can be found in this article](#). You can also rename site URLs with PowerShell using the `Start-SPOSiteRename` cmdlet. Be aware that some consequences of site renaming exist, as [explained in Microsoft’s documentation](#).

Controlling Site Creation

It is possible to allow users to create new Sites Collections or restrict creation to only administrators. Because of the tight connection that Team Sites have with Microsoft 365 Groups (including Teams), this is not a simple matter as you must consider whether you want users to be able to create sites, group-enabled sites, or both.

Basic control over Site creation is achieved by showing or hiding the Create site command on the SharePoint home page of the root site. This is the button that invokes the Create Site wizard. A SharePoint tenant setting controls whether the button appears on the page for all sites. To access the setting, open the SharePoint admin center and then **Settings**. On the Settings page, click on **Site creation** and then simply switch on/off the **Users**

can create sites and then (optional) **Show the options to create a site in SharePoint and create a shared library from OneDrive** option.

Creating a Group-Connected Team Site

If the SharePoint settings for a tenant allow the creation of group-connected sites and the user can create Microsoft 365 Groups, the team site creation process creates a group. The new group holds the membership for the site and the Microsoft 365 Groups membership service is used to allow site members access to group resources.

After SharePoint creates the new group object in Entra ID, a directory synchronization process makes the existence of the new group known to Exchange Online and forces the creation of the group mailbox. While this process proceeds, the user can build out the contents of the SharePoint team site with new lists, document libraries, a customized home page, and so on. The same creation process to set up a new team site and group occurs when a user invokes this choice from OneDrive for Business.

Connect existing SharePoint Team Sites to new Microsoft 365 Groups: Existing SharePoint sites, including classic sites, can be connected to a new group (or "groupified") using the *Set-SPOSiteOffice365Group* cmdlet, SharePoint APIs, or using the **Connect to new Microsoft 365 Group** feature available in site settings options. When this happens, the existing content, hierarchy, and permissions for a site stay intact, and SharePoint Online connects the site to a new group and populates with the group membership using the existing site membership. The owner can adjust the group membership after creation. A tenant or SharePoint Online Administrator can disable this option by selecting the option **Prevent site collection administrators from connecting sites to new Microsoft 365 groups** in the **Settings** page in the classic SharePoint admin center settings page. Microsoft [gives detailed information](#) about the types of SharePoint sites that can connect to a new Microsoft 365 Group, a [scanner tool](#) to analyze if existing SharePoint sites are suitable to be connected to Groups, and PowerShell scripts to enable modern features in the Sites and configure group membership.

Settings and Permissions for Group-enabled Sites

When someone creates a new group-enabled team site, SharePoint creates a team site to host the document library and shared notebook for the group. The gear (options) menu for a site reveals the Site Information panel used to customize the details published to users about the site as well as its classification or label defining the importance of the information held in the site and the Hub site association in case the site is not a Hub itself. Also, the owner can access the Site Permissions panel and set the desired level of access for different member types.

The default configuration for a group-enabled site is that group owners have SharePoint full control permissions over the site, while group members have SharePoint Edit permissions. If the site is public, every account in the tenant excluding external users has SharePoint Edit permissions. Amend the permissions for the site to restrict access as needed but be aware that because you are working with Microsoft 365 Groups rather than individual user accounts (as is the case for on-premises SharePoint or classic sites), you should take care to ensure you do not interfere with the ability of group members to access the resources available to the group, or for group owners to manage the group. It is also possible to select an individual user account and give them full control of the site. This permission is a SharePoint permission over the team site and does not make the user an owner of the group.

One of the permissions you can assign to a site is "Share Site Only" access, which means that the owner can give someone access only to the SharePoint resources instead of all the resources belonging to the group. Also, it is possible to assign a user read-only access to the site, which removes their ability to edit or remove data from the site (they might still be able to share files from the site). Assigning read-only access to users is a

good approach to take for sites holding information (like HR documents) and it is necessary to make the site content generally available.

Apart from the ability to set access to site control through these settings, it is unwise to try and use traditional SharePoint access control over team sites used with groups because these controls expect to deal with individual users rather than when an identity is shared by group members.

Associating Sites with Hub Sites

A Hub site is a modern team site, a communication site registered as a Hub using PowerShell, or a site converted to be a Hub site using the "Register as hub site" option in the SharePoint admin center. [Registering a hub site with PowerShell](#) can be done with cmdlets from the SharePoint Online module or PnP cmdlets (we discuss how to manage SharePoint Online with PowerShell later). This code opens a connection to the tenant and then creates a team site, elevates it to a Hub site, and associates other sites with the Hub.

```
Connect-SPOService -Url https://<TenantName>-admin.sharepoint.com
Connect-PnPOnline -SPOManagementShell # Will ask for the site URL
New-PnPSite -Type TeamSite -title "New SiteColl" -alias "NewSite" -Description "New SiteColl"
# Create a new Site
Register-PnPHubSite -Site https://<TenantName>.sharepoint.com/sites/NewSite # Register the SiteColl
as a Hub site
New-PnPSite -Type TeamSite -title "Sub-SiteColl" -alias "SubSite" -Description "Sub-SiteColl"
# Create a sub-site collection
Add-PnPHubSiteAssociation -Site https://<TenantName>.sharepoint.com/sites/SubSite -HubSite
https://<TenantName>.sharepoint.com/sites/NewSite # Associate the subsite to the Hub site
```

Associating a site with a Hub site is a task that only site administrators and site owners can do. Hub owners can manage visitor permissions for the Hub site itself and sites joined to the Hub. This feature, off by default, can be enabled by a Hub owner through the Site permissions panel for the Hub site. When enabled, a new SharePoint Group with read permissions is created in the Hub site and Hub owners can add users, Microsoft 365 groups, and security groups (up to a maximum of 10) that can optionally synchronize with any Site joined to the Hub. The synchronization of visitor permissions from the Hub site to a site joined to the Hub must be explicitly done for each site.

A [Hub site can be associated with another Hub site](#) as a way to expand search results across multiple Hubs in an organization allowing in fact to define information architectures with more than two levels deep. Hub to Hub association is a very simple process in the SharePoint admin center:

- In the active sites list, select an existing Hub site.
- Edit the Hub settings through the Hub settings panel.
- In the **Parent hub association** field, select the Hub to associate with.
- Save the changes.

Some limitations exist for Hub sites: there's no workflow around the publishing process, anyone who has edit permissions for a site can change any element of that site, and any new story pushes older ones down the stack, making it impossible to create a "Most important" news that stays always at the top.

SharePoint Spaces

[SharePoint Spaces](#) creates mixed reality experiences on SharePoint sites. When enabled on a site (go to the Site settings page and enable the Spaces feature on the Sites features page), users can create spaces by defining a structure, background, and theme. The next step is to add Web Parts to visualize 3D objects, 360-degree images, videos, 2D images, and text. Once a space is ready, it can be viewed in a web browser or with a mixed-reality headset.

Modernization of Classic Sites

Although Microsoft introduced modern sites some years ago, it's still common to find classic sites in use. Microsoft recommends that tenants upgrade classic sites to take advantage of modern site technology. To help this modernization, Microsoft and the SharePoint community have released tools to speed up the upgrade process:

- Microsoft automatically updates any classic site with a home page that isn't customized with a modern page.
- The [SharePoint Modernization Scanner](#) is a tool originally built by the PnP Community to identify the work that must be done to modernize sites.
- The [Enable-SPOCommSite](#) cmdlet (in the SharePoint Online module) converts a classic team site (STS#0 template) that meets the requirements described in [this link](#) into a Communication site.

Managing Performance for SharePoint Sites

A key factor in the success of any SharePoint site is achieving good performance when navigating across pages on a given site. To optimize performance in SharePoint sites, two out-of-the-box tools are available:

- [Site performance page](#): is accessible by Site owners and editors through the site settings menu. This page provides access to the Page Diagnostics for SharePoint tool that identifies any performance issue present on modern SharePoint pages and suggests actions to address issues found. Page Diagnostics for SharePoint tool uses a browser extension available for Microsoft Edge and Google Chrome.
- [SharePoint Portal Launch Scheduler](#): a feature to launch specific SharePoint sites that are expected to receive high volumes of traffic using a phased deployment. The tool also includes, if needed, an automatic redirect for existing sites. The SharePoint Portal Launch Scheduler is available through the `New-SPOPortalLaunchWaves` cmdlet.

Managing SharePoint Embedded Containers

The Active containers list displays active (not deleted) SharePoint Embedded containers owned by the tenancy. To see the details of a specific container, select its name to display details such as the container name, the sensitivity label applied, when it was created, the application using the container (for instance, Loop workspaces), the storage in use, and the publisher. The container details panel also shows container membership information (Owners, Managers, Writers, and Readers). To delete a container, select the container and then Delete. To export the list of containers in the tenant, select the Export action in the Active containers list.

Deleted containers in the tenant are listed in the Deleted containers section in the SharePoint admin center. An administrator can select any deleted container and restore it using the "Restore" option. To permanently remove a container, select the "Permanently delete" option.

Managing Access Control

The SharePoint admin center includes settings through the Access control page to control access to SharePoint Online sites and OneDrive for Business accounts:

- **Unmanaged devices:** Settings to control how unmanaged devices can access SharePoint sites, OneDrive for Business (ODFB), and information stored there. Access control to SharePoint Online and ODFB is done through the creation of conditional access policies, which require an Entra ID P1 license. Among other settings, these policies can exert control over access from devices that are not compliant or joined to a domain (unmanaged devices). By default, SharePoint Online and OneDrive contents are accessible from unmanaged devices but it's possible to configure limited access or even block access through Entra ID conditional access policies, including the use of authentication contexts

with sensitivity labels. You can also apply conditional access policies at the site level as explained in [this link](#). The Identities chapter contains examples of how to process unmanaged devices in conditional access policies.

- **Idle session sign-out:** Disabled by default, [this setting](#) is a mechanism to first warn and then sign out users on unmanaged devices if they have been inactive for a period and they don't opt to stay signed in when they sign into SharePoint Online, OneDrive for Business, or Microsoft 365. Two settings can be configured when this setting is enabled: the idle session period (15 minutes minimum, 24 hours maximum) and the warning notice (one minute minimum, 30 minutes maximum). Idle session timeout can also be configured by running the [Set-SPOBrowserIdleSignOut](#) cmdlet. For example, this command enables a session timeout and sets a warning period of 45 minutes (2700 seconds) and a forced sign-out after an hour (3600 seconds). The timeout values apply to both SharePoint Online and OneDrive for Business sessions.

```
Set-SPOBrowserIdleSignOut -Enabled $True -WarnAfter (New-TimeSpan -Seconds 2700)
-SignOutAfter (New-TimeSpan -Seconds 3600)
```

- **Network location:** When configured, it lists the IP addresses from which clients can access SharePoint and OneDrive for Business.
- **Apps that don't use modern authentication:** Enabled by default, the setting blocks access to SPO from Apps that don't use modern authentication. Office 2013 or earlier clients are examples of Apps that don't use modern authentication and can pose a potential security problem for the information stored in SharePoint Online. In general, it's recommended to use this setting to block access for older clients.
- **Limit OneDrive access:** This setting limits the use and access of OneDrive for Business to users in specific (up to 10) security/Microsoft 365 groups. This setting is only available for tenants with Microsoft 365 E5 licenses or Microsoft Syntex-SharePoint Advanced management add-on.

Applying Authentication Contexts to Sites Not Owned by Groups: The easiest way to mark a site with an authentication context for processing by conditional access policies is with a sensitivity label. This is fine for sites owned by Microsoft 365 groups because these sites can inherit settings from sensitivity labels. Sites not owned by groups might also need special processing by conditional access policies. For instance, a site might contain a document library holding some sensitive files that people should not access from an external network. In these scenarios, you can mark the site using the [Set-SPOSite](#) cmdlet. For example:

```
Set-SPOSite -Identity https://office365itpros.sharepoint.com/sites/Confidential -
ConditionalAccessPolicy "CA Policy Restrict Access Confidential Documents"
AuthenticationContextName "InternalAccessOnly"
```

Managing Global SharePoint and OneDrive Settings

Management of global settings for SharePoint Online and OneDrive for Business is through the Settings section of the SharePoint admin center:

- **Home site:** Controls the selection of an existing site as the tenant's Home site. The chosen site can be removed at any point and replaced with a different site. This setting does not allow the configuration or modification of existing Home Sites for tenants where a Home site is selected through the Viva Connections experiences setup in the Microsoft 365 Admin Center. In that case, this setting displays an information panel with a link to the Viva Connections experience page.
- **Notifications:** Controls if users of the SharePoint mobile app receive notifications about site activity.
- **Pages:** This section allows administrators to change global settings for creating and commenting on modern SharePoint pages. By default, both settings are enabled.
- **Site creation:** Configure the managed path and time zone used when creating a new SharePoint site and whether end users can create sites (from SharePoint, OneDrive, PnP PowerShell, and the

SharePoint REST API). Administrators can also configure whether to show the create site option in the SharePoint home and OneDrive shared libraries section.

- **Site storage limits:** [Defines how SharePoint Online manages its storage](#). Two options are available: *Automatic* and *Manual*. Automatic quota management means that storage is handled automatically: sites use what they need when they need it. The use of manual quotas implies that a default quota limit and threshold is configured for all sites created. This default quota can be modified at site creation time. If you prefer to fine-tune the storage space allocated to each site, set the storage management option to "manual" and specify individual site storage limits.
- **Versioning history limits (in preview):** Limits the number of file versions kept in new OneDrive accounts and new SharePoint document libraries to save storage. Site owners can override this setting for individual libraries. This setting does not apply to existing OneDrive accounts or SharePoint document libraries. Two version limit options are available:
 - Automatically: Optimizes version recovery and storage without estimating limits. Versions are deleted over time based on activity and when the file was created.
 - Manually (default value): Limits versions by count or version age. The default number of major versions is set to 500. When versions exceed the version limit configured or the version age, the oldest versions are deleted.
- **Stream:** Defines the default destination for the Stream app launcher tile. Three options are available:
 - Automatically switch to Stream (on SharePoint) when recommended. This is the setting configured by default and it means that Microsoft controls what version of Stream users access through the app launcher.
 - Stream (on SharePoint).
 - Stream (Classic).
- **Link to the Classic settings page:** Gives access to several other settings from the classic SharePoint admin center.

OneDrive settings configurable in this section are explained later.

Managing Content Services

The content services section in the SharePoint Admin Center manages and publishes Content Types (A collection of metadata that defines a business concept or entity within a SharePoint site) and managed metadata (A special metadata type that allows [the definition of taxonomies and data hierarchies](#) to organize and classify content in SharePoint sites) for a SharePoint Online tenant.

Term Store

The Term Store is a central location to [create and store taxonomies, which](#) can be used to:

- Create and manage metadata fields to permit the classification of a document or a list of items through a term defined as part of a specific taxonomy.
- Improve end user experience when using search capabilities utilizing the search dictionaries that contain specific Term sets to provide features such as including or excluding words for query spelling correction.

A custom taxonomy consists of a Group, at least a term set in the Group, and terms in a term set. The maximum number of levels of nested terms in a custom taxonomy is seven. The Term Store also contains enterprise keywords and hashtags as a mechanism to allow users to tag content with existing or new keywords created by end users. The maximum number of terms supported by the Terms Store is 1,000,000. Finally, the filters panel in modern Document libraries supports managed metadata.

Content Type Gallery

The Content type gallery is a central location to manage and publish custom types to any site in the tenant. To create a new content type:

- Access the Content type gallery in the SharePoint Admin center and click **Create content type**.
- Type the information required to create a content type (Name, Description, Parent content type, and Category) and click on Save.

After the content type is created, select its name in the list of content types to access the content type details page where you can take the following actions:

- Modify the details of the content type.
- Add site columns to the content type. You can choose between adding existing site columns or creating new columns. To create a new site column, provide the name, description, category, and column type. Depending on the column type, you might need to configure additional settings.
- Publish the content type so it can be used on any site in the tenant.
- Access to advanced content type settings such as the document template to use (only for document types), permissions to enable/disable the modification of the content type, and enabling/disabling the update of the content type on sites and lists when it's updated.
- Access to the content type policy settings.
- Delete the content type.

To use the content type in an existing document library:

- Browse the document library where you want to use the content type, click + **Add column**, and then **Content type** to open the Add content type panel.
- In the panel, select the content type you want to add to the document library and click **Apply**. Note that before applying the content type you can optionally indicate if a specific view based on that content type is added to the library or if the content type columns should be added to the current view.

Any published content type in the Content Type Gallery can also be added to a site by using the [Add-PnPContentTypesFromContentTypeHub](#) PnP cmdlet. If the content type already exists in the site, the published version is synchronized to the site.

SharePoint Online Reports

The Reports section provides access to Content services, Data access governance, and OneDrive accounts reports. [Content services reports](#) are available only for tenants with a Microsoft Syntex subscription. The reports contain insights about the usage of terms and terms sets in the global Terms store across the tenant:

- **Term store operations:** A graph showing details of the Terms store operation over the last 15 days.
- **Term store composition:** Displays an overview of the number of terms in the Term store identifying the terms distribution (regular, hashtag, and keywords). From this report, it's possible to promote keywords to become terms in the Term store.
- **Open and closed term sets:** Indicates the total number of term sets and the distribution between open and closed term sets.
- **Terms without synonyms:** It reflects the percentage of terms in the Terms without synonyms or abbreviations specified.

Three [Data access governance reports](#) are available:

- **Sharing links** reports monitor sharing activity across the tenant and identify potential oversharing situations. Three kinds of sharing reports identify the sites where users create the highest number of

"Anyone", "People in your organization" and "Specific people" links. It's possible to run all reports together or one by one. It can take a few hours to generate these reports.

- **Sensitivity labels applied to files** reports the sites including files with a specific sensitivity label. To get a report for a specific label, you must add the report and then run it. Note that you cannot create more than ten sensitivity labels reports.
- **Shared with 'Everyone except external users'** reports displays sites where the Everyone except external users (EEEU) built-in group has been added as a site member, or view files, folders and lists shared with EEEU group. These reports contain data from the last 28 days.

Data access governance reports are a premium feature requiring an Office 365 E5, Microsoft 365 E5 license, or the Microsoft Syntex SharePoint Advanced Management license.

The [OneDrive accounts report](#) displays accounts that have been in an unlicensed state for more than 90 days due to one of the following reasons:

- **Retention period:** the account is no longer licensed but the retention period defined for deleted OneDrive for Business accounts stops the account from being deleted.
- **Retention policy:** the account is no longer licensed but a retention policy prevents the deletion of the account.
- **Active user with no license:** the Entra ID account owning the OneDrive for Business account is active but is not licensed for OneDrive.
- **Duplicate accounts:** An account is considered a duplicate when a licensed user has multiple OneDrive accounts associated with their account.

By downloading the OneDrive accounts report (a CSV file), administrators can see why the accounts appear on the list. Administrators can then decide to resolve the unlicensed status for the accounts by deleting the accounts if their content is no longer required.

After January 25, 2025, SharePoint Online automatically moves unlicensed OneDrive for Business accounts into Microsoft 365 Archive for long-term retention. An Azure subscription is required to pay for storing the OneDrive accounts and to restore an account from Microsoft 365 Archive. A restored account is accessible for 30 days after which SharePoint Online archives the account again.

If accounts are left in Microsoft 365 Archive for more than 180 days after becoming unlicensed and the tenant does not take out an Azure subscription to pay for the Microsoft 365 Archive storage costs, SharePoint Online can delete the accounts.

Managing SharePoint Search

Search is one of the core features in SharePoint Online that administrators [can customize](#) to ensure that end users have a great experience when searching documents by content and metadata through any site in the tenant. The search administration, which can be found in the More features section, includes the following items:

- **Search Schema:** This option provides access to the list of managed properties and crawled properties in the tenant. An Administrator can update existing managed properties or create new ones. Each managed property can be mapped to one or more crawled properties. A crawled property is just content and metadata that is extracted during a crawl from an item stored in SharePoint, such as a document, a SharePoint page, or a list item. A good overview of crawled and managed properties can be found in [this Microsoft article](#).
- **Query Suggestions:** Using this option we can upload query suggestions to the search engine so when the user enters some search criteria in the search box, search suggestions for that search criteria are shown.

- **Result Sources:** The ability to [limit searches to a subset of search results](#) is achieved through Result Sources. From the Result sources page, a SharePoint Online administrator can review existing Result sources or create new ones. The Result sources managed at this level can be used for all sites. A Site administrator or a site owner can manage result sources for a site.
- **Query Rules:** Search results can be improved through [Query rules](#) that give a mechanism to specify conditions and actions to promote the relevance of the search results that meet those conditions. As an example, we could create a query rule that boosts technology news in our Intranet that are tagged with a specific category so when someone searches for that news category, all the news in that category is displayed on the top of search results. Over time, Query rules in SharePoint online search will be replaced using answers in Microsoft Search.
- **Remove Search Results:** Lists the URLs removed from search results.
- **Search Center Settings:** This page allows administrators to define the URL of the Global Search Center in the tenant and the search results loading strategy used in the tenant.
- **Export Search and Import Search Configuration:** Those options provide a simple mechanism to export to a text file any customization done in search configuration (query rules, result sources, result types, ranking models, and site search settings) or to import a search configuration file.
- **Crawl Log Permissions:** This page lists the users with read access to crawl log information in the tenant.

Changes done in the search administration page are applied to the whole tenant, but it's also possible to customize search at the site level.

Managing Apps

SharePoint Online is extensible through [Apps or Add-ins](#). In general, two types of Apps can be added to a SharePoint site:

- **SharePoint Add-ins**, [defined by Microsoft as self-contained extensions](#) that may include logic and data deployed in the cloud, SharePoint components (such as Content types, Lists, Document libraries, etc.), and client-side scripts.
- **Web Parts and Extensions created with the SharePoint Framework**. SPFx Web Parts can be added to both classic and modern pages. SPFx extensions can only be used in the modern SharePoint experience.

SharePoint Apps are installable only from the SharePoint Store or the [global App Site](#). A tenant can have only one global App Site, a special type of site a SharePoint Online Administrator must create. Through the global App site administrators can install and distribute apps, including SPFx solutions (Web Parts, Extensions, and [Adaptive Cards Extensions](#)) for SharePoint sites, Microsoft Teams, and Viva Connections. Administrators can also distribute custom apps or install apps from the SharePoint Store. End users can request the addition of new Apps to a site through the My Apps page by browsing the SharePoint Store to select and request an app. Tenant administrators can then approve or deny the app requests. Finally, site owners can delete requested apps, even if administrators approve their installation, from the My requests section on the My Apps page.

For more granular Apps deployment and isolation, [Apps catalogs](#) can be created in specific sites. To create an App catalog, connect to SharePoint Online with PowerShell and run the following command:

```
$sSiteCollectionUrl = "https://<Site_Collection_Url>"  
Add-SPOSiteCollectionAppCatalog -Site $sSiteCollectionUrl
```

You can only install Web Parts and Extensions deployed to a site catalog in the root site and any site created in the collection, but not in any other site. To create a site catalog, the user executing the [Add-SPOSiteCollectionAppCatalog](#) cmdlet must be a site admin for the global App catalog.

Legacy Services and Settings

Some legacy services and settings originating from SharePoint on-premises exist in SharePoint Online. This section provides an overview of the legacy services and settings that can be managed through the shortcuts provided in the **More features** section in the SharePoint admin center. Table 7-1 details legacy services and settings in SharePoint Online.

Legacy service	Legacy service Details
User Profiles	The User Profiles service acts as a mechanism to modify existing user properties or add new properties. Behind the scenes, a SharePoint timer job imports account information from Entra ID into the User Profiles service.
Records Management	It allows administrators to create new Send To connections that can be used by a Content Organizer configured on a SharePoint site to route documents to a specified location (a document repository or a records center).
Secure Store	The Secure Store service is designed to manage and store the credentials needed to connect to an external data source.
Hybrid Picker	SharePoint Online and SharePoint On-Premises can be integrated and connected in a hybrid deployment. Assuming the pre-requisites required for a hybrid deployment are met, the hybrid features available are OneDrive redirection, Hybrid search, Hybrid App Launcher, Business to Business (B2B) Extranets, Hybrid Taxonomy, and Hybrid Self-Service site creation.
InfoPath FormsServices	InfoPath Forms Services enabled tenants to easily design electronic forms that can be deployed to any SharePoint site in the tenant using InfoPath Designer 2013 as an authoring tool. Microsoft has committed to support InfoPath Forms Services in Microsoft 365 and InfoPath 2013 clients until its retirement in 2026 and has positioned Power Apps as the natural replacement. To understand how InfoPath is used in an organization, Microsoft has a Power BI InfoPath report generated by the Microsoft 365 Assessment tool to scan the tenant for InfoPath usage.
Business Connectivity Services	BCS Services provided a simple mechanism to connect a SharePoint site to external business data sources such as SQL Azure Databases or any other one exposed by a Windows Communication Foundation (WCF) service. BCS is now retired from SharePoint Online . At the time of writing, Microsoft blocks BCS in new Microsoft 365 tenants. The scheduled date for complete removal of BCS is September 30, 2024. In SharePoint Online, the integration of external data in sites can be achieved by using a combination of modern cloud technologies and platforms such as Power Apps, Power Automate, Azure Logic Apps, or cloud development patterns.

Table 7-1: Legacy Services and Settings in SharePoint Online.

Managing SharePoint Online with the Microsoft Graph API

Another approach to [managing SharePoint Online is through the Microsoft Graph API](#). A settings endpoint (/sharepoint/settings) is available to query and manage many of the SharePoint (and OneDrive) tenant-wide settings that are otherwise only available in the SharePoint admin center. To use the Graph to administer SharePoint Online:

- Use the Graph Explorer (see the PowerShell book) or another Graph-capable program (like PowerShell).
- Make sure that the app has consent to use *SharePointTenantSettings.Read.All* for GET (retrieve) operations and *SharePointTenantSettings.ReadWrite.All* for PATCH (update) operations. The endpoint supports both delegate and application permissions.

As an example, the following GET request retrieves the current settings:

GET <https://graph.microsoft.com/v1.0/admin/sharepoint/settings>

To modify an existing setting, use a PATCH operation and include details of the setting (in JSON format) to modify in the request body. For instance, to disable comments in modern pages the request body is:

```
{
    "isCommentingOnSitePagesEnabled": false
}
```

After running the PATCH request, the Microsoft Graph responds with a 200 OK response and a refreshed list of the SharePoint settings. As explained in [this article](#), it's also possible to update multiple settings in one Graph request.

Sharing

As the application name implies, sharing documents, folders, and sites with internal and external users is an important SharePoint feature. Microsoft's terminology can be confusing because of the way SharePoint documentation refers to "external users." For SharePoint, an external user is someone outside the tenant. That user might have a guest user account in the tenant, created by an administrator, or because they were invited to join a Group or a Team. On the other hand, an external user can also be an ad-hoc recipient of a sharing invitation, in which case they authenticate with an access code, or they can receive an anonymous link, which allows anyone with the link to access the content.

The current advice is that SharePoint Online sharing should use the following approach:

- Use Groups and Teams to control ongoing access for external users to content in SharePoint team sites. External people who join Groups and Teams automatically get a guest user account as part of the invitation process and use those accounts to access the document library belonging to the team or group they join.
- Use guest user accounts to control access for external users for a sustained period to content in traditional SharePoint sites. You can create these accounts in the Users section of the Entra admin center. SharePoint creates guest accounts when someone shares a site with an external user.
- Use one-time passcodes (OTP) for one-time access for external users. The one-time passcodes are one-time eight-digit numbers sent to an email address contained in a sharing invitation to allow them to open content. Codes are good for 15 minutes.

SharePoint and Entra ID B2B Collaboration

SharePoint Online uses [B2B Collaboration](#) to control sharing. This means that when someone creates a sharing link, SharePoint uses the Invitation Manager to create a guest account in the tenant. The sharing link contains an invitation for that person, much like adding someone to a team or group creates a sharing invitation that the external recipient must accept before they can access resources. When the person uses the sharing link and goes through an OTP challenge to validate their credentials, Entra ID redeems the invitation and makes the guest account fully active. Thereafter the guest can use their account to access tenant resources. The resources include individual documents, folders, and sites shared with them together with Groups (including Teams) that they join. When the [Integration with B2B Collaboration](#) is enabled, SharePoint Online creates guest user accounts for all types of sharing recipients as described in Table 7-2.

Target Sharing Recipient	Sharing Steps	Guest account created
Microsoft (MSA) account.	Sharing link sent. User goes through the account validation process. Sharing happens.	Yes

Account in another directory (for example, Zoho Mail). Gmail can federate with Entra ID, in which case users sign-in directly.	Sharing link sent. User redeems OTP. Sharing happens. User must redeem a new OTP for each session.	Yes
Account in another Entra ID tenant, including those without Office 365 (like Yandex.com).	Sharing link sent. User redeems OTP. Sharing happens. User doesn't need OTP for future access.	Yes

Table 7-2: Guest accounts created by sharing activities in SharePoint Online

More information about how to manage guest accounts is in the Managing Users chapter.

Site People View: The SharePoint browser interface keeps track of external people with whom users share resources. Sometimes, errors creep into the list of external people, such as when people enter incorrect email addresses into sharing links. To remove these errors and prevent them from showing up as suggested users in sharing dialogs, a site administrator can access the list by adding `/_layouts/people.aspx?MembershipGroupId=0` to the site URL. This exposes the All People view listing all the internal and external users with access to the site. You can remove users from this list whose entry is incorrect for some reason (like a bad email address) or who no longer have access to site resources.

Sharing Controls

SharePoint Online supports up to 50,000 external shares per securable object (a site, a list/document library, a folder, or a(n) item/document), which should be enough for even the most dedicated sharer. For performance reasons, Microsoft recommends keeping the number of shares on an object to 5,000 or less. Somewhat confusingly, the settings that control how users can share SharePoint content are in two administrative consoles:

- **Microsoft 365 admin center:** Select Settings → Org settings → Security and privacy, and then sharing. A link to the sharing controls is in the Sharing side panel.
- **SharePoint admin center:** Select Policies and then Sharing.

The same basic settings for sharing controls are available through both consoles and the same values appear in each. However, you will find some differences in presentation and emphasis in the two consoles. And of course, you can use PowerShell to adjust settings too.

The **Sharing** section of the SharePoint admin center (exposes the settings to control how sharing with external people occurs within a tenant. Sharing occurs through the exchange of sharing links between the person sharing a file or folder with another internal or external person. The sharing link is a revocable secret to allow access to designated content. The link can be transferrable or confined to a set of recipients. SharePoint Online and OneDrive for Business support four types of sharing links, listed here in order from the most permissive to the most restrictive:

- **Anyone:** Also called anonymous sharing, this is the loosest permission. It allows users to share files and folders with anyone who has an email address. SharePoint sends an email with a link to allow the recipient access to the content, but anyone who subsequently has access to the link can use it to access the associated content. If you allow anonymous sharing, you can limit the lifetime of a link (to say, 7 days) and restrict access to view-only rather than view and edit.
- **New and existing guests:** Users can share with external users if those users can authenticate themselves by signing into the tenant using a guest account or by using a verification code.
- **Existing guests:** Users can share with external people, but only if the target users already have a guest account in the tenant directory. It is a good idea to create guest accounts when users need to

- share information with known external people over a sustained period. Guest users use their credentials to access content shared with them.
- **Only people in your organization.** Users cannot share files or folders with external people. Microsoft 365 Apps such as Microsoft Teams and Microsoft Lists use the same controls to control sharing links for content within and outside the tenant.

Shared with information in the sharing control. The sharing control used across Microsoft 365 [lists the set of people](#) whom a file, a folder, or a list item is already shared with so that document owners know how many people already have access to a file and who they are.

If you do not change the default sharing setting, users can create Anyone links. Changing the sharing setting for a tenant can be a slow process and can take several hours before a change is effective. The sharing settings also allow you to control the type of link created when a user shares a document with someone (choose from Specific people; Only people in your organization; Anyone with this link) as well as the [default permission](#) for the object type (files or folders). Because users usually accept the default link type, you should set the default permission to view-only. We can also restrict users so that they can only share files with authenticated external users who belong to specific domains. The sharing settings apply to every SharePoint Online site and OneDrive for Business account in a tenant.

You can also [customize sharing for a site including the](#) per-site Anyone Link expiration policy, but you cannot make sharing more permissive at a site level than it is for the tenant. [Per-site Anyone Link expiration](#) can be configured through the Sharing option in the SharePoint Admin Center or using the `Set-SPOSite` cmdlet to set the `AnonymousLinkExpirationInDays` parameter that overrides the tenant policy and set a more or less restrictive expiration policy for target sites. This parameter controls how all anonymous/anyone links that have been created (or will be created) will expire after the set number of days. It only applies if the parameter `OverrideTenantAnonymousLinkExpirationPolicy` is set to true. For example, the following command sets a 10-day Anyone link expiration period for the <https://Office365itpros.sharepoint.com/sites/Confidential> site:

```
Set-SPOSite -Identity https://Office365itpros.sharepoint.com/sites/Confidential  
-AnonymousLinkExpirationInDays 10 -OverrideTenantAnonymousLinkExpirationPolicy $True
```

Administrators can override the Anyone Link expiration period for OneDrive for Business sites by running the `Set-SPOSite` cmdlet and passing the desired expiration period in the `AnonymousLinkExpirationInDays` parameter.

To define which sharing type should be the default shown to users, run the `Set-SPOTenant` cmdlet. This example shows how to set the default to be a direct sharing link restricted to the people defined in the link

```
Set-SPOTenant -DefaultSharingLinkType Direct
```

The other permissible values are None, Internal, and AnonymousAccess. Do not use the last value as setting anonymous access to be the default sharing link type is a very bad idea.

Advanced Settings for External Sharing

Advanced settings for external sharing include:

- Create an allow list for external domains with which you are happy for users to share files. Conversely, you can create a block list to prohibit sharing with specified domains. You can have either a block or an allow list; you cannot have both. You can enter a maximum of 120 domain names separated by spaces.
- Restrict external sharing only to users who are members of a specific security group in the tenant.
- Control whether external users can share items they do not own (a bad idea, normally).
- Define the number of days after which access for guest users to a Site and OneDrive for Business expires.

- Establish how long a verification code sent to external users is valid before they must re-authenticate. The default value for this setting is 30 days.

Epiring Access Policy

The expiring access policy allows organizations to control how long (between 30 and 730 days) external users can access SharePoint Online and OneDrive documents. The mechanism works by placing an expiration date on the sharing links created for external users. When the expiration date approaches, site owners receive prompts in the SharePoint Online and OneDrive for Business browser GUIs and via email to manage expiration. They can either [extend access or let the access expire](#).

To enable the Expiry access policy for a tenant, access the sharing policy in the SharePoint Online admin center and edit the *Guest access to a site or OneDrive will expire automatically after this many days* setting. Alternatively, run the *Set-SPOTenant* cmdlet. For example:

```
Set-SPOTenant -ExternalUserExpireInDays 60 -ExternalUserExpirationRequired $True
```

Administrators can override the tenant guest expiration setting for individual sites by running the *Set-SPOSite* cmdlet. For example:

```
Set-SPOSite -Identity "https://office365itpros.sharepoint.com/sites/CriticalSite1" -OverrideTenantExternalUserExpirationPolicy $True -ExternalUserExpirationInDays 730
```

It's important to underline that this setting applies only to sharing links, direct permission changes, and SharePoint group membership and does not apply to guest access to SharePoint Online sites granted through the membership of Microsoft 365 Groups. Guests who are members of Microsoft 365 Groups can continue to access the content of the group-connected sites for as long as they are members of those groups. Setting an expiring access policy for a tenant or site applies only to sharing granted after the policy becomes effective and only for the sharing links created for guest accounts.

Other Settings for External Sharing

Other configurable settings are available in the Sharing section of the admin center:

- Enable (default option) or disable the setting to display the names of people who viewed their files.
- Provide site owners with the ability to display the names of the people who viewed files or pages in SharePoint.
- Shorten links or change their default permission.

Per-Site Sharing controls

Administrators can configure Sharing settings at the site level. Select a site from the Active sites list, select an existing site, and click **Sharing**. In the Sharing settings panel, you can then select the following configurations:

- Change the current **External sharing** setting to another value such as Anyone or Existing guests only. The choice of permitted values depends on the global sharing setting at the tenant level. The external sharing capability for a site can also be set by assigning a sensitivity label with container management to the site. See the Information Protection chapter for more information.
- Create a list of **external domains** with which site members are allowed to share site content.
- Configure a guest access expiration policy for the site.
- Set the **default sharing link type**. Note that to choose the *Anyone with the link* setting, the site must first be configured to allow anonymous sharing. This link type also allows users to override the default *link expiration*.
- Override the **default link permission** (view or edit) for sharing links.

It's possible to disable company-wide sharing links for individual sites. This is a good idea for sites that hold confidential information because it forces users to define exactly who should receive access to content. To disable company-wide sharing links, run this PowerShell command:

```
$Site = "https://office365itpros.sharepoint.com/sites/ProjectX"  
Set-SPOSite -Identity $Site -DisableCompanyWideSharingLinks Disabled
```

If external sharing is disabled on a site, an administrator can configure a custom sharing help link to explain why external sharing is disabled or how to request a policy change. This feature can be enabled by running the following PowerShell command:

```
Set-SPOTenant -CustomizedExternalSharingServiceUrl <url-address>
```

Per-Site Sharing Links default to people with existing access. A SharePoint Admin can also set the default sharing link for a site to "People with existing access" by running the *Set-SPOSite cmdlet* with the *-DefaultLinkToExistingAccess* parameter. Once the setting is applied, any user sharing a file or a folder from the site will get an existing access link that does not change permissions on the file or folder being shared.

Sharing Content with View-Only Permissions

When you create a sharing link with view-only permissions, individuals who receive the link can copy the link from the Share dialog when they wish to share the link with others. If the sharing option is set to Only people with existing access, the user can send a request through the sharing control to the file owner to ask them to share the content with specific individuals. The file owner can choose to approve or deny the request.

Link Settings to Control Access to Documents

Sharing links created by SharePoint Online and OneDrive for Business can [block recipients from downloading copies](#) when an Office document is shared anonymously, to all users in the organization, or specific people. To block downloads, a user edits the sharing link settings and toggles the "Block download" setting (Figure 7-1). When a sharing link blocks downloads, recipients can use Office Online to view the content.

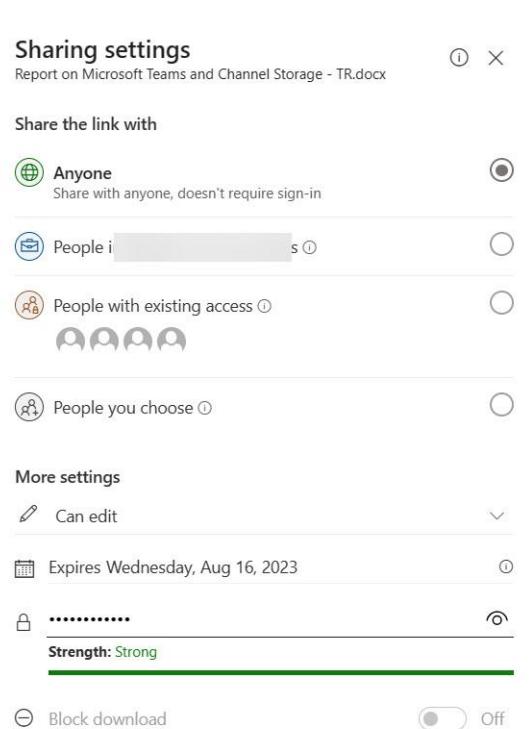


Figure 7-1: Editing a sharing link to block downloads and requiring a password to open the document

As the name implies, an Anyone link allows anyone with the link to open the associated content. When an Anyone link includes a password, people must enter the password before they can access the content. SharePoint Online and OneDrive for Business do not distribute the password: the person who creates the Anyone link must transmit the password to authorized recipients separately (it is a bad idea to include the password as a comment sent in the link). The presence of the password means that the content is safe if the link is forwarded or reshared with others (unless the password is also shared). The ability to block the download of other file types (images, 3D, PDF, and more) is also supported and it's [the default setting for some audio and video files](#). You can also set an expiration date for the sharing link as an additional protection mechanism. This expiration date can be configured for [Anyone, Company-wide and People you choose links](#).

If your organization uses sensitivity labels, the sharing link dialog displays the label assigned to a file as a visual reminder to users that they should be careful when sharing confidential information.

Open in review mode in Word Online. Users can choose to share Word documents with the "Can review" option. When enabled, recipients can only open the Word file in the online app with the "Reviewing" mode enabled. While in Reviewing mode, users can suggest changes (using the track changes feature) and make comments, but they cannot make edits. Owners of the document have the option to accept or reject the suggestions made by the recipient.

Sharing with External People

When a user shares a document or folder with an external person using a company link, the [sharing dialog](#) automatically prompts to confirm the action. If confirmed, SharePoint updates the sharing link from an internal-only link to a Specific people link. Otherwise, SharePoint signals an error message: "This link won't work for people outside of your organization."

To share content in a Microsoft 365 application, a user can use two methods:

- Invite: Grants direct access to the file or folder for the people chosen by the sharer. Each sharing recipient receives an invitation e-mail to allow them access to the shared file or folder.
- Copy link: Generates a sharing link for the file or document with the sharing settings defined by the user.

Sharing with Microsoft 365 Groups or Teams

Every group has a SharePoint site with a document library. This applies whether the group supports conversations through Outlook, Viva Engage, or Teams. SharePoint sets the sharing capability for the sites belonging to new groups to *ExternalUserSharingOnly*, which is a level of access enough to allow guest accounts to work with content in the document libraries.

During the creation of a new group or team, SharePoint Online provisions a site to hold the document library and other resources. The tenant sharing settings control what sharing group users can do for files in the document library, but a group owner or tenant administrator can make the sharing more restrictive by changing the *SharingCapability* setting for the group's site. The values that you can set are equivalent to the four settings available for the SharePoint tenant as explained above.

The tenant sharing setting prevails over the setting for a site. If you want to use a setting like *ExternalUserAndGuestSharing* for the site belonging to a group, you must first make sure that the organization allows anonymous sharing.

To check the sharing capability for a group, run the command (A connection to both SharePoint Online and Exchange Online is required):

```
$sGroupName="Office365forITPros"
```

```
Get-SPOSite -Identity (Get-UnifiedGroup -Identity $sGroupName).SharePointSiteUrl | Select SharingCapability
```

SharingCapability	: ExistingExternalUserSharingOnly
--------------------------	-----------------------------------

In this instance, the sharing capability for the site matches that of the tenant and is appropriate to support guest access to the site's document library through Groups or Teams.

Other sites might implement a different sharing model to that used by Groups. If you want to align the two sharing models, you can restrict sharing to external users who already have guest accounts in your tenant directory. When this happens, administrators must create guest accounts in the directory before users can invite the holders of those accounts to access their documents. You should also allow SharePoint users to search for guest accounts in the people picker used to select with whom to share a document. By default, guests do not show up in the people picker, so to enable them to appear, you need to run the *following cmdlet*:

```
Set-SPOTenant -ShowPeoplePickerSuggestionsForGuestUsers $True
```

Not all team sites are group-enabled. Some are still of the classic variety to serve specific purposes. To list all the team-enabled sites in a tenant, use this cmdlet, which includes the template for group-enabled sites to isolate the set we want to see:

```
Get-SPOSite -Template "GROUP#0" -IncludePersonalSite:$False
```

Taking this a little further, this code processes the set of group-enabled team sites and reports information about the sharing activity for each site.

```
$SiteNumber = 0
ForEach ($Site in Get-SPOSite -Template GROUP#0 -IncludePersonalSite:$False)
{
    $SiteNumber++
    Write-Host "Site number: " $SiteNumber " " $Site.Url
    Write-Host "Owned by: " $Site.Owner
    Write-Host "Sharing: " $Site.SharingCapability
    Write-Host "-----"
    Get-SPOExternalUser -SiteUrl $Site.Url
}
```

Tracking Document Sharing Through Audit Records: Each time someone shares a document or folder, SharePoint records the event in an audit record. You can search the audit log to retrieve and analyze these records to understand what sharing occurs within a tenant. See the Reporting and Auditing chapter for details.

Move Files and Keep Sharing

When users move files from a SharePoint site to another site, from a SharePoint site to OneDrive, or from OneDrive to a SharePoint site, they have the option to retain the sharing of the file with the same people at the new destination. When this option is used, those with access to the file receive an email to tell them that the file has been moved and that they have a new link or direct permissions to match those at the source location.

Sharing with LinkedIn Contacts

If a tenant is configured to connect to LinkedIn, Microsoft 365 users can connect their accounts to their LinkedIn accounts (see the Managing Users chapter for details). When an account is connected to LinkedIn, first-degree contacts are downloaded from LinkedIn and included in the “suggested people” list used by

browser interfaces such as SharePoint Online and OneDrive for Business clients. The suggested people list also includes tenant users (including guest accounts) and email addresses from Outlook's auto-complete list.

When the user next shares a document from SharePoint Online, OneDrive for Business, or the online Office apps, the name they enter is checked against the suggested people list. If a match is found against a LinkedIn contact and the user goes ahead and shares the document, the sharing invitation is sent to the contact's email address.

At a Glance Summaries in Sharing Emails for Word Documents

When a user shares a Word document, the notification to inform the recipient about their access to the document includes a list of key points in the text and the time estimated to read the content. Files identified as sensitive by Data Loss Prevention policies will not include this information.

Administrators can disable the feature for the tenant by running the *Set-SPOTenant* cmdlet:

```
Set-SPOSite -IncludeAtAGlanceInShareEmails $False
```

Generate a Summary with Microsoft 365 Copilot When Sharing

Users can include a document summary of a Word document generated by Microsoft 365 Copilot when sharing with other users. The document summary adds more context for the document and is included in the notification e-mail sent to the sharing recipient. This feature requires users to have a Microsoft 365 Copilot license and works only with Word documents.

Request Files

The [Request files feature](#) allows users to create a special sharing link to ask external people to upload files to a specific folder in a document library or OneDrive for Business. Any site member/OneDrive user can use the request files feature. It cannot be restricted to site owners. When a user selects a SharePoint Online or OneDrive for Business folder and clicks "Request files," it results in a file request link. Anyone can use this link to upload files to the target folder, but they cannot view, edit, or see who else may have uploaded files using the link. When someone uses the Request files link, SharePoint redirects them to a special page where they can select the files to upload together with some personal details (First and Last Name) to let the requestor know who uploaded files to the folder. When SharePoint uploads the file to the target document library, it prefixes the file name with the first and last name of the person who uploads a file.

Administrators can control the Request files feature for the tenant or a specific site using the *Set-SPOTenant* and *Set-SPOSite* cmdlets. In this example, the first command enables the Request Files feature for the tenant and sets an expiration period of 7 days for the links used to upload files; the second disables the feature for a specific site:

```
Set-SPOTenant -CoreRequestFilesLinkEnabled $True -CoreRequestFilesLinkExpirationInDays 7  
Set-SPOSite -Identity $SiteURL -RequestFilesLinkEnabled $False
```

To check the site settings, run:

```
Get-SPOSite -Identity $SiteURL -Detailed | Select-Object Request*  
  
RequestFilesLinkEnabled RequestFilesLinkExpirationInDays  
-----  
False 7
```

As you can see, the site configuration supports a link expiration setting. By default, the site inherits the value for the setting from the tenant configuration, but you can define a more restrictive expiration period if you like. You can't override the tenant configuration and define a less restrictive expiration period for a site. The

link expiration period can be anything from 0 (zero) to 730 days (two years). Usually, the more secure the site, the lower the link expiration period.

OneDrive for Business also supports the Request Files feature. The *OneDriveRequestFilesLinkEnabled* setting in the tenant configuration controls if the feature is available in OneDrive for Business accounts while the *OneDriveRequestFilesLinkExpirationInDays* sets the expiration period for the sharing links. You can't prohibit Request Files for selected OneDrive for Business accounts. The feature is either enabled or disabled for all.

```
Set-SPOTenant -OneDriveRequestFilesLinkEnabled $True -OneDriveRequestFilesLinkExpirationInDays 7
```

Sharing from Microsoft Lists

[Microsoft Lists supports sharing](#) in two ways:

- By granting access to the entire list with specific permission (Full control, Edit, View) to specific users, mail enabled security groups, Microsoft 365 Groups, or security groups. In practice, granting access in this way implies the creation of unique permissions for the list.
- Through the sharing link that is generated when a specific list item is shared through the universal sharing dialog.

Sharing SharePoint Pages and News

Individual SharePoint pages and news can be shared by users without having to share the entire site. When a SharePoint page or news is shared, the pages and items on the page like images are shared. Other content linked in the page like embedded links or documents is not shared unless the items were individually shared before being added to the page.

Managing Sharing and Access Request Settings

Site admins and site owners can manage **Sharing and access request settings** directly from the site permissions panel (through the **Change how members can share** link). From this panel a site administrator or owner can:

- Modify sharing permissions by choosing one of the following options: "Site owners and members can share files, folders, and the site", "Site members can share files and folders, but only site owners can share the site" and "Only site owners can share files, folders and the site."
- Allow or deny access requests to the site. This setting, enabled by default, also includes the choice to direct site access requests to site owners or to send the requests to a specific e-mail address. A custom message for the access request page can be added.

Managing Access to Files and Folders in SharePoint Online

The **Manage access** popup makes it easy to manage access permissions, remove individual recipients from shared links, and stop sharing overall. This popup, available for both SharePoint Online and OneDrive for Business, shows up when the user clicks the **Manage access** link under the **Has access** link in the files/folder details pane. From here, the user can easily grant access to the selected file/folder, stop sharing, or manage existing sharing permissions. Existing sharing permissions in the file/folder are displayed in three tabs:

- People: Shows individual users and their permissions for the file/folder.
- Groups: Displays the list of SharePoint Groups, Microsoft 365 Groups, and Security Groups (and their permissions) with access to the file/folder.
- Links: Shows the sharing links created to share the file/folder. For a given sharing link, it's possible to update the settings of the link or remove it.

The popup also shows up when the user selects a file and then clicks on the **Manage access** option present as a command in any Document library and OneDrive for Business.

Sharing Reports for SharePoint Online and OneDrive for Business

Site owners can generate a CSV file to report site content shared with any user. The option is available on the Site usage page. To create a Sharing report, a site owner browses the site usage page and clicks the **Run report link** in the **Shared with external users** section. When prompted, the user selects a folder to save the CSV report and then clicks **Save**. Once the report is generated, SharePoint sends a notification to say the CSV file is available in the chosen location. The report contains a row for every file or folder shared by the user with [the following information](#): File/Folder path, item type (Web, Folder, Document), permission level applied to the item (Total Control, Collaborate, Read), user name, user e-mail, the user or group type (Internal, External, SharePoint Group, Security Group or Microsoft 365 Group), link identifier, link type (Anyone, People in the organization with the link, People with existing access or Specific people) and the link ID used to access the item.

A similar sharing report feature is available for OneDrive for Business, the difference being that instead of focusing on the sharing activities for everyone on a site basis, the OneDrive variant only looks at sharing of a specific user's personal files. The **Run sharing report** link used to generate a sharing report is available on the modern OneDrive settings page. An example of how to use the Microsoft Graph to report sharing within OneDrive is [posted here](#).

Tracking Shared Files

The *Set-SPOTenant* cmdlet also controls a setting often used by administrators to keep track of files shared with external users. The example shown below sets the *BccExternalSharingInvitations* setting to *\$True* to force SharePoint Online to generate a BCC message to a nominated list of email addresses (in a comma-separated list with no spaces) each time a user shares a file stored in a SharePoint Online or OneDrive for Business document library with an external person. The users specified in the *BccExternalSharingInvitationsList* parameter will receive a message saying that the user wishes to share a file with the addressee of the message.

```
Set-SPOTenant -BccExternalSharingInvitations $True -BccExternalSharingInvitationsList  
administrator@Office365ITPros.com
```

OneDrive for Business Notifications: SharePoint Online controls many settings for OneDrive for Business, among which are notifications for events connected with sharing files. The Sharing settings available in the SharePoint admin center allow you to opt for users to receive notifications via email when:

- Users invite external users to access shared files.
- External users accept invitations and open shared files.
- Users create or update an anonymous link used to share files.

SharePoint Online Extensibility Options

Traditionally, one of the strongest characteristics of SharePoint has been its natural extensibility: an organization can change the system to meet business requirements in several ways. Unfortunately, the introduction of SharePoint Online initially featured a strong reduction of the extensibility options when compared to SharePoint on-premises. This was due to the intrinsic multitenant design of the platform and because Microsoft wanted to reduce the fragility of custom development.

SharePoint Online inherited the Add-ins model from SharePoint Server as a customization mechanism. This model supports the creation of integrated applications in the platform while running totally outside the main

structure. Furthermore, it is not possible to install and run server-side code in SharePoint Online, something that removes the possibility of creating traditional SharePoint artifacts such as classic Web Parts, Timer Jobs, Event Handlers, etc. As the SharePoint Online platform matures and evolves, substitutes for older integration mechanisms have been added to SharePoint Online through the natural integration with other platforms (Azure, Power Apps, Power Automate), the work done by the SharePoint Team with SPFx, and SharePoint community initiatives such as the PnP project.

SharePoint Add-In and Azure ACS retirement: Microsoft is retiring the [SharePoint Add-In extensibility model](#) and the [use of Azure ACS for SharePoint Online authorization](#). The retirement plan is as follows:

- New tenants cannot use the SharePoint Add-In and Azure ACS from November 1, 2024.
- Existing tenants will lose access from April 1, 2026.

Tenants can use the [Microsoft 365 Assessment Tool](#) to audit the usage of SharePoint Add-Ins and Azure ACS by scanning for apps that use these technologies. The recommendation is to migrate Add-Ins and Azure ACS to modern cloud solutions built with the SharePoint Framework (SPFx), Microsoft Azure artifacts (Web Apps, Azure Logic Apps, Azure Functions, and others) using Entra ID as the authorization mechanism.

SharePoint Apps and the Global App Catalog

SharePoint Apps are self-contained pieces of functionality that extend the capabilities of SharePoint to solve business problems. Apps don't have custom code that runs within SharePoint Online: all custom logic moves to servers outside the SharePoint platform. Keeping custom code out of SharePoint guarantees that the App can't harm SharePoint or reduce the performance of the system.

The Global App Catalog makes internal custom Apps available for users to install when they search for apps using the "From my organization" filter on the My apps page. Site owners can add these apps to customize sites with specific functionality or to display information. After a Global App Catalogue has been created, it is possible to upload any custom App that the organization has developed by uploading the App package and setting some properties in the Manage apps section. The global App Catalogue also supports the management of App requests from users, checking how Apps are used, and the maintenance of license information.

Site App Catalogs are configured and managed using PowerShell. Before management of Site App Catalogs is possible, the Global App Site must exist. Use the *Add-SPOSiteCollectionAppCatalog* cmdlet to create a Site App Catalog, indicating the site where the app catalog should be created with the *-Site* parameter. An "Apps for SharePoint" document library will be added to the site to deploy SharePoint Apps including SPFx solutions. To disable the Catalog, use the *Remove-SPOSiteCollectionAppCatalog* cmdlet indicating the site in the *-Site* parameter; this prevents new components from being added and any previously installed components from executing their code. It is not possible to enumerate with PowerShell all the site collections in the tenant that have the Site App Catalog enabled, but it's possible to see those Site App Catalogs through the "Site App Catalogs" list in the Global App Catalogue. This is a hidden list that stores a record for every Site App Catalog created in the tenant. In addition, be aware that although solutions installed in Site App Catalogs can only be used in these specific sites, they can theoretically use resources from other sites in the tenant.

SharePoint Framework (SPFx)

SPFx is a Page and Web Part development model for client-side development and integration with the Microsoft Graph. It is based on open source tooling and JavaScript technologies. SPFx is used in SharePoint as the extensibility paradigm for the client-side development framework to allow developers to implement new functionality in SharePoint.

SPFx is used extensively by Microsoft to build the modern user experiences seen in SharePoint Online, but external developers can use the same technology, tools, and techniques to build more productive experiences and apps that are responsive and mobile-ready.

From the infrastructure point of view, the files required for SPFx are just JavaScript archives plus the accompanying style sheets, graphics, and other required files that should be deployed to [an accessible place for the client computers](#). This can be implemented using the SharePoint Content Delivery Network (CDN), a SharePoint document library, the Azure CDN, or any other available private or public CDN. Additionally, a manifest file must be deployed to the SharePoint Catalog, so that SharePoint is aware of the existence of the components. Normally a distribution package is created by the developers and delivered to the administrators that install them in the SharePoint Catalog, in a similar way as for SharePoint Add-ins.

Microsoft 365 Patterns and Practices (PnP)

The [Microsoft 365 Patterns and Practices community](#) initiative comprises components aimed at enhancing the functionality of SharePoint on-premises and Online in several ways, filling the development and infrastructure gaps left by Microsoft. The components include:

- [**PnP Framework**](#), a .NET standard 2.0/.NET 6.0/.NET 7.0 library targeting Microsoft 365 containing useful extensions to extend SharePoint and Microsoft 365 APIs.
- [**PnP Transformation Framework**](#), a generic solution designed to transform any web-based/content-based solution into a modern SharePoint Online Portal.
- [**PnP PowerShell cmdlets**](#).
- [**PnP Scripts Samples**](#), a website with several samples demonstrating how to use PowerShell in different use cases about getting information and managing SharePoint Online and other Microsoft 365 workloads.
- [**PnP Core SDK**](#), a unified object model to work with SharePoint Online and Teams that is agnostic to the underlying APIs. Over time, the developers plan to extend the SDK to support other Microsoft 365 workloads.
- A complete [**PnP Provisioning Engine**](#) is included in the PnP Framework.
- [**PnPJS**](#), a JavaScript library to help consume SharePoint and Microsoft 365 APIs securely.
- PnP tools, such as the PnP SPFx Yeoman Generator, the CLI for Microsoft 365, or the Microsoft Graph PowerShell SDK among others.
- **Ready to use solutions** such as the [**PnP Starter Kit**](#).
- **The SharePoint look book**, a [**free service**](#) to deploy customized sites in a SharePoint tenant based on a selected site template. The service includes several ready-to-use templates. Each template consists of a customized home page, lists, document libraries, and custom Web Parts.

Using PnP reduces the development effort needed to work with SharePoint. For example, to create a new list or document library you only need to connect to SharePoint Online for a tenant and use *New-PnPList* as follows:

```
Connect-PnPOnline -Url "https://tenantname.sharepoint.com/sites/namesitecollection" -  
SPOMgmtShell  
New-PnPList -Title "PnPList" -Template GenericList -Url "Lists/PnPList"
```

The *Connect-PnPOnline* cmdlet needs valid user credentials to make the initial connection to the tenant. Then a new list called "PnPList" is created using the *New-PnPList* cmdlet and the *Template* parameter to specify the list template to use. Be aware that the connection is only valid for the given URL endpoint; if you want to use another site, you need to make a new connection.

Provisioning is probably the most used and most powerful PnP feature. The recommended way to provision in SharePoint Online is to create a new "standard" object in SharePoint, and then apply all the customizations

using scripting (thus not creating new templates as traditionally used). The PnP provisioning engine is powerful enough to create and modify almost any element in a site: the creation of Lists, Libraries, Custom Fields, Content Types, views, attach users, etc. There are several cmdlets and ways to provision them using PnP:

- Make a template (just an XML file) that contains all the elements to be created, deleted, or modified, and run the *Invoke-PnPSiteTemplate* cmdlet pointing to the XML file and URL endpoint. The creation of fully customized SharePoint objects using this way is possible (and recommended).
- Manually create all the customization required in a dummy site and generate the XML template using the *Get-PnPSiteTemplate* cmdlet. Then, the template can be used to provision as many clones as necessary using *Invoke-PnPSiteTemplate*.
- PnP Provisioning Engine and XML templates can be used in .NET code, so the same process described to get and apply a provisioning template with PowerShell can be done programmatically.
- There are also specific PnP cmdlets to manage some provisioning objects. For example, to create a new view for the early created List, use:

```
Connect-PnPOnline -Url "https://tenantname.sharepoint.com/sites/namesitecollection"
$myList = Get-PnPList -Identity "Lists/PnPList"
Add-PnPView -List $myList -Title "myView" -SetAsDefault -Fields ID,Title,Created
```

Site Scripts and Site Templates

Site scripts and site templates are [extensibility mechanisms for SharePoint Online](#) to allow administrators to create, deploy, and apply templates to a site. Site scripts and site templates can be applied during site creation, as part of a hub association, or to existing sites. End users with the required permissions can also apply [scenario-based templates](#) or organization templates to existing SharePoint sites by using the *Apply a site template* option in the site settings menu. This option is also based on the site scripts and templates extensibility model.

The following site types support site scripts and site templates:

- Modern Team Sites linked to a Microsoft 365 Group (GROUP#0).
- Modern Team Sites not linked to a Microsoft 365 Group (STS#3).
- Communication sites (SITEPAGEPUBLISHING#0).
- Channel site templates (TEAMCHANNEL#0, TEAMCHANNEL#1). The latter template is now generally used for sites belonging to both private and shared channels.

Site templates and Hub Sites: Site templates can be [applied to Hub Sites to apply to the associated sites too](#). This option is an optional setting for a given hub site and requires the site template and site script to already be available in the tenant.

Site templates are always based on an out-of-the-box template, and can be deployed through PowerShell as follows:

```
Add-SPOSiteDesign -Title "HR Site" -WebTemplate "64" -SiteScripts "<ID>" -Description "HR Department Site"
```

Site templates always reference one or more site scripts (by their identifiers) to apply the customizations defined by the script. *WebTemplate 64* is the identifier for the Modern Team sites while 68 is for Communication sites and 69 for Teams channel sites. It's important to note that there is a limit of 100 site scripts and 100 site templates per tenant.

A site script is a JSON file defining the customizations to be added to a new site (where the site template is the actual template to define the site). Site scripts are uploaded to a gallery at the tenant level, making them

available for all sites. Site scripts are deployed using the `Add-SPOSiteScript` cmdlet, which returns the ID to be used by `Add-SPOSiteDesign`:

```
Add-SPOSiteScript -Title "Create HR lists" -Content $mySiteScript -Description "Creates lists for HR site"
```

In the above example, the `$mySiteScript` variable contains the JSON string with the actions to implement.

Site template JSON Schema: The [JSON schema](#) defines all the actions and sub-actions that can be included in a site template. To simplify the creation of a Site template, there is a [free online tool](#) to visually define the JSON structure for a specific Site Design.

Using PowerShell to Apply Site Templates

A site template can be applied to an existing site by using the Apply a site template option in the settings menu for a site or by running the `Invoke-SPOSiteDesign` or `Add-SPOSiteDesignTask` cmdlets. The first option allows the site administrator to view all the site templates available and apply them to the site while updating site templates with PowerShell is a good way to automate updates across a set of sites. The two cmdlets take a different approach in how they implement site templates:

- `Invoke-SPOSiteDesign` applies the site template to the site immediately.
- `Add-SPOSiteDesignTask` adds the site template application to a schedule to be run as a background job. In addition, this cmdlet extends the 30-action limit in a site script that is applied synchronously to 300 actions (or 100,000 characters). More information about the limits applying to site scripts and site templates [can be found in Microsoft's documentation](#).

Site scripts can also be generated from existing sites, lists, and document libraries, which means that existing site settings, lists, and document libraries can be easily ported to another site. The `Get-SPOSiteScriptFromList` cmdlet can be used to autogenerate a site script from a list. Alternatively, the `Get-SPOSiteScriptFromWeb` cmdlet can autogenerate a site script that includes the following site settings: branding, theme, regional settings, sharing capability, and the lists and document libraries specified in the `IncludedLists` parameter:

```
$sSPOSiteUrl="https://office365itpros.sharepoint.com/sites/0365ExchPro"
Get-SPOSiteScriptFromWeb -WebUrl $sSPOSiteUrl -IncludeBranding -IncludeTheme
-IncludeRegionalSettings -IncludeSiteExternalSharingCapability
-IncludedLists("Lists/TemplateName1","Lists/TemplateName2")
```

Discover which site templates are applied to a site: The `Get-SPOSiteDesignRun` cmdlet shows all the site templates that have been applied to an existing site. The `Get-SPOSiteDesignRunStatus` cmdlet returns the result of each action from every site script in a site design. Site owners can also [view templates](#) through the View template history link available in the Site Information panel.

Configuring Site Regional Settings with Site Templates

Site scripts can set default regional settings for new sites. This is important if you want to ensure that sites display the correct document creation and modification times in local format when accessed through a browser. By default, SharePoint Online sets the default time zone to Pacific Daylight Time (UTC -8), which is fine for people in Redmond but not so good for users elsewhere in the world. You can always update these settings by accessing the Regional Settings of a site. However, given that Teams and Groups create many of the new SharePoint Online sites and their owners are usually people with little knowledge of SharePoint internals, it is best if the settings are correct from the start.

An example of [how to configure regional settings](#) is available on GitHub. The steps are straightforward. First, create a JSON-formatted input file holding the settings that you want to use. In this example, I select GMT as the default time zone, that we use the 24-hour format instead of the 12-hour format, and Ireland is the

default country (locale id or LCID). Examples of other locale ids are 3082 (Spain), 5129 (New Zealand), and 1035 (Finland). A [full list of locale ids](#) is available online.

```
{
"$schema": "schema.json",
"actions": [
    {
        "verb": "setRegionalSettings",
        "timeZone": 2, /* Greenwich Mean Time */
        "locale": 6153, /* Ireland */
        "sortOrder": 25, /* Default */
        "hourFormat": "24"
    }
],
"bindata": { },
"version": 1
}
```

Save the JSON data to a file. Then connect to SharePoint Online with PowerShell and execute the following command to retrieve the settings from the file and load them into a variable (`$SiteScript`).

```
$SiteScript = (Get-Content "C:\Temp\RegionalSettings.json" -Raw | Add-SPOSiteScript -Title "Set Ireland Regional Values" -Description "Sets locale, time zone, and hour setting for Ireland")
```

Now run the `Add-SPOSiteDesign` cmdlet to load the settings as default regional values.

```
Add-SPOSiteDesign -Title "Set Ireland Regional Values" -WebTemplate "64" -SiteScripts $SiteScript -Description "Applies Ireland regional settings" -IsDefault
```

To test that the change is effective, create a new team or group and examine the regional settings for the site that SharePoint Online provisions. Open the site with SharePoint, select Site Contents, then Site Settings, and then Regional settings. The locale and time zone settings should be the values set in the script. Alternatively, you can apply the site template to an existing site through the Site templates dialog available in the settings menu, just select the desired site template and click on the “Apply to site” button.

If you make a mistake, you can update the site design with the `Set-SPOSiteDesign` cmdlet or remove the site template and start over. Run the `Get-SPOSiteDesign` cmdlet to return a list of site templates in the tenant and note the identifier (Id) for the design you want to remove. Then run the `Remove-SPOSiteDesign` cmdlet to remove it.

Get-SPOSiteDesign

```
Id : f466a1da-e2a2-4107-b558-35954ad199de
Title : Default
WebTemplate : 64
SiteScriptIds : {9e287dd9-b2b1-4ceb-8649-998f43b24c1d}
Description : Applies Ireland regional settings
PreviewImageUrl :
PreviewImageAltText :
IsDefault : True
Version : 1
```

```
Remove-SPOSiteDesign -Identity f466a1da-e2a2-4107-b558-35954ad199de
```

Setting default regional settings for new sites with a site script does not update regional settings for existing sites. If you want those sites to use the correct time zone and locale, you can either update the settings manually or use a script. Here’s an example that looks for Microsoft 365 Groups that are provisioned for SharePoint and then applies a site template (identified with a GUID) to each site.

```
$SitesUpdated = 0
$DesignID = "f466a1da-e2a2-4107-b558-35954ad199de"
```

```
$Groups = (Get-UnifiedGroup | Where-Object {$_.SharePointSiteUrl -ne $Null} | Select-Object SharePointSiteUrl, DisplayName, Alias)
ForEach ($G in $Groups) {
    Try {
        Write-Host "Processing" $G.SharePointSiteUrl "for group" $G.DisplayName
        Invoke-SPOSiteDesign -Identity $DesignID -WebUrl $G.SharePointSiteURL -ErrorAction Stop
        $SitesUpdated++
        Set-UnifiedGroup -Identity $G.Alias -CustomAttribute13 "Site Design Updated"
    }
    Catch {
        Write-Host "Problem Processing" $G.SharePointSiteURL
    }
}
Write-Host $SitesUpdated "sites updated successfully. You need to check the following and update them manually"
Get-UnifiedGroup -Filter {CustomAttribute13 -eq $Null} | Sort-Object DisplayName | Format-Table DisplayName, SharePointSiteURL
```

The list of groups generated at the end of the script includes all groups that we cannot update. In some cases, this is because SharePoint is not fully provisioned for the group (a more common problem for older groups) and no one has ever tried to access the document library. If the site does not exist, we cannot update its regional settings. In other instances, the account used to run the script might not have the necessary permissions to update site settings. Administrators can update these sites manually as time allows.

Managing Built-In Site Templates

SharePoint administrators can control the set of built-in site templates that are available to site creators. To retrieve the current state of specific built-in site templates, run the [Get-SPOBuiltInSiteTemplateSettings](#) cmdlet. Then, to show or hide a template, run the [Set-SPOBuiltInSiteTemplateSettings](#) cmdlet. For example, to hide the “Event planning” site template, run the following command:

```
Set-SPOBuiltInSiteTemplateSettings -Identity '9522236e-6802-4972-a10d-e98dc74b3344' -isHidden $true
```

Additional Features and Settings in SharePoint Online

Apart from the day-to-day business of site and service management, several operations exist that administrators perform on an on-demand basis.

Enabling or Disabling Web Parts

SharePoint pages can be customized with web parts to show information from other Microsoft 365 services and non-Microsoft services such as Kindle or YouTube. SharePoint Administrators [can use PowerShell to hide specific web parts from end users](#) by running the *Set-SPOTenant* cmdlet to set the *DisableWebPartIds* property. For example, to hide the Web Part for Kindle, you run this command:

```
Set-SPOTenant -DisableWebPartIds 46698648-fcd5-41fc-9526-c7f7b2ace919
```

GUIDs for multiple web parts can be specified in a comma-separated list. To view a list of disabled web parts, run the *Get-SPOTenant* cmdlet. To reenable disabled web parts, run *Set-SPOTenant* and specify only the GUIDs for the web parts that you want to disable in *DisabledWebPartIds*. To enable all web parts, run:

```
Set-SPOTenant -DisabledWebPartIds @()
```

Disable Creation of New SharePoint 2013 Workflows

Although Microsoft [has deprecated](#) SharePoint 2013 classic workflows in SharePoint Online, it’s still possible to create new SharePoint 2013 classic workflows in a tenant. To disable the creation of new workflows, a SharePoint Admin can use the *StopNew2013Workflows* parameter in the *Set-SPOTenant* cmdlet:

```
Set-SPOTenant -StopNew2013Workflows $True
```

Existing SharePoint 2013 workflows won't be affected when this setting is true and will continue running. If necessary, the workflows can be modified. Microsoft strongly recommends that organizations move 2013 workflows to Power Automate. To help, an open-source [SharePoint 2013 Workflow assessment tool](#) is available. The tool provides usage data of SharePoint 2013 classic workflows and generates a Power BI report to help plan the migration to Power Automate.

SharePoint 2013 workflow retirement: SharePoint 2013 workflows deprecation is happening in two stages:

- First, SharePoint 2013 workflows are turned off for any new tenant created after April 2nd, 2024.
- Second, the ability to run, create, or execute SharePoint 2013 workflows will be disabled for existing tenants. This is expected to happen on April 2nd 2026.

Site Swap

Site Swap allows SharePoint Admins to replace the location of a SharePoint root site with another site using *Invoke-SPOSiteSwap*. For example, this [PowerShell command performs a Site swap](#):

```
Invoke-SPOSiteSwap -SourceURL https://office365itpros.sharepoint.com/sites/NewMarketingComms -  
TargetURL https://office365itpros.sharepoint.com -ArchiveURL  
https://office365itpros.sharepoint.com/sites/0ldMarketingComms
```

Invoke-SPOSiteSwap requires the [following attributes](#) to be configured:

- *SourceURL* parameter indicates the site that is going to replace the root site.
- *TargetURL* parameter indicates the root site to be swapped.
- *ArchiveURL* parameter indicates the new URL for the former root site.

After running the cmdlet, a background job performs the site replacement and after some minutes and some occasional 404 errors, the new root site will be available. Some restrictions exist for consideration before making a Site swap. The most important of these is that source or target sites can't be associated with a modern Team Site or a Hub Site.

Tenant Rename

Tenant rename allows organizations with less than 10,000 sites (including OneDrive and SharePoint sites) to [change the SharePoint domain name](#) using the following steps:

- Add and verify the new domain name in the custom domain names blades in the Entra admin center.
- Initiate the SharePoint tenant rename using the *Start-SPOTenantRename* cmdlet with the attributes *DomainName* and *ScheduledDateTime* configured with the target domain name and the date and time to start the rename process. For example, this command instructs SharePoint Online to begin the domain rename process on October 31, 2023, at 10:25 UTC.

```
Start-SPOTenantRename -DomainName "NewDomainName" -ScheduledDateTime "2023-10-31T10:25:00"
```

- Give the tenant rename process some time (it can take several hours or even days depending on the number of SharePoint sites and OneDrive accounts to process) before starting to review if everything works as expected under the new domain.

To check the status of the rename operation, use the *Get-SPOTenantRenameStatus* cmdlet. Similarly, the *Get-SPOSiteRenameState* cmdlet checks the state of a specific site.

[Advanced tenant rename](#) is available to organizations with between 10,000 and 100,000 sites and requires the tenant to have SharePoint Advanced Management licenses. Advanced rename does not work for multi-geo tenants.

Microsoft Defender for Office 365

[Microsoft Defender for Office 365](#) can be enabled on E5 tenants or E3 tenants to run check files in document libraries to make sure that they're not infected with malware. Microsoft Defender for Office 365 P1 is also available in Microsoft 365 Business Plans.

Microsoft Defender for Office 365 works across all SharePoint Online and OneDrive for Business sites in a tenant. It uses a mixture of technologies, including advanced threat heuristics generated from intelligence gathered by Microsoft about malware to find suspect files. Instead of scanning all files, which would consume enormous server resources, Microsoft Defender for Office 365 focuses on blocking the spread of malware. When a user shares a document, it checks whether sharing should go ahead. If all is well, sharing proceeds as normal. If not, SharePoint locks the file and disables the ability to download, open, or share it. The user can remove the file to solve the problem. See the Mail Flow chapter for additional information about Microsoft Defender for Office 365.

Restore This Library for SharePoint Online

To help recover documents from accidental deletions, a malware attack, or other data loss, the Restore this library feature (available to administrators and site owners in the library settings panel) is a self-service recovery mechanism to allow site administrators and site owners to roll back changes made to a document library to any point in time during the last 30 days. You can select from several out-of-the-box restore points (Yesterday, One week ago, Three weeks ago, Custom date and time), or use a slider to move through the set of changes for the library to select any point up to the 30-day limit (Figure 7-2). The changes that can be rolled back include updates to document properties such as title or assigning a retention label.

After you select a restore point, SharePoint prompts you to confirm to go ahead with the restore, and if confirmed, SharePoint rolls back all the changes from the library to the chosen point in time to restore the library to its state at that time.

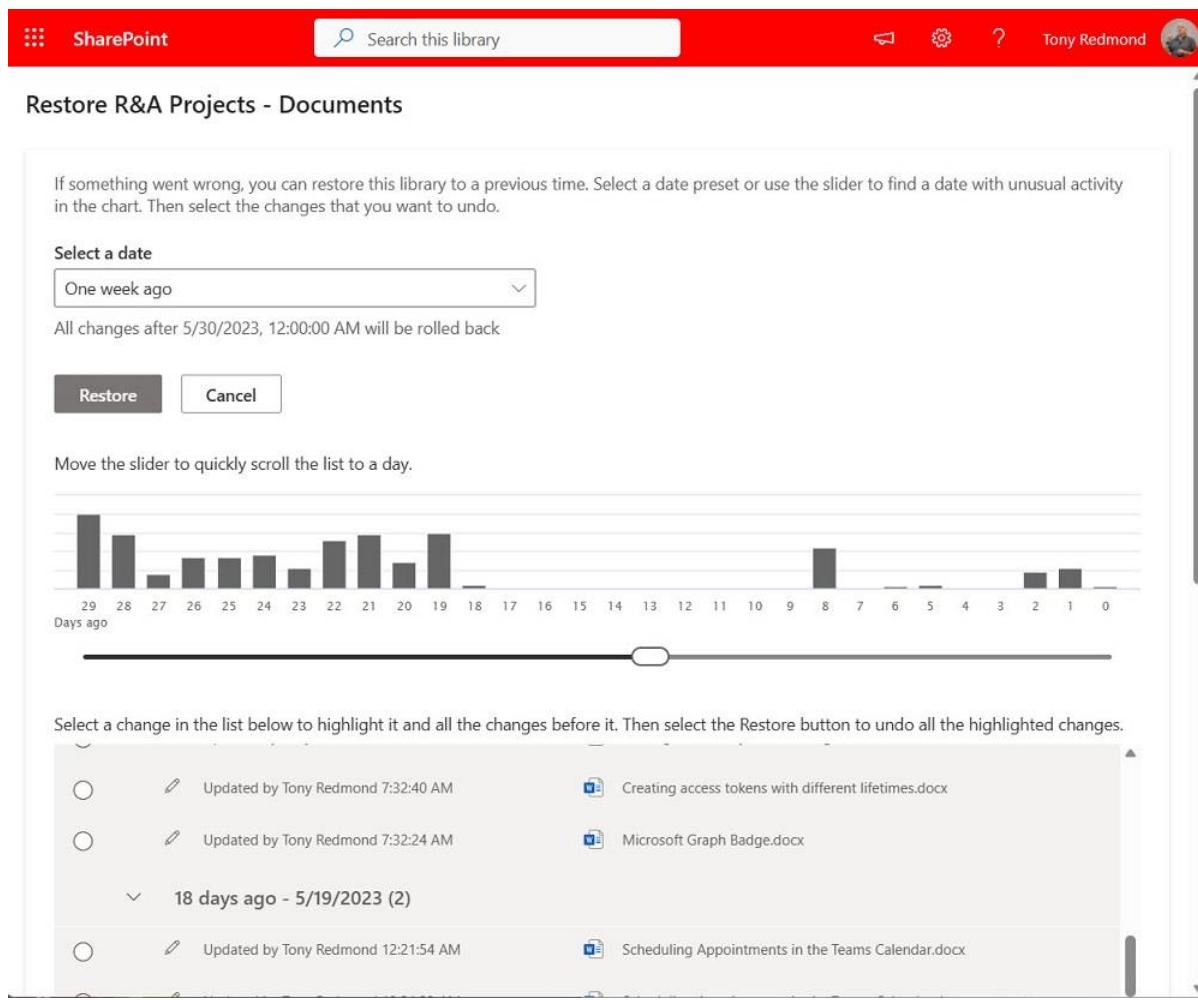


Figure 7-2: Using the Restore this library feature

Multi-Geo Support for SharePoint Online

[Multi-Geo support for SharePoint Online and OneDrive for Business](#) is a mechanism to control where data from both services are stored at rest to meet data residency requirements when users work in multiple regions other than the default region for the tenant. [Multi-Geo capabilities are available as an add-on for specific Office 365 Plans](#) for Enterprise Agreement (EA) and CSP customers. Note that Microsoft requires customers wishing to support users in satellite regions to purchase multi-geo licenses for at least 5% of the eligible Microsoft 365 seats in the tenant. Furthermore, Multi-Geo Capabilities in Microsoft 365 are governed by a user-level add-on license meaning that each user in a satellite region must have a multi-geo license. For more information about multi-geo, including pricing, contact your Microsoft account team.

Encryption for SharePoint Online and OneDrive for Business Storage

Files in SharePoint Online and OneDrive for Business are protected by unique, per-file keys that are exclusive to a tenant. The keys (AES 256-bit), which are created and managed by the SharePoint Online service itself or by customers (when customer-managed keys are used), are used to encrypt files stored in SharePoint Online and OneDrive for Business.

Comments on non-Office files in SharePoint Online and OneDrive for Business

The Microsoft 365 file viewer supports more than 350 file types and includes the ability for users to collaborate and communicate about non-Office files with comments and replies. Anyone who opens a non-

Office file can view the comments through the details pane and leave additional comments. File owners will receive notifications when someone comments on their files. Notifications are also sent to users when someone leaves a reply to their comments. Users may unsubscribe from these e-mail notifications via the "Unsubscribe" link in the notification e-mail.

Intelligent File card in SharePoint Online and OneDrive for Business

The File card in SharePoint Online and OneDrive for Business incorporates several [intelligent features](#) to quickly get deeper information about relevant activities happening around the document (edits, mentions, and comments), document statistics (number of views, number of viewers, and details about who viewed the file), suggestions about to who share the document based other people the current user frequently works with, and [conversations](#) happening in e-mail or Teams about the document.

SharePoint App Bar

The [SharePoint App bar](#) and the SharePoint start page give users direct access to relevant sites, news feeds, lists, and files. From the App Bar, users can also [create Sites, Lists, Documents, pages, and news](#). The SharePoint App Bar cannot be disabled.

SharePoint eSignature

[SharePoint eSignature](#) is an electronic signature service to enable signature processing for PDF documents stored in SharePoint Online for both internal and external recipients. eSignature is a pay as you go service (\$2 per request) initially only available in the US.

Signature requests created in document libraries where eSignature is enabled create [working copies of the documents stored in a hidden document library](#). The working copies:

- Appear as unsigned until all the recipients have signed the documents.
- Are retained for five years or in accordance with the document retention policy defined by the SharePoint or tenant administrator.

[SharePoint eSignature integrates with third-party electronic signature services](#). For now, it supports integration with DocuSign and Adobe Sign.

SharePoint and Viva Connections Brand Center

The [Brand Center](#) supports central management for brand assets (colors, fonts, and images) and themes for SharePoint sites, pages, and Viva Connections. To activate the Brand Center, a Global Admin needs to perform the following steps:

- Create a new Site in the tenancy or select an existing Organization Assets site or create a new Site to host the Brand Center app.
- Enable the use of public CDN (Note: This step is not necessary if the tenant is configured to use a private CDN).

Once the Brand Center is enabled, users with the right permissions in the Brand Center site can perform the following tasks:

- Upload branding assets such as custom fonts and images to customize sites. Custom fonts are initially supported in specific areas of SharePoint sites as well as some of the default Web Parts provided by Microsoft.
- Create new brand colors that can be used in custom themes.

- Create custom themes that can be applied to existing sites and Viva Connections experiences. Note that themes previously created with PowerShell remain outside of this management experience in the Brand Center.

OneDrive for Business

OneDrive for Business (or OD4B as it is known in the Microsoft 365 ecosystem) is a cloud-based file sharing service based on SharePoint Online that provides users with personal storage. From an administrative perspective, a OneDrive account behaves like a personal version of a SharePoint document library. Microsoft Search indexes all the information stored in OneDrive, meaning that it is discoverable and available for compliance purposes.

Referring to anything as a personal storage space is a bit of a mouthful. In a practical sense, users can store anything in their OneDrive for Business account, just like they would do with a personal network share on an old-fashioned file server. Indeed, the prime purpose of OneDrive for Business is to help companies to wean themselves off file servers by moving the content held on the servers into the cloud. Users who have personal files stored in network shares can move their information to OneDrive for Business while Teams or SharePoint Online team sites are good homes for organizational or shared information.

Access on Multiple Devices

The big advantage of using OneDrive for Business from a user's perspective is that once they store files on OneDrive, the files are available from any device. When network connectivity was not as pervasive and capable as it is now, it would not have been possible to contemplate such a movement, but it is now. Although you need to have network access to browse OneDrive for Business sites, the OneDrive sync client allows users to work with files copied to a local cache. Some restrictions exist in terms of the types of files and the names of files that OneDrive for Business supports. It is sensible to check on the [current limits and restrictions](#) before you start a project to help users move their information from file servers. The limits for the current OneDrive sync client are much higher than in earlier versions, so you should confirm whether any limits that stopped a project moving forward still exist. It is also sensible to implement whatever controls are necessary for client synchronization at the start of a migration project instead of trying to retrofit some restrictions afterward.

The ability of OWA, Outlook, and Teams to access files held in OneDrive for Business gives further encouragement to use the service. For example, users can upload files to OneDrive for Business and then send a link to the attachment (a "cloudy" attachment). Users can also save attachments from Outlook or OWA directly to OneDrive for Business or to the document libraries in Groups and Teams where they are members. The intention behind making these features available is to help users change their habit of storing email attachments on their local PCs and refocus toward cloud-based storage instead. Whether it is possible to break the "always send full copies of attachments by email" habit is debatable. What is for sure is that breaking the habit requires people to change their personal workflow, and that is always hard.

Another advantage gained by keeping files in OneDrive for Business is that users can grant others the right to edit the document in place, which might encourage better collaboration. By using cloudy attachments, recipients always work with the latest version of the information because they access the version held in OneDrive for Business rather than a personal copy. This avoids the problem where individual recipients update their copies of files received as attachments and thus create the requirement for manual reconciliation of the various edits.

Install OneDrive as a Progressive Web App: OneDrive can be [installed as a Progressive Web App](#) in Microsoft Edge, Google Chrome, or any other modern web browser that supports Progressive Web Apps.

OneDrive for Business Contents and Limits

The first time a user accesses OneDrive for Business, SharePoint Online provisions the site. Once the site is ready, the user can upload files to the site and share those files (or complete folders). Users can attach files from OneDrive to messages as easily as local files. To ensure that users have enough space to move their personal information from old file servers, [depending on their license type](#), users receive up to 1 TB of online storage, which comes from an allocation that is separate from and not counted against the pooled storage used for SharePoint Online. Tenants that have five or more licenses for E3 or higher enterprise plans (plus government and academic equivalents) can take advantage of "unlimited storage".

OneDrive assigns a default storage quota of 1 TB to each user for their personal site, which should be enough to move personal files off file shares and even from local PC hard drives. If you want to adjust the OneDrive for Business storage for an account, you can either send a support ticket to Microsoft or ask an administrator to run the *Set-SPOSite* cmdlet to increase the quota. Here is how to increase the storage quota from the default 1 TB to 5 TB for the *Tony.Redmond@Office365ITPros.com* account.

```
Set-SPOSite -Identity
https://office365itpros-my.sharepoint.com/personal/tony\_redmond\_office365itpros\_com -StorageQuota
5242880
Get-SPOSite -Identity
https://office365itpros-my.sharepoint.com/personal/tony\_redmond\_office365itpros\_com | Format-List
```

[This article](#) describes how to assign OneDrive for Business storage quotas based on group membership and includes an example script. If the tenant has the necessary Entra ID P1 licenses, membership of administration units could replace groups.

You can keep on increasing the storage quota assigned to a OneDrive for Business account in 5 TB chunks as the need arises. For instance, if an account approaches the 5 TB storage limit, you can increase the quota to 10 TB (set the value to 10485760). An attempt to increase the quota will only succeed if the used quota approaches a chunk boundary. In other words, you cannot increase the quota assigned to an account from 3 TB or 15 TB but must first increase the quota to 10 TB and then wait until the storage used passes 12 TB or thereabouts before upping the quota to 15 TB.

To check the quota assigned to each user and how much of the quota they use, you can run the following PowerShell snippet.

```
Get-SPOSite -IncludePersonalSite $True -Limit All -Filter "Url -like 'my.sharepoint.com/personal/' |
Select Owner, StorageUsageCurrent, StorageQuota
```

Owner	StorageUsageCurrent	StorageQuota
-----	-----	-----
james.gangley@office365itpros.com	1	1048576
brian.weakliam@office365itpros.com	1	1048576
tony.redmond@office365itpros.com	3727	5242880

No error checking is in this simple code, so you will see an error if an attempt is made to check a user's OneDrive site that has not yet been provisioned because the user has never used OneDrive. To fix that problem, you can request OneDrive for Business to provision a site for the user by running the *Request-SPOPersonalSite* cmdlet. The input is a comma-separated list of email addresses for the users for which OneDrive is to create sites. You can specify up to 200 email addresses in the list.

```
Request-SPOPersonalSite -UserEmails "Sanjay.Ramaswamy@Office365ITPros.com,
David.Pelton@Office365ITPros.com" -NoWait
```

OneDrive uses a timer job to create the sites. The actual time when the sites are available depends on the system load.

Views and Sections in OneDrive for Business

OneDrive for Business includes different views and sections to give the user the ability to access their files and the information they have shared with other users and the information other users have shared with them. Table 7-3 details the current views included in OneDrive for Business.

Information View/Section	Information View/Section Details
Home	This view shows files recommended for the user and a list of recent files the user has worked on across Microsoft 365. For each file, OneDrive lists relevant file activity such as when it was last opened, the file owner, and the last activity for the file.
My files	Shows the files and folders stored in the user's OneDrive for Business account.
Shared	Two information views are available. "With you" shows files and folders shared with the user including who shared the file or the folder and the last file or folder activity. When a user opens a shared folder in this view, he/she is taken to the shared folder within the People view of his/her own OneDrive. "By you" view shows the files the user has shared with other users and the last file activity.
Favorites	Shows a list of files tagged as favorites across Microsoft 365 (in the Microsoft 365 Home page, in SharePoint Sites, or OneDrive).
People	Shows a list of shared files organized by the people who shared them with the user.
Meetings	Displays a list of files shared in Teams meetings.
Media	Allows users access to photo and video content in OneDrive.
Quick access	Lists the different document libraries the user has access to. Document libraries appear in two categories: "Frequent" and "Followed". From the Shared libraries view, users can create new document libraries and/or access the SharePoint Online landing page.

Table 7-3: Information Views in OneDrive for Business

Some of [these views are also available in File Explorer in Windows](#) (Recommended files, Favorites files, and Recent files).

Content creation in OneDrive for Business

OneDrive for Business users can create new content by selecting the **Add new** button to:

- Create new folders.
- Upload files and folders.
- Create a document (Word, Excel, PowerPoint, OneNote, Forms for Excel, Visio drawing) from a blank template.
- Create an Office document (Word, Excel, PowerPoint) from a Microsoft-provided template or an organizational template stored in an organizational asset library configured in the tenant.
- Create a link to a web page or a document.

Sharing in OneDrive for Business

Sharing is one of the key capabilities provided by OneDrive for Business driven by the same features previously described for SharePoint sites.

OneDrive for Business Link Open Receipt

When a user opens a file or folder shared from OneDrive for Business, the service sends an e-mail to the user who shared the item to notify them about the opening of the file or folder. The notification e-mail also includes a link to file or folder permissions management to review how the file or folder was shared and even remove the sharing link.

Customer Branding in Sharing Email

If a tenant configures Entra ID with custom branding for the organization, their [logo appears in the sharing e-mail sent](#) when a file is shared from OneDrive for Business or SharePoint Online. Information about how to apply custom branding for Entra ID is in the Identities chapter.

Add a Shortcut to OneDrive

The Add Shortcut to OneDrive feature allows users to add shortcuts to SharePoint Online and OneDrive for Business folders and files that they commonly access. This feature only applies to folders and files in the same tenant. The folders and files can be:

- Folders and files shared with the user from OneDrive or SharePoint.
- Folders and files in any SharePoint Online document library the user can access.

[To add a shortcut to a shared folder](#) in OneDrive, select Shared > Shared with me in OneDrive and then click Add shortcut to My files. Following the same approach, users can add a shortcut to any folder or file they can access in Teams or SharePoint. Shortcuts appear in OneDrive's My Files view. Folders pointed to by Shortcuts are accessible from any OneDrive App, synced across all devices, and shared like any other folder owned by the user. Owner information is visible in the Sharing column to differentiate it from the user's own content. The group name appears for content shared from sites owned by Microsoft 365 groups. Shortcuts to shared folders retain all policy, compliance, and permissions settings from the source. Shortcuts [can be moved from the Files root in OneDrive to a public or shared folder](#).

When the user deletes a file or folder shortcut, OneDrive only removes the shortcut and keeps the shared files and folders intact.

OneDrive Client and Synchronization

A key OneDrive for Business benefit is the ability to synchronize content stored in SharePoint Online document libraries and OneDrive for Business accounts to workstations using the OneDrive Sync Client. System requirements for the OneDrive Sync Client, including the list of supported platforms and operating systems, are detailed in [this support article](#). In addition, [Microsoft has a native OneDrive for Business Sync Client for ARM devices](#) for Windows and Mac OS and Apple Silicon devices (currently in preview).

The synchronization mechanism depends on the host operating system and application. For Windows, OneDrive uses the Windows Push Notification Service (WNS) to synchronize files. The basic approach is:

- A change occurs in a file stored in Microsoft 365. WNS notifies the OneDrive sync client of the change.
- The OneDrive sync client adds the change to its Internal Server Changes Queue. If the change involves file metadata, like renaming or deleting a file, the client processes the change immediately. Otherwise, the sync client starts a download session to update the local copy of the file.
- When a file change happens locally, WINS notifies the OneDrive sync client that it needs to update the copy in Microsoft 365.
- The client starts a session to upload the file to Microsoft 365.

The synchronization mechanism differs depending on the file type. For non-Office files, the client uses Background Intelligent Transfer File (BITS) sessions. The client transfers files smaller than 8 MB in a single HTTPS request. It divides larger files into chunks and transmits them separately to the service. Each chunk has a unique identification and a separate key for protection. After the client has transmitted all the chunks, the server can reassemble the file. This mechanism allows the OneDrive sync client to process very large files up to the 250 GB current limit.

Office applications have built-in synchronization capabilities to enable features like autosave and co-authoring. The OneDrive sync client offloads synchronization processing to the relevant Office application, which sends changes to SharePoint Online or OneDrive for Business. This can only happen when the Office application is active. If it is not and it must copy an Office document, the OneDrive sync client processes it like it would any other file.

OneDrive Sync Client and Files on Demand

The OneDrive for Business sync client (OneDrive.exe) supports OneDrive for Business and SharePoint sites, including the document libraries used by Groups and Teams, and can perform read/write synchronization of document libraries with more than 20,000 files, including required metadata. The client is integrated with Windows File Explorer to allow users to choose which files have local copies and which are copied on demand (when needed). A feature called Differential Sync copies only the parts of files changed during edit sessions instead of the entire file. This feature is especially important when the OneDrive sync client processes large files up to its 250 GB limit. The sync client can pause synchronization in low-bandwidth environments (such as when connected to Wi-Fi on an airplane).

Restrictions and Limitations in OneDrive for Business Synchronization: OneDrive for Business can sync both OneDrive for Business libraries as well as SharePoint Online document libraries from team sites, but there are some [documented restrictions and limitations](#) that must be considered when synchronizing files to a local workstation. The file size limit for both SharePoint Online and OneDrive for Business is 250 GB. This limit applies to web uploads and synchronization activities.

The **Sync** section in Settings in the SharePoint admin center includes the **Show the Sync button on the OneDrive site** setting to control access to the sync client for the tenant. You can hide the button completely if you do not want users to be able to synchronize OneDrive to their workstations.

Files On-Demand is a feature that allows users to control local storage for files held in OneDrive for Business or SharePoint Online sites. The feature is managed through the **Settings → Sync and backup** tab of the OneDrive sync client, where users can set the checkbox to enable Files on Demand for their account. Afterward, they can select how to store remote files locally for the folders from OneDrive and any synchronized SharePoint site that they want to see on the device. Synchronized files can usually be in the following states:

- **Online-only files** are in OneDrive or SharePoint sites but appear in File Explorer to let the user know that they exist. These files occupy no disk space on the local computer.
- If users open online-only files, File Explorer downloads them from the host site and makes the files **locally available**. A locally available copy can be opened at any time, even if a network connection to a document library is unavailable. When a network connection becomes available, the OneDrive sync client synchronizes any changes made on the workstation with the host site.
- Users can also decide to mark files as **Always keep on this device**. This means that the OneDrive sync client copies these files from the host site to make them available locally even if the user never opens them.

File Explorer uses [different icons to show users the status of files](#). Online-only files have a cloud icon, while copies available locally have a white circle with a green checkmark, and files always present on the device have a green circle with a white checkmark (Figure 7-3).



Figure 7-3: Files On-Demand icons

When the OneDrive sync client is processing a file, the icon changes to two curved arrows in a circle. To change the synchronization status of a file, select it (or several files at one time), and use the right-click menu. You can see the icon showing the synchronization state of the files in the Status column. Files on Demand settings are unique to a device. If you use several devices, you must configure the settings on each device.

Reset the OneDrive Sync Client: Sometimes the OneDrive sync client can experience issues that cannot be resolved through normal troubleshooting techniques such as pausing synchronization for a short time or stopping and restarting the sync client. If necessary, you can resolve the problems by resetting OneDrive by typing the following instruction in the Windows command line:

```
%localappdata%\Microsoft\OneDrive\onedrive.exe /reset
```

This command forces OneDrive to perform a complete synchronization of all connected personal and business sources, including the user's OneDrive for Business account and any SharePoint Online document libraries they have opted to synchronize. After running the reset, you might need to manually restart OneDrive. As the operation resets all OneDrive settings, if the user has selected to synchronize specific folders, they must [make the folder selection](#) again.

Files on Demand Prerequisites

Files On-Demand prerequisites for Windows platforms are detailed in [this support article](https://support.microsoft.com/en-us/article/save-disk-space-with-onedrive-files-on-demand-for-windows-10-0e6860d3-d9f3-4971-b321-7092438fb38e). The prerequisites for MacOS are outlined in [this article](#). Files On-Demand is part of the [Storage Sense](#) feature, so when disk space runs low, OneDrive frees up space automatically by moving back the oldest files (not marked as "always keep on device") to a cloud-only state.

Support for UPN changes in the OneDrive sync client: the OneDrive sync client for both Windows & Mac automatically syncs the correct OneDrive location after a user's UPN changes. To learn how UPN changes affect OneDrive, see this [Microsoft article](#).

Open in App

[Open in App](#) is a feature available in OneDrive for Business, SharePoint Online, and Teams to allow users to open Office and non-Office files in their native applications. If a default app is not configured, the user is asked to select a default app to open the file type. Open in app requires the OneDrive sync client to be installed and running. If the sync client is not running, opening in the app will start the client.

Disable Windows Permission Inheritance in Folders Synced Read-Only

Through [this setting](#) in the Group Policy for OneDrive for Business, admins can instruct the sync client to manage permission inheritance for folders that are synced as read-only on a Windows Computer. When enabled, the performance of the sync client is better when synchronizing folders for which the user has only read-only permissions.

Smart Upload Management

[Automatic bandwidth management for upload](#) controls the sync client upload rate based on bandwidth availability. In this mode, OneDrive consumes only unused bandwidth to cause no interference with any other network application. Smart Upload Management uses the Windows LEDBAT (Low Extra Delay Background Transport) protocol and is available on devices running Windows 10/11 or Windows Server 2016 (or later).

OneDrive Sync Client Mass Delete Prompt

OneDrive monitors the removal of files from a device and prompts for confirmation if the user deletes many synchronized files on their computer at one time. If the user didn't intend to delete so many files, they can tap **Restore Files** to recover. If not, OneDrive removes the files from the device and the cloud locations. If a user wants to skip the new behavior, they can select the Always remove checkbox to skip the prompt for future mass deletes.

Error Resolution for Illegal File and Folder Names in OneDrive

There are situations where the OneDrive client can't sync a file or a folder because its name contains invalid characters. To solve the problem, the OneDrive client includes a **Rename** button to automatically fix these sync problems when file and folder names meet the following criteria:

- Beginning or ending with a space.
- Beginning or ending with a period.
- Containing unsupported [Unicode](#) code points.
- Named with [surrogate](#) pair issues.

In all these situations, OneDrive replaces the illegal character with an underscore. As detailed in [this support article](#), there are still other invalid characters that cannot be renamed by the Sync client. To help users fix invalid characters, Microsoft created the [Incident deflection feature for the Sync Client](#), an in-app resolution to sync errors. For example, when the sync client meets an invalid condition like using an asterisk "*" symbol or any file name starting with "~\$.", the OneDrive sync client renames the file and continues with the upload.

Request Assistance Feature

A ["Get Help" option](#) in the OneDrive activity center is available for end users so they can initiate a support ticket in case they have problems with the Sync client. Administrators can turn off this setting by running the PowerShell command:

```
Set-SPOTenantSyncClientRestriction -DisableReportProblemDialog $True
```

Sync Machine Specific Files

The OneDrive sync client is designed to ignore machine-specific files used by File Explorer on Windows and Finder on macOS, but situations exist where these files might end up in OneDrive such as during a file migration. To prevent the visible errors displayed when those files are copied to OneDrive, the Sync client will delete the erroneous copy without touching the local copy.

Per-machine Sync Client Installation

Instead of installing the OneDrive Sync client for each user account under the "%localappdata%" folder, you can install a shared version of the sync client under the "Program Files (x86)" directory. This means that all the profiles on the computer use the same OneDrive.exe binary. [Per-machine installation mode](#) enables the following scenarios:

- Automatic conversion from per-user to per-machine.
- Automatic updates when a new version is available.

Exclude Specific Files from Upload

[This setting](#) prevents the sync client from uploading specific files to OneDrive or SharePoint sites. Excluded files appear in File Explorer with a "do not enter" icon in the Status column. It can be set in the admx/adml files. Once enabled, the sync client will not upload new files that match the specified restrictions. There is no impact on existing files uploaded to OneDrive and SharePoint.

Controlling Sync Client Auto-pause Behavior

OneDrive users can [control the OneDrive sync client's auto-pause behavior](#) on their PCs when they are connected to a metered network or if the device is in battery saver mode. The options to control this behavior are found in the Settings menu.

Controlling Client Synchronization

A common issue often raised by management and those responsible for the protection of intellectual property is the potential undesirability of allowing users to synchronize documents to their PC, possibly including a PC at home. The same synchronization issue occurs for SharePoint Online document libraries too. Users often store confidential information on home PCs (the blurring of home and work life encourages this practice). It's also true that various blocks can prevent this behavior (such as [restricting synchronization to domain-joined PCs](#)). However, users have been swapping data between PCs ever since floppy diskettes and will likely find new methods of moving information to desired locations as quickly as IT closes off loopholes.

Automatic Updates: Microsoft releases updates to the new OneDrive client independently of other updates. The updates are downloaded and installed automatically on client computers unless a [group policy is implemented to control OneDrive updates](#). Like many current Microsoft products, OneDrive updates are released in "rings". You can update a PC to receive updates faster by configuring a system registry DWORD value called **EnableTeamTier_Internal** at HKEY_CURRENT_USER\Software\Microsoft\OneDrive. Set the value to 1 if you want to receive early updates (fast ring) or 0 (zero) to receive updates as normal (slow ring).

Several approaches can help control the content held in OneDrive for Business sites. First, sensitivity labels (see the Information Protection chapter) can protect confidential information so that only the intended recipients can open protected files. Second, Data Loss Prevention policies can stop users from inadvertently sharing sensitive information outside the company. Third, as mentioned above, you can configure SharePoint Online so that the OneDrive sync client will only copy files to workstations that belong to specific on-premises Active Directory domains. The intention here is to stop corporate data from ending up on PCs not managed by the organization, such as home devices. As shown below, the synchronization block is set by running the [Set-SPOTenantSyncClientRestriction](#) cmdlet to enable checking against a set of known domains, each of which is identified by a GUID. You can use the `Get-ADForest` PowerShell cmdlet to return the set of domains in an Active Directory forest and then `Get-ADDomain` cmdlet to find the `ObjectGUID` for each domain (see [this page](#) for information on how to determine the `ObjectGUID` for a domain).

```
Set-SPOTenantSyncClientRestriction -Enable -DomainGuids 'Domain-GUID1; Domain-GUID2; Domain-GUID3'
```

When the block is in place, users see that they cannot synchronize OneDrive for Business libraries for offline access on an unmanaged PC. Administrators can use information in the audit log (see the Managing Reporting and Auditing chapter) to create a report to highlight computers that OneDrive blocks from syncing files to discover whether users have tried to take files offline and then take the necessary action to tell those users why this facility is unsupported.

Although this synchronization block will not stop mobile clients from using OneDrive for Business, it does block Mac clients. For this reason, you should not implement the block if Mac clients are in use in your organization. Another restriction is to constrain users to upload files with a set of known extensions. For

example, if you do not want to have users uploading executables, zipped files, and PSTs to OneDrive for Business, you can run the following cmdlets:

```
Set-SPOTenantSyncClientRestriction -ExcludedFileExtensions "exe;zip;rar;pst"
```

```
Get-SPOTenantSyncClientRestriction
```

TenantRestrictionEnabled	AllowedDomainList	BlockMacSync	ExcludedFileExtensions
False	{}	False	{exe, zip, rar, pst}

Separate each file extension with a semi-colon and do not leave any extra spaces. The *Get-SPOTenantSyncClientRestriction* cmdlet can check that the proper restriction is in place. If necessary, you can clear the set of excluded files by setting the property to *\$Null*. The setting only controls the OneDrive.exe Windows client, so you can add excluded files to a OneDrive for Business site with another client before the exclusion kicks in to prevent file synchronization with the PC.

Blocking OneDrive Consumer: The OneDrive sync client can synchronize both OneDrive for Business and OneDrive consumer accounts to a single PC. Consumer accounts can be manually added to the Sync client by end users or automatically detected by the Sync client, which will prompt end users if they would like to sync their consumer files using the detected account. Some organizations do not want to allow users to synchronize their OneDrive consumer accounts to corporate PCs. It's possible to block synchronization of consumer accounts through a Group Policy setting called *DisablePersonalSync*. For organizations that allow end users to manually sync consumer accounts but want to disable the autodetect prompt messages, the *DisableNewAccountDetection* policy setting blocks those messages. See [this Microsoft page](#) for information on how to control the settings and to learn about other Group Policy settings used with OneDrive.

The last approach is to remove the temptation for users to synchronize files from certain document libraries by hiding the Sync button for those libraries. If the Sync button is not available for a document library, users cannot start the synchronization process. To do the job, you need to write some PowerShell code that uses PnP PowerShell cmdlets. Fortunately, [an example exists](#) to help start the job. You can take the sample PowerShell code and change it to meet your needs. For instance, you might use a CSV as the input to specify the target sites to disable synchronization. It is important to realize that removing the Sync button will not interfere with or stop synchronization if the user previously set it up for a document library. However, it stops new synchronization.

It might seem that controlling client synchronization is a big issue for OneDrive, but it is not really. Similar issues to those listed above often happen in how people use (or abuse) personal file shares. The best thing about ODFB is that all the features of Microsoft 365 security and data governance protect the information in user sites. In addition, because OneDrive for Business is an area of focus for Microsoft, a reasonable expectation exists that more features will become available over time.

Prevent Users Syncing Content from Shared Libraries in Other Organizations

[B2BSync](#) allows users to sync SharePoint and ODFB content shared with them by people from other organizations. This feature works with the external sharing integration previously described and requires recipients to have a guest user account. B2BSync can be disabled through the *BlockExternalSync* setting as described in the *adm\OneDrive.admx* and *OneDrive.adml* files.

Allow Syncing OneDrive Accounts for Specific Organizations

This [setting in the OneDrive for Business policy](#) prevents users from uploading files to other organizations by creating a list of allowed organization IDs (Tenant IDs). When enabled, users see an error if they try to add an account from a prohibited organization. This setting takes priority over Block syncing OneDrive accounts for specific organizations.

Configure OneDrive to Automatically Sync SharePoint Team Site Document Libraries

This feature allows administrators to [automatically connect and synchronize specific SharePoint team site document libraries](#) as part of a OneDrive deployment. To help configure a team site to sync automatically, a new group policy ("Configure team site libraries to sync automatically") is available for admins to deploy.

Once deployed, the OneDrive sync client automatically syncs the contents of the shared library as online-only files the next time the user signs in, within an 8-hour window to help distribute network load. Once configured, the user cannot stop syncing the shared library unless they disable the policy. Disabling the policy does not unmount the shared library but does make the option to stop syncing the library available.

PC Folder Backup

[PC folder backup](#) simplifies the process of moving user contents located in well-known PC folders (Desktop, Documents, and Pictures folders) to OneDrive for Business. PC folder backup automatically syncs user content held in several well-known PC file locations to OneDrive for Business. To start using this feature, end users only need to click on a PC folder backup toast notification or click the **Manage backup** button under the Sync and backup tab of OneDrive Client settings dialog. Before the OneDrive sync client starts synchronization, it checks for the presence of any unsupported files and then begins to copy the folders from the workstation to OneDrive. Well-known folders are created in the user's OneDrive using the same locale present in the user's workstation. PC folder backup works on Windows 10, and 11 workstations.

PC folder backup also comes with the ability to silently redirect Windows known folders to OneDrive without user interaction. To enable this setting, a group policy must be enabled.

Restore files to their original location when turning off folder backup: When users turn off PC Folder Backup, they have the option to restore the files back to their original location. If a folder contains files stored in the cloud, those files will not be moved and remain in the cloud.

OneDrive Sync Health Reports

The [OneDrive sync health reports](#) section in the Microsoft 365 Apps Admin Center is a dashboard to check and identify OneDrive sync app versions, sync status, sync errors on individual devices, and monitor the deployment of OneDrive features such as KFM. To feed that dashboard, Admins can configure the OneDrive sync client to send health and diagnostics data by using the Group Policy Object setting [EnableSyncAdminReports](#).

The dashboard includes a summary of how well OneDrive synchronization works within the organization in terms of how many devices have at least one sync error, the percentage of computers synchronizing known folders (KFM), and the percentage of computers with the current version of the OneDrive sync client. The Details tab provides deeper and more granular information on the OneDrive sync status for each user in the organization. Administrators can use this information to track sync errors, review error details, and do some basic troubleshooting tasks before contacting users experiencing sync problems. The Issues tab shows an aggregated view of the top sync errors happening to end users including the number of affected devices.

Offline Mode in OneDrive for Web

Offline mode in OneDrive for Web allows users to continue working with the OneDrive browser app, OneDrive PWA, or Teams when they are offline. Enabled by default, this feature is available on Windows and macOS devices where the OneDrive sync client is running and allows users to view, rename, move, and copy files and folders. OneDrive automatically synchronizes any change made offline when Internet connectivity is restored. Admins can control some offline mode settings using [OneDrive for business Group Policies](#).

Restore a OneDrive for Business Account

Ransomware has the nasty habit of infecting important documents, no matter what their location. If an attack happens against a OneDrive site, you can use **Restore Your OneDrive** (click the cogwheel to expose the option) to restore files from the document library versions to a point in time. OneDrive comes with some out-of-the-box restore points (such as a week ago), but you can select any point up to a 30-day limit. When you select a restore point, OneDrive prompts you to confirm to go ahead with the restore, and if confirmed, OneDrive restores files as they were at that point.

The consumer version of OneDrive also supports the ability to restore synchronized files to a point in time. The feature is only available with a paid subscription (Microsoft 365 Personal or Microsoft 365 Family).

Managing OneDrive for Business

While OneDrive for Business is a core service in Microsoft 365, it no longer has a dedicated administrative console. Instead, all the required OneDrive admin features are part of the SharePoint admin center. Currently, the following OneDrive admin controls are available in the SharePoint admin center (Settings page):

- Notifications: Enable/Disable device notifications about OneDrive activities.
- Retention: Set the default OneDrive retention period for deleted users.
- Storage: Set the default OneDrive storage limit applied to all the users in the tenant.
- Sync: Manage the following OneDrive sync controls:
 - Show/Hide the sync button in OneDrive and SharePoint Document libraries.
 - Enable synchronization only on devices joined to specific domains that are identified by a GUID.
 - Block the upload of specific files in OneDrive.

Admins can also manage specific settings of OneDrive sites through the user details panel in the Microsoft 365 Admin center. Specifically, the following OneDrive options can be administered through the panel:

- Storage limit: By default, this setting honors the global OneDrive storage limit value, but it can be overridden to set a specific value for the user.
- Manage external sharing: This setting updates the global OneDrive sharing setting to another sharing option.
- Create an Admin link to the user's OneDrive so the administrator is added as a OneDrive admin.

Using PowerShell to Manage OneDrive for Business

Although Microsoft offers no specific tools to manage OneDrive for Business with PowerShell, the same principles and guidelines used for SharePoint Online apply. A SharePoint Admin can also use the SharePoint Online Management Shell, PnP Cmdlets, and SharePoint and Microsoft 365 APIs to manage OneDrive. For example, to generate a CSV file with details of the storage quota, consumption, and percentage of storage used for the OneDrive for Business sites, run the following PowerShell code:

```
$ODFBSites = Get-SPOSite -IncludePersonalSite $True -Limit All -Filter "Url -like 'my.sharepoint.com/personal/*'" | Select-Object Owner, Title, URL, StorageQuota, StorageUsageCurrent | Sort StorageUsageCurrent -Desc
$TotalODFBGBUsed = [Math]::Round(($ODFBSites.StorageUsageCurrent | Measure-Object -Sum).Sum /1024,2)
$Report = [System.Collections.Generic.List[Object]]::new()
ForEach ($Site in $ODFBSites) {
    $ReportLine = [PSCustomObject]@{
        Owner      = $Site.Title
        Email     = $Site.Owner
        URL       = $Site.URL
        QuotaGB   = [Math]::Round($Site.StorageQuota/1024,2)
        UsedGB    = [Math]::Round($Site.StorageUsageCurrent/1024,4)
        PercentUsed = [Math]::Round((($Site.StorageUsageCurrent/$Site.StorageQuota * 100),4) }
```

```
$Report.Add($ReportLine)
$Report | Export-Csv -NoTypeInformation c:\temp\OneDriveSiteConsumption.csv
Write-Host "Current OneDrive for Business storage consumption is" $TotalODFBGBUsed "GB. Report is in C:\temp\OneDriveSiteConsumption.csv"
```

Because many different types of sites exist in SharePoint Online the code needed to create a storage report for SharePoint Online sites is a little more complicated. An example script is [available in GitHub](#).

Modern OneDrive Settings

The modern OneDrive settings page gives access to the minimum settings required by any user to manage his/her OneDrive for Business site. Compared with the classic OneDrive for Business admin options, the settings page only includes two sections: Notifications and More settings. Notifications are all about enabling/disabling the different notifications related to OneDrive activities:

- Reminders for missed Sharing emails.
- Notifications sent when OneDrive detects massive files deletion over a short period.
- Notifications sent when others reply to user comments.
- Notifications sent when others comment on the user's documents.
- Notifications sent when the recipient clicks the link in a sharing e-mail.
- Notifications sent when others upload files to file requests.
- Send a daily digest of all Loop app notifications sent.

Additional settings include links to different OneDrive configuration options such as Manage guest expiration, Site administrators, Run sharing report, Regional and language settings, Site features, and Storage metrics. The page also includes a link to the classic OneDrive settings page.

Microsoft Loop

Microsoft Loop is built with Microsoft's Fluid framework, a technology ([available as open source software](#)) designed to help developers build better collaborative applications using "live" components, now called loop components. The big selling point for the Fluid framework is its synchronization capabilities, which allow components to coordinate updates made by multiple people in shared content. The Microsoft Loop app organizes information into workspaces, pages, and individual components and stores its information in special hidden SharePoint Online sites within tenant data boundaries. Loop components are also available in several Microsoft 365 apps, including Teams chat and channel conversations, OWA, SharePoint pages, Word Online, Microsoft Whiteboard, and Outlook desktop (Win32 classic and Outlook Monarch). See the Teams chapter for more information about the implementation of loop components in Teams.

Control over the use of loop components for Teams and OneNote is through settings in the SharePoint Online tenant configuration:

- ***IsLoopEnabled*** controls the availability of Loop components in Teams.
- ***IsCollabMeetingNotesFluidEnabled*** controls if Fluid components are available in OneNote collaborative meeting notes.

You can update the settings with the `Set-SPOTenant` cmdlet. For example:

```
Set-SPOTenant -IsLoopEnabled $True
```

To disable Loop access using either setting, update the setting to `$False`.

Two methods are available to control user access to the Loop app and loop components in Microsoft 365 apps other than Teams:

1. Enable access to Microsoft Loop through the Org Settings section of the Microsoft 365 admin center. To create new Loop workspaces, user accounts must have the Microsoft Loop service plan (identifier `c4b8c31a-fb44-4c65-9837-a21f55fcabda`). The plan is included in the Microsoft 365 E3 and E5 product SKUs for enterprise organizations and the Microsoft 365 Business Standard and Premium SKUs for small to medium enterprises.
2. Use a [Cloud Policy](#) to allow access for selected user accounts defined in a group. See [this page for more information](#) about updating items in the Cloud Policy service through the Microsoft 365 apps admin center.

Loop workspaces and pages do not currently support full eDiscovery functionality. Components are discoverable, but an issue exists with offline access to components found by eDiscovery searches. Due to these shortcomings, some organizations have restricted access to Loop technology. Microsoft is working on an offline access capability to allow investigators to view loop data recovered by searches, but this is not yet available.

Users can create any number of Loop workspaces in a tenant. The space used by the workspaces counts against the tenant's SharePoint storage. To enumerate the Loop workspaces in the tenant, run:

```
Get-SPOContainer -OwningApplicationID a187e399-0c36-4b98-8f04-1edc167a0996 | Format-Table
```

The value of *OwningApplicationID* for the Loop app is always `a187e399-0c36-4b98-8f04-1edc167a0996`. For every Loop workspace, the command returns the following columns: *ContainerId*, *ContainerName*, *CreatedOn*, and *Status*. To get detailed information (including the storage consumed) for a specific Loop workspace, run:

```
Get-SPOContainer -OwningApplicationID a187e399-0c36-4b98-8f04-1edc167a0996 -Identity <ContainerID>
```

Where *Identity* is either the value of the *ContainerId* column of a Loop workspace obtained with *Get-SPOContainer* or its Site URL. [This article](#) explains how to create a report of the storage used by Loop workspaces together with the licensing status for user accounts.

Migrating to SharePoint Online and OneDrive for Business

A very common need from any organization that is on Microsoft 365 or thinking to start the Microsoft 365 journey is the migration of corporate assets (On-Premises and/or in other cloud services) to SharePoint Online and ODFB.

Moving Windows File Servers to SharePoint

Moving individual files from a network file share to a SharePoint document library, perhaps one connected to a group or team can be a tiresome process. People often use the OneDrive sync client to move files between different libraries, and you can use it to move files from network shares too. Here's how:

- Synchronize the target SharePoint document library to a workstation with the OneDrive sync client.
- Map the source network file share on the workstation.
- Use File Explorer to copy files from the source network share to the folder holding the synchronized content from the SharePoint document library.
- The OneDrive sync client will then synchronize the copied files to the document library.

This is an effective approach when you have a few hundred files to move. Things become more complicated when you have more files to process. At this point you can consider:

- Run a PowerShell script to move files. Microsoft's SharePoint PowerShell module does not have cmdlets to directly copy files to SharePoint Online or OneDrive, but it provides cmdlets to migrate on-

premises contents by creating a migration package that can be submitted to be [imported by the Office 365 Import Service](#).

- The SharePoint [Patterns and Practice \(PnP\) module](#) includes cmdlets to copy contents to a SharePoint document library. Here is [an example of a script that uses the PnP module](#) to copy files from a network file share to a SharePoint document library.
- Use Microsoft's free SharePoint migration tool (see the section later).
- Use the Migration manager.
- Use a commercial third-party product. These products vary in terms of capability and cost, so some testing is necessary to figure out which best suits your circumstances.

SharePoint Migration Tools

Microsoft's free [SharePoint Migration Tool](#) can move files from on-premises SharePoint Server (2010, 2013, 2016, and 2019) sites, file servers, and [Azure file shares](#) to SharePoint Online sites. The tool also supports migration to OneDrive for Business. The sole requirements are that the tool must be able to read data from the sources and write to the target sites. After checking that access is available, the tool extracts documents from the source and creates a set of XML manifests and content. The tool then uploads the content package to a secure location in Azure and invokes a migration job in SharePoint Online to fetch the content and import it into the target locations. [Version 4 of the toolset](#) includes features such as:

- [Scan SharePoint server](#) to identify issues that might happen in a migration and help to plan migration tasks.
- Simplified management of migrations or scans through search and filters to locate specific tasks, view the can/migration progress, and/or start, stop, delete, and edit migrations from the buttons on the toolbar.
- Select SharePoint Online Sites, ODFB, or Teams in Microsoft Teams as possible destinations for a given migration.
- For SharePoint Server to SharePoint Online migrations, choose to migrate the site structure as it is in the source (if using a classic information architecture) or promote all the subsites to site collections and associate them with a hub site.
- Create the destination site for a migration in case it does not exist.
- JSON and CSV support for use in bulk migrations.
- [Migrate full SharePoint sites](#) including some site features (those included in [this list](#)), some Web Parts (those included in [this list](#)), Pages, Site Description, Site Icons, Site Navigation, Content Types, and existing taxonomies defined in the Manage Metadata Term Store.
- Migrate SharePoint lists created using a [list template supported by the tool](#).
- Migrate SharePoint Server 2010 out of the box list workflows, including Approval and Collect feedback workflows, to Power Automate Flows.
- [Migrate SharePoint Server 2010 and 2013 designer workflows](#) to Power Automate Flows.
- SharePoint Server subfolder selection.
- Document sets and document templates.
- Select Teams and channels directly from the destination selection page.
- Ability to create sites during file share migration.
- Support for migrating SharePoint on-premises Record libraries.
- Support for migrating basic SharePoint on-premises settings such as site logo, title, description, and some other general settings.
- Support for migrating files up to 250 GB.
- Provide feedback to Microsoft from the tool.

See the SharePoint Migration Tool [release notes](#) for more information about the SharePoint Migration Tool.

PowerShell support for the SharePoint Migration Tool: There are [eight PowerShell cmdlets](#)

documented to automate migrations to SharePoint Online using the SharePoint Migration Tool. A sample migration script showing how to use the cmdlets can also be found in the cmdlet documentation

Migration utilities typically work on the basis that they move documents and metadata from a source to a target destination (a SharePoint Online site). Inevitably, some documents end up in the wrong place and need repositioning to the correct destination afterward. Until Microsoft upgraded SharePoint's "Move to" feature to allow the movement of files to a different site, rearranging documents post-migration was difficult and time consuming. Now, you can move documents to any folder in a SharePoint Online or OneDrive for Business site to which you have write access. Moving is different from copying because a move includes all the versions of a file instead of just the final version. In addition, a move preserves metadata between source and target destinations by matching column names (if a column name does not exist for the target, the move drops that metadata). Moves also respect compliance policies.

You cannot beat the zero-cost price point for the Microsoft migration tool. However, the tool offers a limited feature set and if you have more complex requirements to move documents, schema changes, metadata, and customizations, you might need a more sophisticated approach to migration such as those available from Quest, AvePoint, or Sharegate. All SharePoint migration utilities use the same APIs and are subject to being throttled. Third-party migration products usually have their own ways to increase throughout or minimize throttling to move data to SharePoint Online more quickly, and this might be a factor in your planning if you have large quantities of data to move. See [this page](#) for more information about likely throughput for SharePoint and OneDrive for Business migrations.

You should decide early on what migration tool to use for your project. Making that choice can take a lot of effort to analyze, test, assess, and eventually decide. Do not underestimate the importance of this work.

On-Premises Inventory/Audit: Before starting a migration to SharePoint Online, it's advisable to make an inventory/review of the contents and structures to be migrated so any issue that surfaces during the migration is found beforehand. Microsoft's [SharePoint Migration Assessment Tool](#) (SMAT) helps identify the impact of migrating from SharePoint 2010/2013/2016 to SharePoint Online. As reflected in Microsoft's documentation, SMAT also includes [support for the identity migration](#) from SharePoint On-Premises to SharePoint Online. Of course, as with the SharePoint Migration Tool, there are also commercial inventory tools that give more detailed information about a SharePoint Farm and issues that can arise when starting a migration project.

Migration Manager

[Migration manager](#) includes a set of migration tools designed to simplify complex migrations where it is necessary to create migration tasks on several migration machines and orchestrate the tasks to a successful conclusion. Migration Manager is integrated into the SharePoint admin center. For the migration of file shares, the process managed by the Migration manager has four steps:

- Install the Migration manager agent in each server from where information is to be migrated to SharePoint Online sites.
- [Scan and assess the file shares](#): The Migration manager performs this step automatically after a data source is added to the service. The scans provide an overview of the contents to be migrated in terms of size, the number of files, or issues that might affect the migration. Scan log files are also available for download to enable deep analysis and troubleshooting on individual files identified.
- Create and configure migration tasks by typing the path of the file share to be migrated and the destination location (a OneDrive for Business site, a Microsoft Teams team, or a SharePoint site).
- Monitor how migration is progressing across the different clients and access reports generated automatically by the Migration manager.

Migration Manager currently supports the migration of contents from file shares, [Box](#), [Google Workspace](#), [DropBox](#), and [Egnyte](#) to SharePoint Online and/or OneDrive for Business. Migration Manager includes the [Migration Time Estimator](#) to provide an estimated duration of migration before it starts. This tool can be used for Google Drive, Dropbox, Box, and Egnyte migrations.

Cross-tenant SharePoint Migration

This feature (available in preview for Enterprise Agreement customers) allows administrators to [move SharePoint Sites from one tenant to another](#) using SharePoint Online PowerShell. The following types of sites can be migrated between tenants:

- Microsoft 365 group-connected sites, including those sites associated with Microsoft Teams
- Modern sites not connected to a Microsoft 365 group.
- Classic SharePoint sites.
- Communication sites.

Cross-tenant SharePoint migration migrates contents, sharing links, and permissions. However, it does not migrate any app or artifact connected to the source site such as Power Apps, or Power Automate Flows. Those apps and artifacts must be re-created and re-connected.

Microsoft Lists

Microsoft Lists is an app that allows end users to create custom lists using a dedicated space hosted in OneDrive for Business (personal lists) or shared lists stored in a SharePoint Online site. A [lightweight version of Microsoft Lists](#) (currently in preview) is also available for small businesses and individuals who don't have Microsoft 365 but regularly use Microsoft Accounts (MSA).

Users can install the Microsoft Lists app as a Progressive Web App in Microsoft Edge, Google Chrome, or Firefox. A Microsoft List is a modern version of a traditional SharePoint list created from scratch or by using one of fourteen out of the box templates (including Issue tracker, Employee onboarding, and Event itinerary). Users can also create lists from an existing list, a CSV file, or from an Excel worksheet in their OneDrive for Business account or from lists in SharePoint sites the user can access. Microsoft Lists incorporate features such as:

- Add new list views to display data in different formats (List, Calendar, Gallery, Board). Depending on the list view type, users can choose more than one layout to display list information. As an example, the calendar view provides a month layout, a week layout, a work week layout, and a day layout.
- Modify a list view by hiding, adding, deleting, moving list columns, or applying filters that are displayed as pills on top of the list actions bar.
- Quickly switch between views in the list using the tabs available in the Lists UI.
- Group list items or filter list items by using the Group by and Filter actions.
- Apply rich formatting at different levels in a List without writing a line of code through column formatting, view formatting, and Forms customization. Additionally, list forms can be customized with Power Apps or the Lists Forms layout designer.
- Create simple business rules to notify when a change in a list record happens (a column changes, a column value changes to something, the creation or deletion of an item, and so on). The integration of Power Automate enables the creation of more sophisticated business processes tied to a list. Business rules are supported in Microsoft Lists and regular Document libraries.
- Export list content to an Excel worksheet, a CSV file, a CSV file with schema (Note: This option keeps custom formatting, choice pills, rich text-based editing, and people data, so source and destination lists will look identical), or a Power BI dataset.
- Mention someone in a list comment by using "@".

- Ability to easily share a personal list created by the user in OneDrive for Business with other users.
- [Create a Power BI report from list data with a single click](#). This feature requires either a Microsoft 365 E5 or a Power BI Pro license.
- Work offline with list data synchronized locally using the [Project Nucleus technology](#) enabled for users through the Nucleus service plan included in all Microsoft 365 SKUs. Synchronization is on by default for eligible lists as explained in [this support article](#). Administrators can manage the sync settings for Lists through [a specific group policy](#).
- Install pre-created Power Automate flows after creating a list. This option is available for the following default list templates: Work progress tracker, Content scheduler, and Recruitment tracker. Additionally, custom list templates created in a tenant can [include Power Automate flows](#) configured in the source lists.
- Integration with the Microsoft Teams approvals app to submit a list item for approval by creating an approval request. Approvers can process the request in both the list and the Approvals app. This integration is available on any list including custom lists.
- Create a custom form to collect data from List owners and collaborators with edit permissions. Custom forms can be created with the form builder using the fields from the list schema for data collection. A form creator can add fields, show/hide fields, change the form theme, and share the form with a link.

Lists are accessed through the Lists app (which presents both personal and shared lists), the SharePoint App Bar, the Site contents page in a SharePoint site, the Lists app in Teams, or through the mobile Lists App available for iOS and Android. A Global or SharePoint admin can control the following [Microsoft Lists settings](#):

- Disable the creation of personal lists by running the `Set-SPOTenant` cmdlet to set the `DisablePersonalListCreation` property to `$True`. This setting stops users from creating personal lists in OneDrive for Business.
- Disable built-in list templates that are not relevant to an organization by running the `Set-SPOTenant` cmdlet to populate the `DisableModernListTemplateIds` with the set of disabled templates. For example, to hide the Issue tracker list, run the following command:

```
Set-SPOTenant -DisableModernListTemplateIds 'C147E310-FFB3-0CDF-B9A3-F427EE0FF1CE'
```

To re-enable a built-in list template, write its GUID into the `EnableModernListTemplateIds` property.

- Disable list comments in any Microsoft Lists list by running the `Set-SPOTenant` cmdlet to set the `-CommentsOnListItemsDisabled` property to `$True`. Note that list comments can be disabled per list through the list settings page.

Custom List Templates

In addition to the default set of list templates available for Microsoft Lists, a SharePoint administrator can add custom list templates using the following steps:

- Extract the site script from the desired list using the `Set-SPOSiteScriptFromList` cmdlet.
- Run the `Add-SPOSiteScript` cmdlet to add the site script extracted to the list of available site scripts in the tenant.
- Run the `Add-SPOListDesign` cmdlet to add the custom list template to the organization lists catalog.
- (Optional) Run the `Grant-SPOSiteDesignRights` cmdlet to indicate who can see and use the custom list template.

The following script is an example of the process:

```
$SPOListURL="https://Office365itpros.sharepoint.com/Lists/Projects"
$SPOSiteScriptFromList=Get-SPOSiteScriptFromList -ListUrl $SPOListURL
```

```
Add-SPOSiteScript -Title "Corporate Projects" -Description "List that contains Corporate Projects"  
-Content $SPOSiteScriptFromList  
Add-SPOListDesign -Title "CompanyDevices" -SiteScripts fcbd3f82-28bb-4de0-b9bb-3e0cb6e6125e
```

After the script runs, users see the new custom template in the *From your organization* tab in the *Create a list* dialog. To remove a custom list template, run the *Remove-SPOListDesign* cmdlet. To grant permissions on a custom list to specific people in the organization, administrators can run the [Grant-SPOSiteDesignRights](#) cmdlet to pass the identifier for the custom template and the list of people allowed to view the template. In addition to creating custom list templates, the same cmdlets can be used to create and manage custom document library templates.

Formatting of Columns, List Views, and List Forms

Document library and list columns are customizable with JSON or by using the Format column designer through the “Format this column” setting available for any column in modern lists and document libraries:

- Advanced mode formatting allows site designers to change the column look and feel with JSON code in different ways, as described in [this How-To article](#).
- Format column designer allows non-developers to add conditional color coding to SharePoint columns, apply color and rounded styling for each choice (Choice pills template), and Data Bars for numeric columns without needing to create JSON scripts. The Format column designer also supports defining rules to apply a color to the column.

Similarly, designers can customize list views with JSON code and/or use the Format view designer to:

- [Apply alternating row styles to the list without writing any JSON code](#). The Format view designer also supports rules creation to define the conditions to apply alternating row styles on lists and document libraries. Column and List View formatting is also supported in the [new enhanced quick edit view](#) in SharePoint lists and document libraries.
- Visually configure the fields to be displayed in cards and their order in views created with the Gallery or Board layouts. A developer can use the [Gallery/Board](#) formatter to define custom card layouts or field values inside a card using the same JSON syntax used for column formatting.
- [Customize the list command bar](#): modify basic aspects (icon and/or text), hide and/or reposition existing options.

It's also possible to customize List forms with JSON code. The following areas in a List form can be currently customized with JSON: List form header, body, and footer.

Microsoft Search

Microsoft Search is available throughout Microsoft 365 to perform searches in clients like OWA, OneDrive for Business, SharePoint Online, and Teams. Microsoft Search is designed to only show results relevant to the user who performs the search. Results are security trimmed, meaning that each user can only see results for documents and other objects that he/she can access. Microsoft Search does not change permissions.

Connecting Microsoft Search to services like SharePoint Online sites, OneDrive for Business, Exchange Online, and Teams means that Bing can include content from these services in its searches. This capability known as [Microsoft Search for Bing](#) is another way to expose content stored in SharePoint Online, OneDrive for Business, and Teams to users.

Microsoft Search is enabled by default in Microsoft 365. No setup is necessary, but, as described here, it's possible to streamline and improve the overall Microsoft Search experience for users. [Management of Microsoft Search settings is through the Search and Intelligence section](#) under Settings in the Microsoft 365 admin center.

The first task is to verify that **Microsoft Search in Bing** is enabled for the tenant through the Configurations tab. You can then configure settings such as Acronyms, Bookmarks, Locations, and Q&A to improve the findability of content. See [this page](#) for more information.

The screenshot shows the Microsoft Bing search interface. At the top, there's a header bar with the Microsoft Bing logo, a back button labeled 'BACK TO WEB SEARCH', and a user profile for 'Tony.Redmo...' with 2885 notifications. Below the header is a red search bar containing the query 'Office 365 for IT Pros'. To the right of the search bar is a magnifying glass icon. On the left side of the main search area, there's a sidebar with a navigation menu. The 'Messages' option is highlighted in grey. Other options in the menu include All, People, Sites, Files, Images, Videos, Power BI, Learning, and Send feedback. The main search results area has a red header bar with the same search query. It displays several search results, each with a small profile picture, the title of the result, and a timestamp. One result is expanded to show a detailed view. This expanded view includes a sidebar with filter options: 'Filters' (set to 'Type (1)'), 'Date' (set to 'Today'), and a dropdown menu for 'Team' which is currently set to 'Teams' (with a checked checkbox). Below this is a list of messages from 'Gareth Gudger (Office 365 for IT Pros) in chat' dated August 29, 2022. The messages are: 'for IT Pros) in chat 2 days ago', 'Office 365 > 2023 Edition (9th)', and 'Teams • Conversation in Office 365 for IT Pros 2024 Edition Editorial Call ...'. The last message is partially cut off. Below these messages is another section titled 'Gareth Gudger (Office 365 for IT Pros) in chat' with the date 'August 29, 2022', followed by the message 'Teams • Conversation with you'. The bottom of the expanded view shows a snippet of the message content: 'Or can I just heavily steal from this page? Why You should buy the world's best Office 365 book - Office 365 for IT Pros (office365itpros.com)<https://office365itpros.com/how-to-buy-office-365-...'. The rest of the message is cut off.

Figure 7-4: Integrating Microsoft 365 sources into Bing search results

Behind the scenes, the services connect to Microsoft Search in Bing (this process might take up to 24 hours to complete), and users see a **Work** link in the result bar to expose results from the organization when they use Bing.com to search or configure Bing as the default search engine for their browser. Clicking the link shows results from the connected sources (Figure 7-4), divided into the following sections:

- **People:** People in the tenant's directory.
- **Sites:** SharePoint sites in the tenant matching the search term.
- **Files:** Documents found in SharePoint and OneDrive for Business libraries accessible to the user.
- **Messages:** [Messages from Teams chats and channel conversations and Outlook](#) (Exchange Online).
Users can only search their mailboxes. They won't find items in shared mailboxes or other user mailboxes they have delegated rights to.
- **Images:** Images files stored in SharePoint sites and OneDrive locations the user can access.
- **Videos:** Video files stored in SharePoint sites and OneDrive locations the user can access.
- **Power BI:** Datasheets and other Power BI components matching the search.
- **Learning:** Content from both the organization and learning partners such as LinkedIn Learning.
- Any custom vertical configured by an Admin.

Brief snippets appear for the most relevant hits in each category. Links are available to bring the user to the underlying applications to view content or perform more exhaustive searches. Users only see information that they can access, and Bing filters the results based on the permissions held by that user.

Integrating Microsoft 365 sources with Bing is only useful if people use Bing as their preferred search engine and is useless when they use other search engines like Google or DuckDuckGo. However, if your corporate standard is Bing, integrating Microsoft 365 workloads into Bing search results is a surprisingly useful and worthwhile extension.

Note that SharePoint search and the search feature in Office.com also present results drawn from across Microsoft 365 like conversations from Teams and Outlook.

Administrator Roles for Microsoft Search

There are two specific Admin roles to manage Microsoft Search in Microsoft 365:

- **Search admin:** This role can manage all the settings configurable for Microsoft Search administration including creating and managing search result content, defining query settings, and all the content management enabled by the Search editor role.
- **Search editor:** Create, manage, and delete editorial content in Microsoft Search such as frequently asked questions and answers or important places and locations.

Microsoft Search Home page

The [Microsoft Search Home page](#) provides a high level overview and insights about how end users make searches across Microsoft 365, the status of the connectors and connections in use showing not only the status, but also the presence of issues and errors or the status of the answers (Acronyms, Bookmarks, Locations, Q&As, and topics) configured for the service.

Acronyms

To help users find terms that might have multiple references within an organization's terminology, Microsoft Search has Acronyms. An Acronym is a type of searchable term supported by Bing, Microsoft 365, and SharePoint. To get answers to an Acronym search, users must enter a specific search pattern in the Search box. For instance, if users are looking for the term DLP (Data Loss Prevention), they should use queries such as *What is DLP, Define DLP or DLP means*.

There are two types of Acronyms in Microsoft Search:

- **Admin-curated acronyms:** created by users with the Search admin role in the Microsoft Search administration.
- **System-curated acronyms:** mined by Microsoft Search from user's personal email and documents and publicly available data within the organization. Bear in mind that mined acronyms from new emails and documents can take up to 7 days to appear in Microsoft Search results.

Acronyms can be added to Microsoft Search in two ways:

- **Manually:** Acronyms are created by Search administrators and defined by the following fields: Acronym (mandatory, stands for (mandatory, spelled out abbreviation), Description (a brief description of the acronym), and Source (URL of the page or website where the users should go for more information about the acronym). Once an acronym is saved, it must be published before it can be used in Microsoft Search.
- **Automatically:** Import a CSV file that contains all the Acronyms to be added to Microsoft Search.

Bookmarks

Bookmarks are a way to provide shortcuts to popular internal or external resources in an organization or corporate applications used to complete tasks such as entering vacation time or reporting expenses.

Microsoft Search includes some predefined Bookmarks and additional Bookmarks can be manually added or imported in bulk through a CSV file or from SharePoint Promoted results from sites.

A Bookmark is defined by the following elements: Title (mandatory), URL (mandatory, URL to an internal website or page), Bookmark description, Keywords (mandatory, search terms commonly used to find the Bookmark), Reserved keywords, and Categories (to organize and group Bookmarks). A Bookmark can have several keywords and several bookmarks can share the same keyword. Some optional Bookmark settings can be configured such as the Dates when the result is going to be available, countries where it's going to be available, or the Groups (Security groups or Microsoft 365 Groups) that can use the Bookmark.

Existing and new Bookmarks can be edited when required. If a Bookmark is not ready to use yet, it can be saved as a draft before being published. Several Bookmarks can be imported/edited in bulk by using the Import action.

To simplify the process of creating and curating Bookmarks, Microsoft Search generates [recommended Bookmarks](#) by scanning content across SharePoint sites to identify potential bookmarks. A recommended bookmark includes the following mined information: URL, Title, Description, and Keywords. Administrators make the final decision to publish or reject the recommended bookmarks.

Locations

To find addresses and locate the organization's buildings, Microsoft Search includes Locations. A Location has the following attributes: Name (mandatory), Country or region (mandatory), Address, Keywords (mandatory), and Reserved keywords. Locations can be added individually or imported in bulk using the import feature. After adding or updating locations, it can take several hours for the new data to appear in search results.

Q&As

Q&As enable [rich-text answers to user questions](#) instead of just providing links to web pages. As in the case of Bookmarks, once a Q&A is added or changed, it's immediately available for users. In case a Q&A and Bookmark share the same keyword, the Bookmark result appears first.

To manually create a Q&A, navigate to the Q&A section in the Microsoft Search administration section and select Add. In the Add Q&A panel, you need to add the following properties:

- Title (mandatory).
- URL (URL to an internal website or page).
- Answer description (mandatory), a brief description of the answer. You can apply some formatting to the description using a rich text toolbar or using existing HTML content,
- Keywords (mandatory, search terms commonly used for the Q&A).
- Reserved keywords.

A Q&A can have several keywords and several Q&As can share the same keyword. Finally, as happens with Bookmarks, some optional Q&A settings can be configured such as the Dates when the result will be available, countries where it's going to be available, or the Groups (Security groups or Microsoft 365 Groups) that can use the Q&A and targeted variations to provide different Q&A messages based on the user's device and location.

Existing and new Q&As can be edited when required. If a Q&A is not ready to use yet, it can be saved as a draft before being published. Several Q&As can be imported/edited in bulk by using the Import action.

Microsoft Search Usage Insights

[Usage reports](#) covering Microsoft search requests over the last 7, 14, 31 days, or 12 months are available to search administrators to help them understand how end users look for content across Microsoft 365 and

specifically in SharePoint Online using out of the box search boxes. Microsoft Search Usage Reports also help identify possible issues faced by end users when they search Microsoft 365 sources. The following reports are currently available:

- **User Analytics:** Displays information on how people are using search in the organization in terms of people who perform at least one search (Users Who Searched), people searching in two consecutive weeks (Users Who Searched Weekly), and people who performed no searches (Users Not Searching). This report allows administrators to compare user engagement in terms of the number of days users performed searches and the distribution of search users per application.
- **Query Analytics:** Shows different charts of the search activity (total queries) by user action, country, occupation, and department or division. The “View queries analytics” button in this section displays a query details page to view and analyze in detail the following top search queries: Most popular search terms, Top 10-no result queries, and Top 10 abandoned search terms.
- **Answers Analytics:** Gives information and insights about the performance of editorial answers configured such as Bookmarks, Acronyms, and Q&A within the organization. The reports include editorial answer impressions, bookmark answer clicks, average click rate for bookmarks, average impressions for Acronyms and Q&A in addition to individual item level impressions, query term analytics for bookmarks, acronyms, and Q&A.
- **Connection Analytics:** Provides an analysis of queries with search results from the connections in the tenant. The connection analytics details page displays and analyzes connection data in more detail.

At the Site level, Site Admins can access [the following search reports](#):

- **Query volume trend graph:** Displays the total number of search queries over the selected time frame. This report includes query volume trends and periods of high and low search activity.
- **Impressions by result type:** provides insights about the number of results by type.
- **Top queries:** Displays the most commonly used search queries. This information helps administrators to understand the types of information users search for.
- **No results queries:** Shows searches that return no results.
- **Abandoned queries:** Shows popular searches where users do not click on the results or the results have a low number of click throughs. This might indicate that the search results do not include information users consider useful or interesting.

Over time, those reports will replace some of the search usage reports available in the SharePoint Online search service.

Customizing the Microsoft Search User Experience

The [user experience in Microsoft Search can be customized](#) in the following ways:

- **Modify existing verticals and create new verticals** to show results of a certain type or from certain content. There are nine default Search verticals that tenants can modify: All, People, Files, Sites, News, Images, Power BI, Messages, and Videos. Note that the [Messages](#) and Viva Learning Search verticals cannot be modified. To create a new vertical, you must provide a name, a valid content source, optionally a KeyQL (Keyword Query Language) query against the content source and optionally custom filters. Note that a connector to a data source must be created and the content indexed (it can take up to 48 hours to index a Connector) before it is effective. Custom filters, which are based on search managed properties, can be added to new and existing verticals. Custom Search verticals are visible to users when they search in Microsoft Office Home, SharePoint at different levels (SharePoint Home page or Sites), and Bing. Once you add a new Search vertical to Microsoft Search, it might take some time before users can view it.

- **Add new Result types** from content sources and customize the layout for the data indexed using result layouts designed with the [Search Layout Designer](#). A Result type allows search results to be displayed in different ways through one or more conditions and result layouts to use for search results that meet the conditions defined. To display results on a Search vertical, at least one Result Type must be created. A Search vertical can have multiple Result types to distinguish different types of search results. For example, you could have a Search vertical to display ServiceNow support tickets and use different visualizations depending on the severity of the support case opened by end users. To create a new Result type, you must provide a name, a content source to be used to render search results, the rules (this is an optional setting) to distinguish search results depending on the conditions met, and a results layout to display the search results.
- **Create custom result layouts** to [customize search results](#) using the Search Layout Designer. A result layout can be created from scratch or any of the existing layouts provided in the tool. Once the layout is ready, the JSON definition must be exported for use in the Result type creation process. Creating custom result layouts requires knowledge of adaptive cards and their schema.
- **Modify existing filters and create custom filters** to refine the results of the queries made by users and display refined results. There are some default filters in default search verticals that can be customized. Custom filters based on refinable managed properties can be added to search verticals at the organization and site level.

If your organization uses Microsoft 365 Copilot, you might want to exclude the information held in certain sites or document libraries from being found by Copilot. When Copilot searches for information, it can only find content available to the signed-in user. To exclude complete sites, go to the Search and Offline availability section of site settings and set the *Allow this site to appear in search results* button to Off.

To stop Copilot from using information stored in a document library, choose the advanced settings under site settings, and set the *Allow items from this document library to appear in search results* button to Off.

Microsoft Graph Connectors

[Microsoft Graph Connectors](#) support the indexing of third-party data hosted on-premises or in public/private clouds to integrate data into Microsoft Search results. Currently, there are thirteen default Connectors available for Microsoft Search: Azure DevOps, Custom connector, JIRA, ADLS Gen2, Oracle SQL database, ServiceNow, CSV, File share, Microsoft SQL Server, MediaWiki, Salesforce, Confluence, and Azure SQL. Organizations can [create custom connectors and add them to Microsoft Search](#). A [Microsoft Graph connectors gallery](#) is available with more than 100 connectors created by Microsoft partners.

Before creating Search verticals and Results, a Connector to a supported data source must first be created. The creation of a Connector follows a step-by-step process that depends on the data source. For instance, to create a Connector to index data for a website, input the following settings:

- **Name:** the connection by providing a connection name, ID, and Description. In this step, you must acknowledge that Microsoft will index data from the data source in the Microsoft 365 tenant.
- **Connection settings:** URL of the website to be indexed, the authentication type to be used (None, Basic), and the credentials (if required) to connect the website. The URL indicated in this step is the URL that initiates the crawl and is used for authentication.
- **Add URLs to exclude:** this is an optional step that allows admins to exclude URLs from search results.
- **Schema:** Defines the schema for the results that will be indexed. In this step, a list of the source properties indexed is shown. For each property, at least one of the following attributes must be set: Queryable, Searchable, Retrievable.
- **Manage search permissions:** For this data source there is no support for ACLs (Access Control Lists), so any user in the organization will be able to make searches against it.

- **Refresh settings:** It allows to indicate the refresh schedule interval for content crawling. This data source only supports full crawls.

Once a Connector is configured, it can be saved in a Draft state or published for use in Search verticals and Result types. Bear in mind that you must wait for some time until the connector starts indexing contents.

Microsoft Search in SharePoint Online and OneDrive for Business

Microsoft Search is integrated with Microsoft 365 and all its core workloads, including SharePoint Online and OneDrive for Business. For SharePoint Online, the integration is available in two ways:

- The search box added to the Microsoft 365 top navigation bar to collect search queries that lead to results tailored for the signed-in user:
 - When the user clicks on the search box, Microsoft Search lists the last applications, files, contacts, and news the user interacted with.
 - As soon as the user types a search term, Microsoft Search immediately suggests search results that meet the search criteria.
 - If the search results returned are not the ones expected by the user, he/she can always expand the results and be redirected to the search results page.
- A dedicated Microsoft Search settings page is available through the Site settings page on a given site. Here a site admin can:
 - Create custom result types based on any of the Search connectors configured in Microsoft Search administration.
 - Create custom verticals to display search results coming from the custom result types configured in the tenant.

Limitations when configuring Microsoft Search in a Site: Some limitations currently exist when Microsoft Search is configured for a specific site such as the inability to modify a custom result type or a search vertical once they are created.

For OneDrive for Business, users can search Files and Folders not only in OneDrive but also in any shared library they can access across the tenant. The search box in OneDrive for Business includes a dropdown to allow users to choose where they want to search.

Restricted SharePoint Search

[Restricted SharePoint Search](#) allows organizations to restrict Enterprise Search to a curated set of sites (up to 100) without affecting how users in the organization interact with files and content they own. The intention is to stop Microsoft 365 Copilot finding and using sensitive or unapproved information in its responses to user prompts. Restricted SharePoint search is available in tenants with a Microsoft 365 Copilot license and is off by default. Applying the restriction only limits the results visible to users. It does not affect the consumption of search results by Microsoft Purview solutions like eDiscovery and DLP.

How Microsoft Viva and Microsoft Syntex Bring AI to SharePoint

Under the umbrella of Microsoft Syntex, Microsoft provides a [set of AI Services](#) in SharePoint Online to recognize content types, capture content, extract information, automatically classify content employing image and text recognition, or perform forms processing. Machine teaching uses AI models to recognize information in unstructured documents such as contracts, proposals, or training materials. Microsoft Syntex also adds SharePoint advanced management features such as Site lifecycle management and Restricted Access Controls (RBAC) for OneDrive for Business and OneDrive.

Microsoft Syntex is becoming SharePoint Premium: Microsoft is renaming Syntex to SharePoint Premium. SharePoint Premium includes current Microsoft Syntex AI features as well as the governance features that are part of the SharePoint Advanced Management Add-On.

Microsoft Syntex

[Microsoft Syntex](#) is available as an add-on for Office 365 and Microsoft 365 plans. Microsoft Syntex uses machine teaching and AI Models integrated into the platform to automatically capture, recognize, and extract key information to ensure that uploaded documents are properly stored and classified in SharePoint document libraries. If configured in the AI Models, Syntex can [apply retention labels](#) or [sensitivity labels](#) automatically to the documents processed.

Among the Microsoft Syntex capabilities are:

- [Prebuilt models options for contracts, invoices, receipts, and sensitive information:](#) Contracts, receipts and sensitive models can be configured to detect and extract a set of standard fields present in these file types. Sensitive information model detects and optionally extracts sensitive information from files created or uploaded to Document libraries where the model has been published. These prebuilt models can be published globally (tenant-level) or locally (site level) so they can be discovered and used by end users.
- [Local Models Creation:](#) Users can create and train unstructured document processing models in sites outside of a Content Center site. Syntex can then apply the models to libraries from those sites.
- [Form processing](#) (structured document processing): Uses Power Platform AI Builder form processing to create AI models that use machine learning technology to identify and extract key-value pairs and table data from structured or semi-structured documents, such as forms and invoices.
- [Unstructured and freeform document processing models:](#) Uses Power Platform AI Builder to automatically extract information from unstructured and freeform documents such as letters or contracts.
- [Content assembly:](#) Supports the conversion of a Word document into a template by defining placeholders in the document for dynamic text. This template can be used later to generate new documents by filling values in the placeholders either manually or selecting data from a SharePoint list.
- Two specific Microsoft Syntex site template accelerators: Content center site template and [Contract management](#) accelerator.
- [Model Usage Analytics:](#) Provides the following insights about how Microsoft Syntex published models are being used:
 - Identify models with more classified files.
 - Determine which models are more efficient in classifying files.
 - Usage analytics for each model.
- [Automation scenarios through new Power Automate integrations](#) powered by specific Microsoft Syntex triggers and actions. An example of these scenarios is the automatic creation of documents from Syntex content assembly.
- [Annotations:](#) Allows Syntex licensed users to highlight, circle, and underline content in PDF and TIFF files without modifying the underlying files.
- [Image tagging:](#) Automatically tags images stored on SharePoint libraries with descriptive keywords. These keywords are in a managed metadata column for the item that is searchable, sortable, or filterable. Microsoft offers Image tagging through the Syntex Pay-as-you-go offering. Image tagging is disabled by default in the tenant. It can be enabled in all the sites or a specific set of sites (up to 100) manually selected or uploaded in a CSV file.

- [Taxonomy tagging](#): Uses AI to automatically tag documents stored in SharePoint document libraries with terms created and configured in the Term store. To use the Taxonomy tagger, the following prerequisites are required:
 - If not already enabled for the tenant, set up Syntex Pay-as-you-go in the Microsoft 365 Admin Center.
 - Add a managed metadata column on each document library where the Taxonomy tagger is going to be used and turn on the tagger control Create column panel. If a managed metadata column already exists in a given document library, then enable the Taxonomy tagger by turning on the toggle in the Edit column settings for the column.
- [Microsoft Syntex OCR](#): Extracts text from images stored in SharePoint sites and OneDrive. After text is extracted, it is available for end-user search. Syntex OCR is charged on a pay-per-use basis through the Syntex Pay-as-you-go program.
- [Merge and extract PDFs](#): Allows to merge two or more PDF files into a new PDF file, or to extract pages from a PDF file to make new individual PDF files.
- [Document translation](#): Allows users to [translate a selected file or set of documents on-demand](#) or through a library rule. The translation process preserves the original format and structure of the translated files. Document translation is licensed through the Syntex Pay-as-you-go offering.
- [Autofill columns](#): Populates properties in document libraries by using AI to extract information from uploaded files.

To evaluate Microsoft Syntex without the need to acquire licenses or even start a trial, Microsoft provides a content center site template to evaluate how unstructured document processing models are created, trained, and managed. Models created in the center can be trained to classify content and extract information but cannot be applied in a document library to run against uploaded files. To get advice on where Microsoft Syntex might fit in an organization, Microsoft offers a [Microsoft Syntex Assessment](#) service. The output is a Power BI report with recommendations based on factors such as the size and structure of libraries, existing use of metadata or content types, and use of retention labels. Microsoft Syntex Assessment is included in the [Microsoft 365 Assessment Tool](#).

Microsoft Syntex Pay-as-you-go: As an addition to the content center site template, organizations can evaluate the potential of unstructured document processing and prebuilt document processing features by configuring Microsoft Syntex for Pay-as-you-go billing model. Over the time, Microsoft will add additional features under this model. Pay-as-You-Go licensing includes also [access to the following additional Microsoft Syntex features for a limited period of time as a preview](#): Content query, Universal annotations, Contracts management accelerator, Accounts payable accelerator, Taxonomy features, PDF merge and extract, Content processing rules, and document translations.

Advanced Search Options Powered by Microsoft Syntex

As explained in the Microsoft Search section, the default user experience when searching is limited to typing a search term and getting results meeting those criteria. When Microsoft Syntex is added to a tenant, the search box in Document libraries is enhanced with the [Microsoft Syntex content query feature](#). Content query provides the following advanced search capabilities:

- Search for metadata in any of the queryable columns in a document library.
- The following default search filters: Keywords, File name, People, Modified date, and File type.
- Search for custom columns present in a document library.

Content query search filters are present in Document libraries of all SharePoint sites, but they are not available in other SharePoint search locations including the SharePoint tenant landing page. Content query is available for users who have per-user or pay-as-you-go licensing.

Microsoft Syntex SharePoint Advanced Management

[Microsoft Syntex SharePoint Advanced Management](#) is an add-on license covering:

- Management and governance features for SharePoint and OneDrive such as:
 - [Block the download of files from SharePoint sites and OneDrive for Business](#) without using Entra ID conditional access policies. SharePoint Online restricts browser access for users. They cannot download, print, or synchronize files, nor open them with desktop apps.
 - [Review recent SharePoint site actions](#) made in the SharePoint Admin center in the last 30 days.
 - [Manage site lifecycle policies](#) to set up inactive sites policies to automatically detect inactive sites and send notifications to site owners via email.
 - [Create change history reports](#) to review SharePoint site property changes or tenant settings changes (in preview) made within the last 180 days. There is a limit of 5 change history reports that can be created.
- Options to secure collaboration based on SharePoint and OneDrive:
 - [Restrict access to a SharePoint Online site to members of a specific Microsoft 365 group](#). This feature also blocks users who previously had access to files in the site. The restricted access control policy applies to Microsoft 365 group-connected sites, non-group connected sites, and Microsoft Teams. A detailed explanation of how to configure this functionality with PowerShell and in the SharePoint Online admin center is in [this link](#). In addition to restrict access to existing sites, Administrators can:
 - Create custom “learn more” links for access denial messages running **Set-SPOTenant** command with the **RestrictedAccessControlForSitesErrorHelpLink** parameter configured with the custom “learn more”.
 - Generate reports with the list of sites protected by a restricted site access policy and details of access denials due to restricted site access. The PowerShell cmdlets to execute, view and download the reports are described in [this link](#).
 - [Limit OneDrive access to a security group](#) so only members of that group can use it.
 - [Restrict access to a user’s OneDrive content to people in an Entra security group](#). This feature prevents anyone who is not a member of the security group configured to access the OneDrive’s content even if they had prior access or it’s shared with them.
 - [Data access governance reports](#) to evaluate how content is shared from SharePoint sites.
 - Use of sensitivity labels with [Entra ID authentication contexts to limit access to SharePoint Online sites](#).

This advanced management add-on requires users who access sites that use the add-on capabilities to have a license for (\$3 per user per month for SharePoint Advanced Management Plan P1 add-on). Users must also have SharePoint K, P1, or P2 via standalone or a Microsoft 365 suite.

Microsoft 365 Archive

[Microsoft 365 Archive](#) allows organizations to move inactive SharePoint Sites into a cheaper cold storage tier within the SharePoint tenancy. Microsoft 365 Archive uses a pay-as-you-go model with charges based on storage consumption and sites reactivations:

- Storage consumption is charged at a per-GB monthly rate (\$0.05 GB/month). Storage consumption charges only happen when archive storage plus active site storage exceeds the total storage capacity available in the tenant.
- Site reactivations are charged at a per-GB rate (\$0.60 GB/month). The reactivation fee is applied no matter the storage capacity status in the tenant. The fee is not applied when site reactivations are executed within a seven-day grace period established once a site is archived.

To enable Microsoft 365 Archive in a tenant, follow these steps:

- Create a resource group in an Azure Subscription linked to your Microsoft 365 tenancy.
- Set up Microsoft Syntex pay-as-you-go billing through the Microsoft Syntex setup options in the Microsoft 365 Admin center.
- Turn on Microsoft 365 Backup in the Microsoft Syntex setting options.

Once Microsoft 365 365 Archive is turned on, to archive an active site:

- Browse the Active sites section in the SharePoint admin center, select a site, and then Archive.
- On the Archive details panel, click on Archive. The site is archived and can be found in the Archive sites section in the SharePoint Admin center.

After January 25, 2025, SharePoint Online [automatically moves unlicensed OneDrive accounts](#) into Microsoft 365 Archive unless an administrator deletes the accounts within 90 days of the accounts becoming unlicensed. Accounts moved into Microsoft 365 Archive are inaccessible unless an Azure subscription is available to pay for access to the accounts on a pay as you go basis. Administrators can retrieve an account from the archive to allow its contents to be reviewed and moved (if necessary) to another repository. Restored accounts are available for 30 days after which SharePoint Online moves the account back into an archived state.

The downloadable OneDrive accounts report lists details of OneDrive for Business accounts in an unlicensed state. Administrators should review the report periodically and decide which accounts to delete permanently and which SharePoint Online should move into the archive.

Microsoft Viva Connections

[Microsoft Viva Connections](#) is an example of a native integration of a modern SharePoint site as a Microsoft Teams app. Viva Connections allows end users to access and browse corporate resources published on the site within Teams. Deploying Viva Connections requires a SharePoint Admin to [follow a step by step process](#) that involves the following actions:

- (Recommended, but not mandatory) Create a [SharePoint home](#) site by running the `Set-SPOHomeSite` cmdlet or the Viva Connections experience in the Microsoft 365 admin center. Creating more than a Home site (up to fifty) requires having a Microsoft Viva suite or Viva Communities & Connections license. Otherwise, a tenant can only support a single home site.
- (Recommended, but not mandatory) Enable global navigation in the home site and customize any navigation link required for end users.
- (Recommended, but not mandatory) Set up the Viva Connections dashboard that can be customized with custom dashboard cards.
- Access the Viva Connections admin center in the Microsoft 365 Admin Center (Settings → Viva → Viva Connections) and select *Create and manage Viva Connections experiences* → *Create* to create a new Viva Connections experience from scratch or select an existing site in the tenant. Select the Viva Connections experience you want to configure. In the Home site details panel, configure the following settings:
 - Status (General tab): Enables the Viva Connections experience in the Viva Connection App. Initially, the experience is created as a Draft experience hidden to end users
 - Audiences: Define who has access to the Home site (All tenant users or users members of specific Microsoft 365/Security groups).
 - Permissions: Define the owners of the Home site.

Once the SharePoint administrator has done his/her job, a Teams administrator can perform the following actions:

- Browse the Manage apps section in the Teams admin center. Look for the Viva Connections Teams app, verify that the app is enabled, and update (if necessary) the following parameters:
 - The name for the app. This name will appear in the Teams navigation bar once the app is deployed.
 - A short and long description of the app.
 - Privacy policy and terms of use.
 - Company name and company website.
 - Large and small app Icons (sized at 192x192 and 28x28 pixels).
- (Optional) Manage and pin the app by default for corporate users by modifying an existing Setup policy or creating a custom one as [described here](#).

Microsoft Viva Connections does not need a specific license. Any user with a Microsoft 365 license can use Viva Connections.

Transitioning to the Viva Home Experience

As an alternative to the default Home Site, tenants can configure Viva Connections to display the [Viva Home Experience](#). This uses a predefined layout to deliver information to end users together with shortcuts to other Viva products such as Viva Insights, Viva Engage, and Viva Goals. SharePoint administrators enable the Viva Home experience using the `Set-SPOHomeSite` cmdlet to set the `VivaConnectionsDefaultStart` property as follows:

```
Set-SPOHomeSite -HomeSiteUrl "https://Office365ITPros.sharepoint.com/sites/0365ITPros" -  
VivaConnectionsDefaultStart $False
```

After a short propagation delay, the Viva Home Experience shows up in the Viva Connections Teams App. To disable the Viva Home Experience and return to the tenant Home Site, run:

```
Set-SPOHomeSite -HomeSiteUrl "https://Office365ITPros.sharepoint.com/sites/0365ITPros" -  
VivaConnectionsDefaultStart $True
```

Other Services Using SharePoint Online and OneDrive for Business

SharePoint Online and OneDrive for Business are not only core workloads but also a key part of other services in combination with other services such as Exchange Online and Entra ID:

- **Microsoft 365 Groups.** Each time a Group is created, a site with a default home page with four Web Parts and a single document library is provisioned for the Group. In the same way, each time a team site is created, a Group is provisioned. Group members can easily store files, create lists, and document libraries and subsites.
- **Planner**, the task management application is deeply integrated into SharePoint Team sites through the Planner Web Part, which allows developers to [incorporate plans in pages](#) in a site.
- **Teams** uses Microsoft Groups as their membership service, which means each time a Team is created, a Group is created behind the scenes together with all its building blocks (a group object, an Exchange Online mailbox, and a team site). Again, all the documents generated through team activity are stored in a document library. Teams also uses OneDrive for Business to store files shared in personal chats. In addition, each time a private or shared channel is created for a Team, a new site is created in SharePoint Online.
- **Viva Engage:** Each time a community is created, a special type of group is provisioned including a team site, a Planner Plan, and a OneNote notebook. All the files uploaded to the community are stored in a document library within the site. Files for stories created by Viva Engage users are in their OneDrive accounts.

- **Microsoft Loop** uses the [SharePoint storage infrastructure](#) to store workspaces, pages, and components.

SharePoint Online can also take advantage of other cloud services:

- **Microsoft Power Apps** can customize lists and document libraries and forms or create standalone Apps that do not require the author to write any code to [create custom forms that are mobile ready](#). The user only needs to click on the “PowerApps” action in a list to either create a custom app or customize the list forms. [A modern PowerApps Web Part](#), still in preview, supports the rendering of Power Apps in SharePoint pages.
- **Power Automate** enables users to design and deploy business processes that work with SharePoint lists and document libraries (see the Power Platform chapter for more information about how to build Power Automate apps).

Chapter 8: Planner and Tasks

Paul Robichaux

Planner Architecture and Management

The quality of planning done for a project can spell the difference between success and failure. In the 1960s, project-planning tools were mostly restricted to extremely large engineering-focused projects such as NASA's manned lunar missions. However, as computer power and capability became more democratized, so did project planning and scheduling methodologies. Microsoft's portfolio has long included Microsoft Project, a sophisticated planning product, about which the kindest thing that can be said is that it is easier to use than its competitors. For smaller-scale needs, every version of Outlook has included a tasks module to create and track tasks alongside email and calendar items. Today, Microsoft 365 has a Task ecosystem where multiple applications generate tasks that share many common elements. The fact that we have Outlook, Microsoft To Do, Microsoft Planner, Microsoft Project, and various other cross-application features to create and manage tasks can be confusing. It helps to reduce confusion once you know that Microsoft now thinks of tasks as falling into three categories:

- **Me tasks** belong to an individual, usually the person who creates, manages, and views the tasks. For example, my list right now includes "update airplane GPS," "reorder cat food," and "Chapter 09 MAC tasks." Usually, people manage their "me" tasks with To Do or Outlook, but you could also use tasks in apps like Planner, To Do, Outlook, or access the task objects programmatically using the Graph API.
- **We tasks** are owned, shared, or worked on by a team. While you could use a shared task list in To Do, it's much more natural to think of these tasks as those associated with plans in Planner.
- **Organizational tasks** represent shared work items defined by an organization. Think of the work a retail company must do each time they open a new store. From site selection to hiring and training to putting out signs on the sidewalk, there's a repeatable process followed each time, but the people who create the process aren't the same ones who carry it out. For example, the local store manager usually hires store staff. Teams includes the ability to publish tasks making up a work plan based on an organizational structure (the team targeting hierarchy).

The Future of Planner: Microsoft is working through a series of changes to the existing Planner, To Do, and Project products:

1. At Ignite 2023, Microsoft announced that they were renaming the "Tasks by Planner and To Do" app in Teams to simply "Planner." This change is now complete.
2. Microsoft also renamed Microsoft Project for the web to "Planner Premium Plan." This change applies to Project for the web, Project tabs in Teams, and the Project Power App. The original intent was to rename Project for the web to "Planner (Project)", but that change was axed.
3. In early March 2024, Microsoft [released the public preview of the new Planner app for Teams](#) with additional functionality compared to the current version. Some of these added features are cribbed from [Microsoft Project for the web](#), and might require payment for an additional license. The rollout started poorly, with a bug that prevented the new Planner from being deployed to many tenants. There are still many missing parity features in the new Planner app; expect more updates to this chapter once the deployment stabilizes and Microsoft has stamped out a few of the more egregious bugs reported by users so far.

4. Starting in October 2024, Microsoft will roll out the new Planner on the web. As part of this release, they originally said that "Microsoft Project for the web will be available in the new Planner app in Teams and the Planner web app." MC887371 has details of the rollout plans.

Some of the [features](#) that will be added to Planner may require an additional service plan subscription. For now, the existing To Do applications will remain unchanged. We'll update this chapter as these changes come closer to reality, but for now this summary may be helpful.

Multiple Clients for Managing Tasks

Based on this division of task ownership, the way Microsoft has organized its task management applications makes more sense. There are a few organizing principles. First is that it's okay—in fact, desirable—for there to be multiple ways to access, edit, and update the same set of tasks. The use of a common task object across Microsoft 365 is why Tasks created in Outlook show up in the To Do app and vice versa. Second, the service should always try to collect all the tasks that "belong to" you in one place. In this case, "belong to" means both tasks that you created and those assigned to you, no matter the type. That's why the Teams Tasks app shows both your personal tasks and tasks assigned to you in Planner plans.

Another organizing principle is that Microsoft distinguishes between task management and project management. As individual people, we all have tasks to manage, but managing larger-scale projects requires different tools because the outputs are different.

Table 8-1 shows a summary of some of Microsoft's task management ecosystem. With that summary in mind, we can dig into the individual applications in more detail.

Individual ("Me")	Team ("We")	Company ("Org")
Outlook Tasks	Planner (including the new Planner app in Teams, Planner on the web, and Planner in Loop)	Project Server / Project Online
Microsoft To Do	Microsoft Lists	Teams organizational tasks

Table 8-1: The continuum of task management from to-do items to projects

Planner

Microsoft Planner is a lightweight task-oriented planning service whose big advantage and unique selling point is its integration with other Microsoft 365 workloads. This integration is facilitated by using the membership and identity services of Microsoft 365 Groups. Planner is included for commercial and [US government cloud](#) tenants with enterprise licenses, the Business Premium and Business Essentials SKUs, and most educational and non-profit SKUs.

Planner might seem to compete with Project Online, other Microsoft offerings like SharePoint Online, third-party offerings that plug into Microsoft 365 for task management (like [Tasks In a Box](#)), and third-party products. It's a fair question to ask what Planner's purpose is given this crowded space. Part of the answer comes from the fact that the same engineering group develops Planner, Project, and Project Online, which means that it's no surprise that Planner and the web version of Project share some code. You can think of Planner as "Project lite," an entry-level task management application. Planner lacks many of the features of Project, like dependencies between tasks, but its user interface offers better sorting and filtering of tasks and people often consider Planner easier to use.

Probably the most accurate way of thinking about Planner is that it is Microsoft's version of the popular and widely used Trello application, which is itself an app that embodies [Kanban-style planning methodology](#). Trello has been around for a while and the two applications share many visual similarities in layout and visual design, albeit with slightly different naming conventions. For instance, Trello lists are equivalent to Planner

buckets. See [this page for a comparison](#) between Planner and Trello. Unlike Trello, though, Microsoft has built Planner so that it can be embedded in other applications.

Like many other Microsoft 365 workloads, Planner's original client was browser-based. The browser client is still around, now hosted at <https://planner.cloud.microsoft>. The initial web client was followed by mobile apps for [iOS](#) and [Android](#) and integration with Teams as an app and channel tab. One of the chief useful features of these clients is that they can aggregate all tasks assigned to a user in a single view on the "My Tasks" page, so no matter what team or Group the original plan is in, all the tasks an individual is responsible for appear in a single place. As with Outlook, new Planner features have historically shown up in the web version first.

Other than the Planner app in the Teams client, there's no true desktop client for Planner. Interestingly, the Planner team did start work on one, but deferred work on it in favor of providing integration between Planner and Teams. The Planner web app works well as a progressive web application (PWA), [as described here](#). Using this workaround, you can have a desktop app which is really a frame around the Planner web app, but that is good enough for many purposes.

There's a Loop component for Planner, which currently works only in the Loop app; Microsoft has promised to bring it to other Loop integrations including Outlook and Teams. The Planner Loop component is enabled by default but can be [disabled using the Cloud Policy service](#). When you create Planner tasks in a Loop component, they show up in Planner (and To Do) like any other tasks. The Loop component provides a simple interface for creating and assigning tasks; to get full access to all the task fields described in this chapter, you'll have to edit the tasks in Planner itself.

If you'd prefer to use Outlook, Microsoft has an iCalendar connector to link tasks assigned to a user to their Outlook calendar (see the later section). In the meantime, a third-party add-in is available in the Office Store from [iGlobe](#) that makes Planner appear as an Outlook resource (just like public folders). You can navigate between tasks and view their details. Another tool from the same company [gives a reporting capability](#) for Planner.

SharePoint Online supports a Planner web part that can be added to a page for a modern site. The web part displays tasks from a plan belonging to the underlying Group. If a plan doesn't exist, you can create it and then add it to the web part.

Microsoft To Do

Microsoft bought the Wunderlist application in 2015, then promptly threw it away and built a new app on top of its cloud infrastructure, called Microsoft To Do. To Do is described as a "simple and intelligent to-do list app that empowers users to keep track of and focus on the things they need to get done." It's meant to provide a consumer-level solution for task management independent of whether the user has access to, or uses, Outlook or Planner. To Do is supported for both Microsoft 365 and Microsoft consumer accounts. In fact, that's how Microsoft positions it—as a single app that lets you manage tasks in your personal life (stored in your consumer account) and your assigned tasks at work. The To Do app supports multiple accounts and it's easy to switch between them as needed.

The To Do clients (available for Windows, the browser, macOS, iOS, and Android) use the Outlook Tasks Graph API to store task info in the Tasks folder of the user's mailbox. When users create a new list with the app, the to-do items for that list go into a sub-folder under Tasks named for the list. Tasks created using Outlook.com or Exchange Online synchronize with the To Do service. Messages flagged in Outlook show up in To Do as tasks in a separate (and optional) *Flagged Email* view. You can use To Do to edit details of the task, assign steps (individual checklist items for the task), mark it as important, set reminders, and add the task to the *My Day* view. Although "My Day" seems simple, this feature made To Do much more useful than before and convinced some people who were dedicated users of Outlook Tasks to adopt To Do as their personal task management app, and it's been popular enough that Planner in Teams has adopted it as well.

By default, Microsoft enables To Do for users with [eligible Microsoft 365 subscriptions](#). There's no longer a way to control To Do on a tenant-wide basis, but you can control access for individual users by editing the options bundled in the Microsoft 365 license assigned to the user to remove or allow access to the application. Like many Microsoft 365 client applications, there's an "[Insider](#)" program for To Do that allows you to get early access to new features in the client and service. There are separate insider programs for Windows, [Android](#), and iOS.

Microsoft Project

Project is Microsoft's high-end project and task management application. To Do is intended to manage personal tasks, and Planner helps you manage tasks for your team or workgroup, but Project is the kind of tool you'd use if you wanted to launch a space mission, build a hospital, or do something similarly complex. Originally launched for MS-DOS in 1984, the capabilities of the Project application have expanded dramatically since. The latest iteration is composed of Project clients and servers, the latter being available in on-premises and [cloud](#) versions. Project is a powerful and sophisticated time and task management application that is much beloved by professional project managers. It can handle the complexities involved in very large projects such as the design and construction of major infrastructure projects. Like many highly functional software packages, learning to use Project can be overwhelming and it can take a long time to become proficient in its use. Those who have mastered Project will probably consider Planner to be simplistic and deficient in terms of charting, dependencies, and other areas. However, it is worth underlining again that Microsoft does not intend Planner to take on the kind of complex, heavy-duty planning requirements that Project is meant for. In short, Project is the right tool to use when you must coordinate multiple milestones, dependencies, and complicated schedules.

If needed, you can [connect tasks managed in Project Online with Planner](#). However, you cannot transfer tasks from Planner to Project or convert a plan into a project or vice versa. With the promise of the new Planner looming, Microsoft has made two other integration changes. First, tasks assigned to a user in Project on the web will appear in that user's Planner task list. Second, Planner users can edit some fields of tasks in a Project project that has been shared with them. The general rule is that Planner users can edit any field that is common both in Project and Planner; items that are Project-specific, such as dependency relations, can only be created or edited by users who have a full Project license. The [Project for the web service description has a helpful table](#) showing which specific Project features are available to Office 365 Planner users, Planner Premium users, and the various Project license levels.

Outlook Tasks

Outlook's Task functionality dates to its original debut back in the early 1990s. Don't expect much from Outlook as a task manager: you can create and manage lists of tasks, assign due dates, and so on. Perhaps the best task-related feature in Outlook is the ability to treat a flagged message as a task, or maybe the ability to drag a message into the Tasks folder to treat it as a task. When you absorb Microsoft's principle of "many clients, one task," it's easier to let go of the concept of using Outlook for task management instead of the easier-to-use and more functional To Do and Planner clients.

Microsoft Lists

At first glance, Microsoft Lists seem very similar to Planner. However, while some crossover exists, the two applications are very different.

- Planner is an out-of-the-box general-purpose task management application for teams. You don't need to customize anything to start creating and managing tasks. It's all done for you in the app. The downside is that you can't customize how Planner works.

- The Lists app is more of a toolbox to create customized applications to track and process different forms of data. You can use Lists to manage tasks, but you'll need to define what a task is and any associated components, like attachments, links, and so on.

Today, no connection exists between Planner and Lists. Microsoft has talked about how the two applications could interact in the future, but no solid plans for this are yet public.

Unified Tasks on the Microsoft 365 Home Page

Users who visit their Microsoft 365 home page see the Planner and To Do tasks assigned to them. These items join the existing summary views of Word, PowerPoint, Project, and Excel documents shown when users visit their home page.

The Planner Back-End

Because Planner supports shared tasks and plans, there's more to it than just another front-end that reads tasks from users' Exchange mailboxes. Before we go any further, it's probably helpful to understand that the fundamental object type in Planner is the *plan*. Think of a plan as a container for tasks that "belong" together because they're related to the same project or owned by the same user or group.

Planner, Microsoft 365 Groups, and Applications

Planner originally had a dependency on Microsoft 365 Groups. Every Group can have a corresponding plan; if a plan exists in a Group, the plan belongs to that Group. Originally, a Group could only have a single plan, the default plan, but this situation changed to accommodate the need for Teams to support multiple plans through channel tabs. The membership of a team depends on the underlying Microsoft 365 Group. However, each channel inside a team can have multiple plans, all of which belong to the team (and the Group). One unique feature of the integration between Planner and Teams is that when you're assigned a task in Planner, the assignment [appears in the activity feed in your Teams client](#) (although thankfully you can turn this integration off).

Group-enabled SharePoint team sites can also create multiple plans, all of which are associated with the team site. You can add these plans (or the default plan for the Group) as links accessible from the home page of the team site or embed one or more plans in site pages using the Planner web part, deciding whether the web part displays boards or charts. The Planner hub does not display the name of the underlying team site that a plan belongs to, so it is wise to include the name of the site when naming a plan.

Technically, users with on-premises mailboxes can use Planner. However, the full functionality available in Planner, particularly the close connection with the underlying Microsoft 365 Group, is only available for Exchange Online mailboxes. Users with an on-premises mailbox will find that some features (such as adding a comment to a task using OWA or Outlook or marking plans as favorites) aren't available.

Lightweight Plans: Plans without Groups

Microsoft supports "lightweight plans," a separate way of creating plans without needing to use a Microsoft 365 Group to host the plan, in Planner. This feature was formerly called "roster containers" and went through several delays.

Instead of using a Group, lightweight plans have a membership roster. Microsoft hasn't yet said how they will use lightweight plans, but it's likely to be associated with features like Teams shared channels, which use external federation rather than Azure B2B Collaboration to allow the sharing of information with people from external tenants. The original release of this feature was [delayed for several months](#). You can create and work with lightweight Plans using Graph API or the PowerShell `*-MgPlannerRoster` cmdlets. Now that [Loop components are available in Teams chat](#), Microsoft will bring support for lightweight Planner plans in Teams chats, too, as opposed to the simple to-do list component now available. This will be a significant upgrade

because the existing fluid task component stores tasks in the Loop components file, which lives in the originator's OneDrive for Business account—meaning that these tasks break the principle of "see your tasks everywhere." We'll have to see if Microsoft delivers on this promise fully with lightweight Plans; expect to see further updates here as this feature evolves.

Personal Plans

In addition to regular and lightweight plans, in the new Planner, Microsoft is introducing what it calls a "personal plan." Like lightweight plans, personal plans aren't associated with a Microsoft 365 Group. Unlike lightweight plans, personal plans aren't shared by default; they are only visible to the owner. The plan owner may share them with a Group at any time. Personal plans are stored in what Microsoft calls a "user container." When the personal plan is created, it appears in the owner's Planner application, although some features that depend on Groups integration (including task comments, attachments, and links to OneNote) aren't available because the plan's stored in a user container. If the owner shares the personal plan with a Group, it's moved to the Group's container, at which point the missing features become available. Note that the plan can't be made personal again. For now, this change is somewhat academic; the existing Planner apps for web and Teams don't have a UI for creating personal plans. They are accessible through Graph, but full support will have to wait for a future release of the new Planner.

Sharing Plans Through Files

As Loop components have become more pervasive across the service, a new problem has occurred: users aren't always aware that the Loop components they add to various places are actually treated in many respects like files. In particular, linking a Loop component to a Planner plan might put users in a state where they could see the component but not the underlying plan. To solve this problem, Microsoft has added the ability to do what they call "plan sharing through file containers." That's a fancy way to say that if you have a file in SharePoint or OneDrive that links to a Planner plan, users who have permission to see the file will also automatically gain access to the plan.

Business Scenarios

"Business Scenarios" is the name of a Planner-related feature that allows application developers to package a set of behaviors that integrate external services and permissions management. The example they give is that you can create a business scenario to define exactly what buckets will be created in a Planner plan when it's created through Graph, automating the process of provisioning those buckets, and at the same time applying permission templates so that every newly created plan has consistent controls over things like which task fields users are allowed to edit. The [beta version of this API and its documentation](#) are available.

Planner Services and Storage

Like Teams, Planner stores data in different places. As described in chapter 1, each of the services Planner uses may have different data locality capabilities, so if data sovereignty is important to you, you should review Microsoft's data storage locations for the services used by Planner. Planner and project data is stored in several locations:

- User tasks created or edited in To Do and Outlook are stored in Exchange user mailboxes. Microsoft warns that if you have users who do not have Exchange Online mailboxes that you may have trouble viewing or editing tasks for those users.
- Plans and their included tasks are stored in Azure.
- Attachments on tasks in plans and projects are stored in the SharePoint site of the Group.
- Premium plans and their included tasks are stored in Dataverse. This follows the storage system used for Project.

The second bullet above needs a little more elaboration. Planner stores the metadata for plans, including information describing the tasks and buckets that make up each plan, in an Azure data service, protected by Azure Storage Service Encryption and complying with the service controls (e.g. ISO 27001) offered by Azure. [Planner is deployed in some, but not all](#), country-level Microsoft 365 data center regions, so your Planner services may come from a regional data center instead of the country. For example, Planner data for tenants in Australia is hosted in Australia, but tenants in Brazil have Planner data held in the US.

Whether your plan is contained in a Group, a roster, or a user container, the *container* for the plan holds the permissions (and other metadata) for the plan, but the tasks and their associated properties are stored in the locations listed above.

Like most other Microsoft 365 services, Microsoft publishes a [list of limits on the Planner service](#). For example, a single task can have at most 20 assignees. Very few of us are likely to run into these limits.

Programmatic Access to Planner Data

Planner supports a [Graph API](#) endpoint to support integration with outside solutions. Microsoft hasn't made an API available to backup and restore Planner data, or to move plans to another Office 365 tenant. There are third-party tools available to migrate plans from one tenant to another, but they can't capture 100% of the plan's data because not all the objects and fields are available through the public Graph API endpoints.

There's also a [PowerShell module](#) (for Windows PowerShell only) but the process for using it is complicated: you have to download the PowerShell module itself, unblock the PowerShell module (.psm1) file and an accompanying DLL, set the execution permissions for the module on the workstation you're using, and import the module. After all this work, you get a limited set of PowerShell cmdlets that only a Global admin role holder can run. That's probably why Microsoft calls the existing PowerShell module the "Planner Tenant Admin" module. However, you can still use PowerShell with Planner to do other useful things. You can:

- Use the PowerShell cmdlets for Groups to manage details of the groups used by Planner.
- Use Graph calls made through PowerShell to access Planner data.

For some examples of creating and updating plans and tasks with PowerShell, you may find this [Practical 365 article](#) useful.

Using the Planner Graph API with PowerShell

You can use the Planner Graph API with PowerShell to create plans, buckets, and tasks and to retrieve information about the contents of plans. You'll need to create an Entra ID registered app to interact with the Graph, assign the needed permissions to the app to access Planner data, and obtain an access token for the app to fetch data, all common steps used to create Graph-based apps. For example, here's the PowerShell code to call the Graph to retrieve the plans for a Group (pointed to by the group identifier):

```
$PlanURI = 'https://graph.microsoft.com/v1.0/groups/' + $Group.GroupId + '/planner/plans'
[array]$Plans = Invoke-WebRequest -Method GET -Uri $PlanURI -ContentType "application/json" -Headers
$Headers
```

If plan data is found, the code loops through each plan to find details about the plan, tasks, and buckets. Here's a snippet of those commands:

```
ForEach ($Plan in $Plans.Value) {
    $PlanId = $Plan.Id
    $PlanCreated = Get-Date($Plan.CreatedDateTime) -format g
    $BucketURI = 'https://graph.microsoft.com/v1.0/planner/plans/' + $PlanId + '/buckets/'
    $Buckets = Invoke-RestMethod -Method GET -Uri $BucketURI -ContentType "application/json" -Headers
$Headers
    $TasksURI = 'https://graph.microsoft.com/v1.0/planner/plans/' + $PlanId + '/tasks/'
    $Tasks = Invoke-RestMethod -Method GET -Uri $TasksURI -ContentType "application/json" -Headers
$Headers
```

{}

After fetching the Graph data, normal PowerShell commands can process the information. For instance, you could create a report listing the number of tasks (and the status of the tasks) and buckets in each plan, when the plan was created, and the number of days since the last task was posted as an indicator whether the plan is active. For more examples about using the Planner Graph API, read these articles:

- Reporting the [incomplete tasks in plans](#).
- Automating [plan creation](#).

A [delta-sync method for the Planner Graph API](#) is available too. The delta method allows applications to request only items that have changed since the previous request.

Planner and Microsoft 365 Compliance

Archiving inevitably brings compliance to mind. As discussed in this book, Microsoft 365 includes a comprehensive suite of data governance technology designed to work across the service. These services can work with Planner data in various ways.

Planner and eDiscovery

Planner creates "digital twins" (compliance records, sometimes called secondary copies) of tasks in Exchange Online mailboxes to ensure their availability for eDiscovery and other compliance purposes. The implementation works like this:

- Planner creates compliance records for tasks assigned to a single user in the *AllToDoTasks* folder in the hidden part of their Exchange Online mailbox.
- For tasks assigned to multiple users, Planner creates a copy of the compliance record for the task in the *AllToDoTasks* folder in each user's Exchange Online mailbox.
- Compliance records for tasks assigned to hybrid and guest users are in the special cloud-only hidden mailboxes used to hold compliance items.

It's important to emphasize that the data held in Exchange Online is for compliance purposes only. Task data in the Planner data store in Azure remain the repository of record.

Unassigned tasks are ignored until they are assigned to a team member. Compliance records are generated when tasks are created or edited. Planner does not go back to generate compliance items for old tasks, meaning that records for these tasks do not exist unless they are updated.

Because the compliance records are stored in Exchange Online mailboxes, task records (including comments and attachments) are indexed and can be found by content searches. In addition to the compliance records, Microsoft Search indexes the documents and comments belonging to plans stored in SharePoint Online and Exchange Online to make sure that they are discoverable.

Note that, as of August 2024, only task data is visible in eDiscovery searches, and plans stored in roster containers and premium plans aren't supported for eDiscovery.

Auditing Planner Activity

Microsoft has added the ability for Planner, Project, and To Do actions to be audited. For example, unified [audit log entries can be generated](#) for creating, removing, and reading plans and tasks. Group creation and updates (like adding a new member to a plan) generate audit records, plan actions such as creating a new bucket or task creation, update, assignment, deletion, and completion do not.

There are additional Project-specific audit items as well, which carry over to Planner Premium. However, to get any of these audit items, the users you're auditing must have a paid license (at least Project Online Plan 1) in addition to a Microsoft 365 license that enables their actions to be audited.

Legal Holds for Planner Data

As of July 2024, Purview support for holds on Planner data is in public preview. To put a Planner plan on hold, you must place a hold on the SharePoint site belonging to the Group that hosts the plan (meaning that you can't place holds on roster or personal plans).

Restricting Task Deletion

By default, any user who has access to a plan can create, remove, or edit tasks in that plan. It would be nice if Microsoft provided more granular control over this behavior. For now, the best you can do is to block people from removing tasks they didn't create. Blocked users can still delete tasks they created or edit any task in the plan. To do this, use the `Set-PlannerUserPolicy` cmdlet from the Planner admin PowerShell module mentioned earlier in the chapter with the `-BlockDeleteTasksNotCreatedBySelf` flag, like this:

```
Set-PlannerUserPolicy -UserAadIdOrPrincipalName andy.ruth@contoso.com  
-BlockDeleteTasksNotCreatedBySelf $true
```

Of course, you can use the same cmdlet to unblock a user and allow them to go back to deleting other people's tasks just by using `$false` as the parameter for `BlockDeleteTasksNotCreatedBySelf`.

When you apply deletion blocking using this cmdlet, there is a (currently) undocumented side effect: the targeted account *also* cannot delete plans. It is not clear whether this behavior is intended or accidental, but you should be aware of it.

Controlling Plan Privacy

The method used to change the privacy setting for a plan depends on if the tenant uses sensitivity labels for container management. If the tenant's using sensitivity labels for container management (as described in the Information Protection chapter), applying a sensitivity label imposes the privacy setting inherited from the selected label. In organizations that are not using sensitivity labels, Group owners can edit the properties of the plan or run the `Set-UnifiedGroup` cmdlet. For example, to set a Group (and its plan) to be private:

```
Set-UnifiedGroup -Identity "Secret Plan" -AccessType Private
```

Because access to a plan depends on its Group, you cannot selectively reveal a plan's contents without also exposing the contents of the Group. For example, you might want to solicit feedback on the details of a plan from outside the project team. To accomplish this, if you set the Group to public, you will also expose the other shared resources (documents, conversations, calendar, and notebook) in the Group. This may or may not be acceptable. Some forethought thought is necessary to figure out whether a plan should be public or private when it is created or if you edit a private plan to change its status to public.

Moving Planner Data to a Different Tenant

Many Microsoft 365 workloads have formally defined processes for moving data from one tenant to another. APIs exist to import and export data from some workloads, and both Microsoft and clever third-party vendors have used these to provide a way to move workload data between tenants. Planner data can be moved between tenants, but it requires that you open a support request with Microsoft to accomplish the move. Before they will execute a requested move, you [must authorize it](#) using the rather scary-sounding `AllowTenantMoveWithDataLoss` flag with the `Set-PlannerConfiguration` cmdlet. No plans or task data are moved when Microsoft runs the move operation, so it's not clear why you'd ask Microsoft to do such a move instead of using a tool such as [MVP Sean McAvinue's PowerShell script](#) or [this one from MVP Alexander Holmset](#).

Controlling Access to Planner Data with Conditional Access Policies

You can control access to Planner data using Entra ID conditional access policies. However, if you create a CA policy for controlling Planner access, it won't actually restrict access for users who are using the iOS or Android Planner apps unless you *also* add CA policies that control access to SharePoint Online and Exchange Online. This requirement makes sense when you remember how and where Planner stores data, but it is not widely known.

Publishing Organizational Tasks in Teams

In addition to personal and team tasks, Microsoft has been extending support for organizational tasks, which you create and publish through Teams. These are primarily useful for frontline workers. When you assign an organizational task to someone, it appears in their individual Planner/To Do scope and can be tracked and managed there just like other tasks, but its status can be centrally monitored, and you can quickly publish fairly long and complex task lists.

Enabling Organizational Task Publishing

Teams understands the concept of a hierarchical organization. This may surprise you because there's little evidence of that in the default Teams permissions (where anyone can create a new Team or channel). However, at present only the Planner app in Teams can interpret the hierarchy definition. To use task publishing, you must define the hierarchy by creating a CSV file and uploading it using the `Set-TeamsTargetingHierarchy` cmdlet. This is a fairly straightforward process, [described in Microsoft's documentation](#). You must set up a hierarchy (even if it's flat) before you can publish tasks. For example, imagine that Contoso has a team called Global Sales for all members of its sales organization worldwide, then region-specific teams for North America, Europe, Asia-Pacific, and so on. They could then define a hierarchy that sets the region-specific teams as subordinate to the main sales team. (Microsoft has teasingly promised that hierarchical relationships between teams will be used in other parts of the Teams client but for now only the Planner tools interpret the defined hierarchy.)

The rules for understanding who can publish lists are fairly simple, and they're based entirely on the hierarchy:

- Any member of a team can publish task lists to descendants of that team, so a user in the Contoso Global Sales team can create lists and publish them to any of the regional sales teams.
- Any member of any team anywhere in the hierarchy can see and receive published task lists. This enables frontline workers and others who are in "leaf node" teams to see tasks. That means members of any of the regional Contoso teams (which don't have any descendants) can still work with published tasks.
- Users who aren't a member of any team in a hierarchy don't see published tasks. A user who's only a member of the Global Marketing team at Contoso can't see any of the tasks lists published to the regional sales teams.

Users with access to task publishing will see two new tabs in the top of the Teams Planner app. **Published Lists** shows the lists that you've published, and **All your tasks** shows the tasks that you are assigned (either directly or through channels or shared plans that you're in). You can choose who gets notifications when you publish or unpublish a task list, which will be useful for ensuring that the correct people see task changes.

As part of the launch of the new Planner experience, Microsoft has added several features since the original release of task publishing:

- You can publish recurring tasks.

- You can assign a task list to a group so that each member of the group gets their own copy. Microsoft gives the example of a set of annual training tasks, where you want each person on the team to complete those tasks on their own.
- You can require that users fill out a Microsoft Forms form as part of marking a task as complete.
- You can require that another user mark the task completion request as "approved" before it's recorded.

Creating and Editing Organizational Task Lists

The basic workflow for publishing task lists works like this:

1. Create a draft list using the **New list** button in the **Published Lists** view.
2. Name the list and add the tasks you want included. You can set several fields for the tasks (including a task title, bucket, priority, start or due date, notes, one attachment, and a checklist of up to 20 subtasks).
3. Edit the tasks as needed. The list remains in a draft state until you explicitly publish it.
4. Publish the list when you're ready. You can choose which teams in the published hierarchy should receive the list.
5. As needed, edit the published list to add, delete, or modify tasks. To do this, you put the published list in edit mode, make the desired changes, and re-publish it.

You can unpublish a task list, but when you do, it removes all the tasks from all the teams that received it. This may confuse users, and it will cause loss of any changes that users have made to the tasks (such as adding notes or attachments).

Within the **Published Lists** view, when you select a list there are two sub-tabs (**Tasks** and **Teams**) that show basic reporting about the assignment and completion percentages for tasks.

Microsoft's documentation has [more step-by-step guidance](#) on how to manage and use organizational tasks.

Linking Planner and the Microsoft 365 Message Center

As an example of what's possible with Planner, Microsoft released a service to synchronize notifications about changes in Microsoft 365 services from the Message Center in the Microsoft 365 admin center (described in the Tenant management chapter) to create tasks in a target plan. Each time Microsoft announces a change in the service, a new task is created that can be assigned to the person or team responsible for communicating and managing that type of change within the organization. A Power Automate flow runs on a scheduled basis to synchronize information from the Message Center to Planner. The integration is enabled through an option above the list of messages in the Message Center. When you select the option, you can choose which types of Message Center notifications you want to be synchronized, and which plan you want them copied into. Synchronization occurs once a day.

Tasks synchronized from the Microsoft 365 Message Center have start dates assigned by Microsoft but no due dates. The start dates are associated with the work being done by Microsoft to introduce a new feature instead of when a feature might be available in a tenant. If you don't adjust task dates after synchronization, it's easy to end up with a schedule full of red (overdue) tasks. For this reason, it's important to assign tenant-specific dates for tasks when assigning tasks to users.

The practical value of this feature is that it lets you capture change notifications in a single plan so that you can review the changes and possibly act, such as assigning tasks to other users, sending out notification emails, making infrastructure changes, and so on. It can be difficult to remember to keep up with the volume of change notifications in the Message Center, which has poor search functionality and no way to create a direct link to an individual notification. Copying these changes into Planner gives you a much more flexible

way to track and manage these changes, and it's a nice touch that highlights how well different parts of the Microsoft 365 platform work together. To learn more, see [this blog post](#).

Linking Planner and Viva Goals

Microsoft introduced the [Viva Goals](#) application as a way to provide company-wide tracking of goals and objectives. It uses the OKR ([objectives and key results](#)) framework to give the organization a systematic way to share, and track progress towards, whatever the organization thinks its key goals are. At Ignite 2022, Microsoft announced that they'd be providing integration between Planner and Viva Goals, and they delivered on this promise in mid-January 2023. The first of these integrations lets you link plans in Planner with specific OKR items in Viva Goals. As tasks in the plan are created, that completion is reflected in the associated goals in Viva Goals. There's currently no way to tie an individual Planner task directly to an OKR, although given how much emphasis Microsoft has put on Viva Goals it seems likely that they'll improve this integration in the future. In October 2023, Microsoft began deploying the ability to use buckets and labels from Planner to filter items in Viva Goals.

Microsoft has also announced support for connecting Project on the web to Viva Goals; you can use Project on the web as a data source for initiatives and key results in Viva Goals too. It's not yet clear how the Ignite 2023 announcement that Planner is replacing Project on the web might affect this integration.

Both of these integrations are controlled using the Viva Goals app itself; using a privileged account, you [enable them on the organization level](#).

Using the Planner Web Client

As of early October 2024, Microsoft hasn't started rolling out the new version of the Planner web client. When they begin, its availability will be controlled by whether you have enabled Targeted Release for your tenant (see the tenant management chapter for more details). At present you cannot use per-user Targeted Release to control who gets the new Planner experience; it's all or nothing. This section covers the "classic" Planner web client; we will update it as Microsoft progresses with the rollout of the new client.

You can access the Planner application with your normal Microsoft 365 credentials by:

- Clicking the Planner icon in the Microsoft 365 app launcher.
- Navigating to the Planner Hub at planner.cloud.microsoft (the old URL, tasks.office.com, still works as of August 2024 but will eventually be deprecated).
- Selecting Planner from the [...] menu of a Microsoft 365 Group when working with conversations in OWA.
- Navigating to it from a Viva Engage community.

The Outlook integration with Groups doesn't support Planner. We'll discuss the Teams integration later.

The Planner web application uses a streamlined interface composed of a navigation pane to the left and a details pane to the right. The user interface accommodates a range of screen sizes and form factors and resizes elements to fit the available space. Figure 8-1 shows how the Planner Hub displays Microsoft 365 Groups as Plans in the navigation pane. Plans marked as favorites show up on top. If you select a plan as a favorite, the groups in the favorites section of Outlook and OWA include the associated Group for the plan.

The "Assigned to me" link in the navigation pane displays tasks assigned to the user. As of August 2024, users will see tasks assigned to them from Planner, To Do, Outlook, meeting notes, Loop components, and Planner Premium (formerly known as "Project for the web").

The **All** pivot lists all the Groups (and thus the plans) to which the user belongs, even if these Groups have no plan information associated with them. The **Recent** pivot exposes Groups where recent activity has occurred,

but not necessarily planning activity. To work with a plan, click the name of an existing plan or create a new plan. You can force a plan to open in Teams by selecting the “...” menu next to a plan in the **Recent** or **All** pivots and selecting the **Open in Microsoft Teams** command.

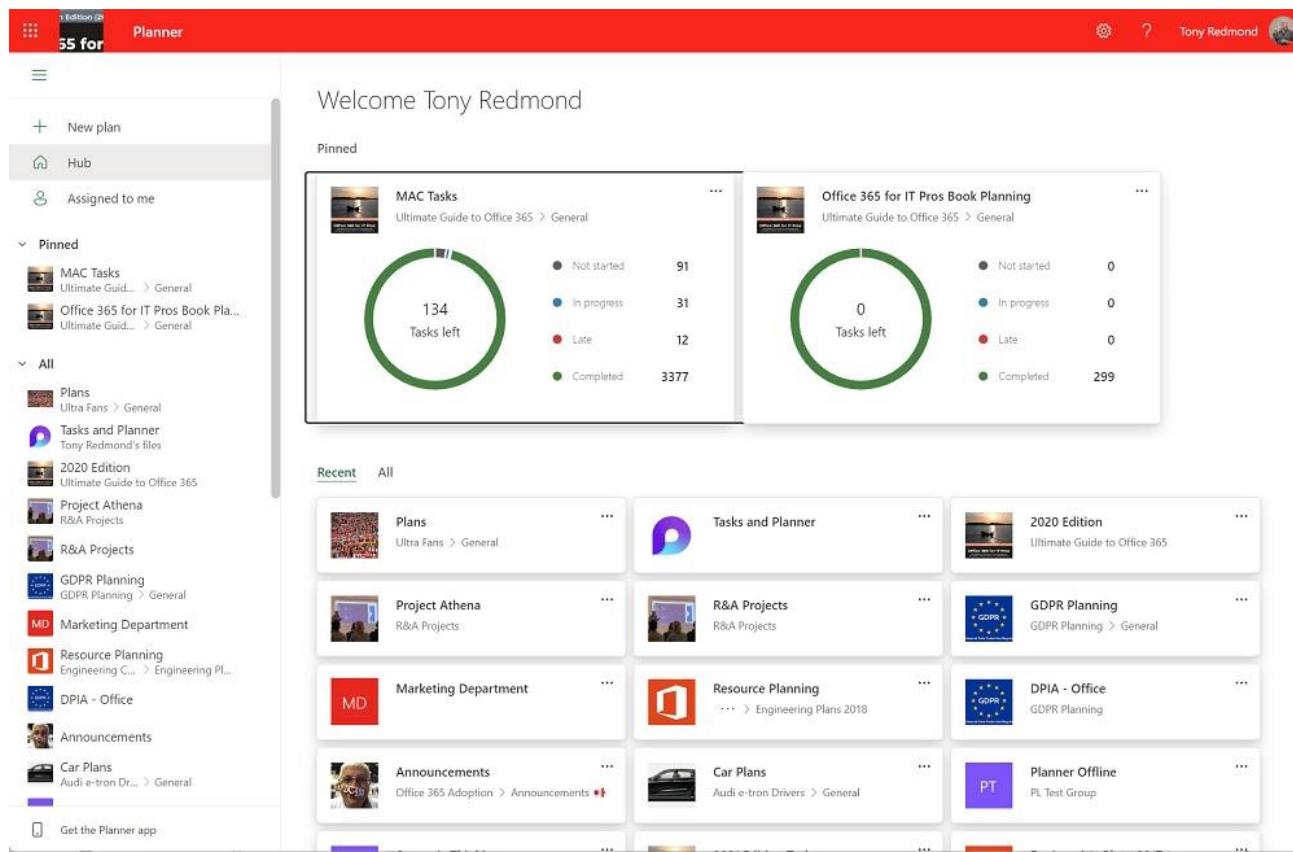


Figure 8-1: The Planner Hub

In addition to the plans belonging to Microsoft 365 Groups that the user is a member of, the Planner hub also lists plans associated with [Loop task list components](#). The middle plan in the set of plan cards is an example of such a plan.

Creating New Plans

You can create a new plan through the **New plan** command. There's no separate policy available to control plan creation, so Planner uses the creation settings from the Entra ID policy for Groups. If a user is allowed to create new Groups, she can create a plan and a new Group at the same time. If she's not allowed to create new Group objects, Planner will still allow her to create a new plan, but she must choose an existing Group to contain it. Planner doesn't give you a way to see multiple plans that belong to the same Group together; they'll still be treated separately. Plans created in an existing Group take on the properties of that Group (for example, public or private access) and are immediately available to its members.

The first choice to make is what template to use when creating your new plan. Microsoft currently offers templates intended for basic use, software development, project management, business plans, or employee onboarding; it's reasonable to expect that they may add more templates in the future. Once you choose a template, you must choose where to create the new plan, which can either be attached to an existing Microsoft 365 Group (or team) or created from scratch. If you opt to attach the new plan to an existing Group, the next step is to select the target Group or team. You may optionally specify whether the plan should be public or private.

Figure 8-2 shows how the Planner hub displays multiple plans belonging to a Group called GDPR Planning. The default plan for the Group takes the name of the Group while the other plans have the Group name shown under their name.



Figure 8-2: Multiple plans for a Group

Provisioning New Groups

If you choose to create a new plan, the service creates a brand-new Office 365 Group to host the plan. A Microsoft 365 Group created by Planner is the same as any other Group, with a SharePoint team site and other resources. If a Group naming policy is in force, the names given to new groups or teams must comply with the policy. The exception is for plans created by tenant administrators, who do not come under the control of the naming policy.

After creating a new plan, you will want to add some members. Click Members in the menu bar to add tenant users and guest users to the membership of the Group. Remember that these people are now full members of the Group and will therefore have access to other resources belonging to the Group.

Planner Tasks, Buckets, and Boards

Tasks form the basic building block for a plan. Each task describes a piece of work, including information such as the person assigned the work, start and end dates, and a priority for the task. Planner uses a card metaphor to display information about tasks. You can customize the cards to display different information about the tasks such as including a graphic, an expanded description, or even a checklist item.

Planner organizes tasks into "buckets." Its primary UI is to arrange the buckets on a "board" (the analogy is to pin index cards with details of tasks to a corkboard). Think of a bucket as a collection of tasks that constitute a major section of a plan, or a collection representing tasks in a specific state. Each plan begins with a "To Do" bucket. You can rename this bucket and create as many other buckets as you need. For instance, some teams use buckets to track tasks for recurring meetings like weekly team briefs. They create a new bucket for each meeting and move tasks still outstanding from previous weeks to the new bucket, which then becomes the central focus of discussion for what needs to be done this week.

You can even use buckets to coordinate several plans within a single overarching plan. In this scenario, each plan, or sub-plan, becomes a bucket. If you remove a bucket from a plan, you also remove all the tasks in the bucket.

Tasks belong to an individual plan. You can move a task between plans in a Group or to a plan owned by another Group. Tasks are arranged for display in six ways:

- **Buckets:** This grouping allows you to view the tasks assigned to each bucket. Some people use buckets to group tasks by importance, some to divide up a project into logical pieces of work, and some to show task status by having buckets with tasks that are completed, on hold, not started, or whatever other status you would like to use.
- **Assigned to:** This grouping displays the tasks assigned to each person. By default, the view only shows tasks that are in progress or not started. You can add the completed tasks to the list by scrolling to the bottom of the list and clicking "Show Completed."
- **Progress:** This view shows tasks in the three stages supported by Planner – Not Started, In Progress, and Completed. Figure 8-3 shows this view.

- **Due date:** Tasks not started or in progress are arranged according to the date set for their completion as:
 - Late.
 - Today.
 - This week.
 - Next week.
 - Future.
 - No date.
- **Labels:** This view groups tasks into the labels (or categories) that you can assign to tasks.
- **Priority:** This view creates a virtual bucket for each of the priorities you can assign (Urgent, Important, Medium, and Low).

The screenshot shows the Microsoft Planner application interface. At the top, there's a red header bar with the title 'Planner' and a 'MAC Tasks' plan icon. Below the header, there are three main sections: 'Not started', 'In progress', and 'Completed'. Each section has a 'Add task' button. Under each section, there are several task cards. For example, in the 'Not started' section, there are two cards related to Microsoft Teams and SharePoint. In the 'In progress' section, there are two cards related to Microsoft 365 Apps and SharePoint Online. In the 'Completed' section, there are two cards related to Microsoft Defender XDR and Microsoft 365 Apps. Each card displays the task title, a small icon, and some detailed information like message ID, published date, category, and tags.

Figure 8-3: Tasks for a plan grouped by bucket

Keep in mind that, when you move a task, some of its items may not move because they remain associated with the original Group—so moving a task will currently cause it to lose its labels and comments.

When you display tasks grouped by bucket, Planner lists the tasks in order of their creation date. There is no way to select a preferred sort order such as by the due date. Buckets are primary elements of the Planner user interface. Unless you use a very wide screen, though, it is best not to have more than five or six buckets per plan; with too many buckets, the user interface becomes cluttered, and it can be difficult to find an individual task. If you think you will need to use more than six buckets to organize tasks, perhaps it is best to split them across multiple plans.

Arranging buckets: You can display the tasks for a plan in different groupings. If you use buckets to arrange tasks into segments of a plan, you can group the tasks by bucket and then drag and drop the buckets into whatever order makes sense to create an overall view of the plan. Grouping by priority is a useful feature that helps make up for the lack of a sort-by-priority option. You cannot reorder the other groupings (by progress or by assignee) in this manner.

Filtering Tasks

Because plans can span thousands of tasks, Planner supports filters for views to allow users to focus on different collections of tasks. Apart from being able to group tasks in buckets, you can filter by:

- **Due date:** Select Late, Today, This week, Next week, Future, or No date.
- **Priority:** Select Urgent, Important, Medium, or Low.
- **Progress:** Select to see all tasks with a specific state of progress.
- **Label:** Select one of the 25 labels assignable to tasks.
- **Bucket:** Select one of the buckets in the plan to see only tasks associated with that bucket.
- **Assignment:** Select a plan member to see the tasks assigned to them.

You can combine one or more values for the different filters to highlight specific tasks.

One common complaint is that it's difficult to search Planner items to find specific tasks. Filtering by keyword gives you similar results as being able to search the title field of your tasks, but there is currently no way to search tasks by labels or description.

The Grid View

The grid view shows your Planner tasks in a simple grid, rather than the board arrangement you may be more familiar with. This grid is conceptually like the grid view you're used to in Excel, Microsoft Lists, and other table-based apps: clicking in a task cell allows you to edit its value, and you can add new tasks with the provided button at the bottom of the list. In some ways this is still an early iteration-- you can't sort tasks using the column headers, and you can't multi-select or perform group operations on the items in the list. You can use the filtering mechanism described above to control which tasks Planner shows in the grid view.

The Charts View

The Charts view presents another way of looking at the tasks in a plan with the screen divided into a chart view of the complete plan and a list of selected tasks on the right-hand side of the screen. In this case, tasks are listed by bucket, but you can apply any of the filters available in Planner to display matching tasks.

With just four charts available (status, bucket, priority, and members), Planner has limited ability to present graphic views of tasks. A simple embellishment would be to allow graphs to chart information for one or more selected buckets rather than a plan. Another obvious enhancement is the addition of a timeline view as people often measure the progress of plans by date. It would be very convenient to be able to drag and drop tasks along a timeline and have their due dates adjusted to match. Microsoft has committed to considering a timeline view in the future but has said that they are unlikely to add more complex or project-oriented charts such as Gantt or burndown charts to Planner as these are more suitable for a product like Project.

The Schedule View

The Schedule view (Figure 8-4) presents open tasks in a calendar, which is a natural way for many people to think about the priority order for their work. The view is like OWA's calendar and lists all open tasks in the plan unless the view is filtered. Clicking a task reveals its full details.

Dates aren't assigned to tasks by default; if you don't assign correct dates, you won't get correct results.

You can add new tasks into the calendar or drag and drop existing tasks to assign them new due dates and put them into the proper position in the plan.

Figure 8-4: Planner's schedule view

Opening Linked Plans

If a plan has a label that says “Linked plan” under its name, that means that its content will be visible in other applications. For now, that means either Teams, SharePoint, or both. In Teams, if you add a plan as a channel tab, it becomes linked, and you’ll see it in the tab, in the Teams tasks app, and in Planner. For SharePoint, you can add a plan as a web part to any page, at which point it will be considered as linked.

Linked plans can be viewed and edited either in the Planner applications or in the linked applications. You’ll see a button labeled **Open** in the Planner menu bar (just to the left of the **Members** pulldown) that, when selected, lets you choose where to open the linked plan.

Plan Settings

The options available in the ellipsis menu [...] in the menu bar for a plan are:

- Links to other Group resources. These choices open new browser tabs.
 - **Conversations:** Opens OWA to view email conversations in the Group mailbox.
 - **Members:** Opens OWA to view Group membership. Group owners can add, modify, or remove members here.
 - **Files:** Opens the document library in the SharePoint team site belonging to the Group.
 - **Notebook:** Opens the shared OneNote notebook belonging to the Group.
 - **Sites:** Opens the home page of the SharePoint team site belonging to the Group.
- **Pin:** As with other parts of Microsoft 365, Planner lets you pin items that you want to refer to often. Pinned plans show up in a separate group in the left navigation rail. If you pin a plan, its Group also appears in the list of favorite groups in OWA or Outlook. If the plan’s already pinned, this command changes to **Unpin**.
- **Copy plan:** Creates a copy of the plan in a new Microsoft 365 Group. See details in the section below.
- **Export plan to Excel:** Creates an Excel worksheet with all the tasks in the plan. Each task occupies a single row. Once you have the plan in Excel, you can print it, combine multiple plans for analysis, or do anything else you can do with an Excel file.

- **Copy link to plan:** Copies a URL for the plan to the clipboard. The link will start with `tasks.office.com`, then include the tenant name and a unique ID for the plan (e.g. `https://tasks.office.com/redmondassociates.org/en-US/Home/PlanViews/knwuDbAxtE2A7iYVAEJ-vpYAFE4L`). When pasted into a browser, it opens the plan.
- **Plan details** are divided into three tabs:
 - **General:** Change the plan name and the background used by Planner. The backgrounds are generated automatically by the PowerPoint Designer component based on the title of the plan. Any Group member can change the plan background, and Designer does suggest different backgrounds to different people. You can't force Planner to use a specific background like a corporate logo. Group owners can also delete the plan here (the Group remains intact when a plan is removed, and other plans attached to the Group are unaffected).
 - **Group:** (only visible to Group owners) Change the display name and description of the underlying Microsoft 365 Group. If the tenant uses sensitivity labels for container management, you can select a label to apply to the Group. A label setting dictates the privacy (public or private) of the Group. If sensitivity labels are not used, the Group owner can choose the privacy setting and classification for the Group.
 - **Notifications:** Planner sends two kinds of notifications (Figure 8-5). The first type of notification is via email when tasks are assigned or completed. Only Group owners can change this setting. Individual users can choose to receive notifications when they are assigned a task and when a task assigned to them is late. Notifications for task assignments are generated when the assignment happens and are sent by email, a notification in the Teams Planner app, and using a push notification to the Planner mobile app. Late task notifications are generated by a background process and arrive only by email. Messages include a link to open Planner and interact with the relevant task.
- **Add plan to Outlook calendar:** Publishes the plan as an iCalendar feed that can be consumed by Outlook. This process is explained later.
- **Leave plan:** A member of a Group can leave a plan at any time. Group owners can't leave a Group if this action would leave the Group without an owner.

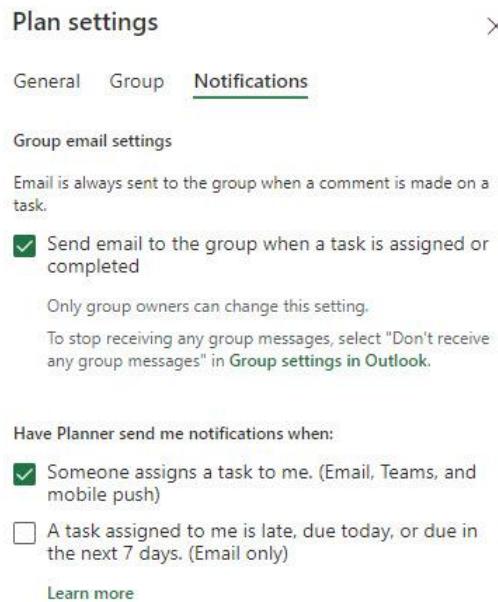


Figure 8-5: Email notification settings for a plan

You may make mistakes when setting up a plan and want to start over. A complete bucket can be selected by clicking its name and then **Delete Bucket** from the ellipsis menu. If you want to remove the complete plan, go to the ellipsis menu for the plan, select **Plan Details**, and then **Delete Plan** (see below).

Private or Public

The privacy setting assigned to its underlying Microsoft 365 Group controls whether a plan is public or private. If public, any tenant user can view plan content but cannot change it. If a non-member wants to update tasks, they must join the Group (using OWA or Teams). If the plan is private, only members have access. If you change the plan's access type, you change the access type for the underlying Group and its team (if enabled).

Copying a Plan

Copying an existing plan solves the problem where many similar projects exist in an organization, all of which have the same basic structure and need. The idea is that you can save some time by creating a template of a plan for these projects and then copying the plan to create a new plan as each new project spins up. You can copy a plan to an existing Group or create a new Group to host the copied plan. Although the choice to copy a plan is revealed to all users, only those allowed to create new Microsoft 365 Groups can create new plans (and Groups) in this manner.

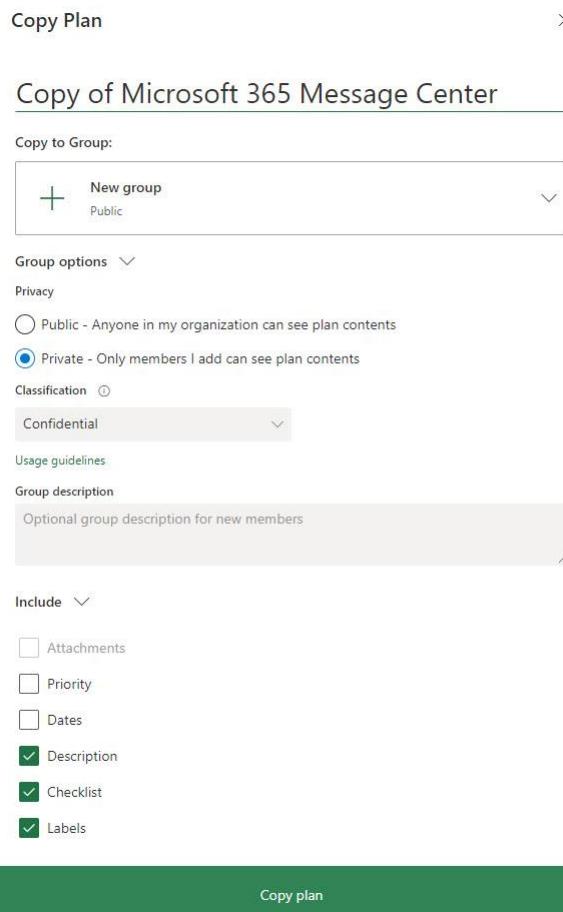


Figure 8-6: Defining details to create a copy of a plan

The **Copy plan** option is available in the ellipsis menu when a plan is open or when viewed through the Planner hub. In either case, when you copy a plan, Planner does the following:

- Copies the plan data to the selected Group. By default, the display name of the new Group is "Copy of" appended to the display name of the source plan. You can override this and compose a different display name and description before you copy the plan (or afterward). The plan's photo is not copied.
- Copies the bucket structure, label assignments, and the tasks (including the chosen details of the tasks) to the new plan.
- Sets the person who copies the plan to be the owner of the new plan (and if a new Group is created, they become the owner of the new Group). Members of the source Group are not added to the new Group, so you must add new Group members after the new plan is copied.
- Sets the privacy and classification settings to the selected values.

Figure 8-6 shows the dialog used to collect information for a plan before copying. In this case, the copy creates a new Microsoft 365 group. If your tenant uses sensitivity labels for container management, the access to the plan is set by the sensitivity label you choose.

Copying a plan creates a new plan based on the source plan's structure. The following information is not copied from the source plan:

- Task assignments, due dates, and progress (all tasks are marked "Not started").
- Comments (stored as conversations in the Group mailbox).

Copying even a very complex plan is very fast. Once Planner finishes, you can open the copied plan to complete the process of establishing the new plan by adding a description and photo, removing unwanted buckets and tasks, updating task descriptions and due dates, and assigning tasks to plan members.

Closing or Archiving a Plan

Apart from abandoning a plan, Planner doesn't include a way to close or archive a plan. No option exists to mark a plan as "done" or place it into a read-only mode. Planner doesn't support the Microsoft 365 information governance framework so you can't apply retention policies to manage completed tasks. If you want to clear out a plan before starting afresh (for instance, at the start of a new year), you must remove old tasks manually. Another approach is to create a new bucket called "Archive" and move all the completed tasks to it before starting work on the next stage of a plan.

Some organizations use the Export to Excel feature to create a monthly copy of plan data in a worksheet that is then stored in SharePoint Online. Although this is a manual process, it has the benefit of creating a snapshot of the plan when the export occurred.

Archival is not just a matter of simply moving tasks to some other repository because tasks often have associated documents and comments. This data is stored in SharePoint Online and Exchange Online. It is reasonably easy to copy the documents held in the SharePoint site belonging to the Group but more problematic to copy the conversations (comments) from the Group mailbox. Even if you write the necessary code to extract the necessary information from the Group mailbox, the challenge still exists to link everything together in a way that you can reliably rebuild a plan if needed.

Deleting Plans and Plan Data

To delete a plan, choose **Plan details** from the ellipsis menu and then **Delete this plan**. Upon confirmation, Planner removes the plan and all its tasks. Removing a plan from Planner does not remove tabs in Teams channels linked to the plan. You'll have to do this manually.

To delete the underlying Microsoft 365 Group, choose **Plan details**, then the **Group** pivot, and then **Delete this Group**. If you go ahead, the entire Microsoft 365 Group and all its provisioned resources are removed and put into a soft-deleted state. The resources might include a team, the Group mailbox, the SharePoint

Online site, the shared notebook, and so on. If you remove a Group accidentally, you can recover it using the procedure described in the Groups chapter.

When you remove a user from Entra ID, their [Planner data is not deleted](#). This is intentional, as a plan will normally be a collaborative object accessed by multiple people, and it would be rude to just wipe it out when the creator's account is removed. If you want to remove plans, tasks, or other data from Planner when a user leaves, you will have to log in with appropriate privileges and remove it manually.

Creating and Managing Tasks

Creating a new task is very straightforward. Click **Add task** and enter details of the task such as the bucket it belongs to, the due date, and the person to whom you assign the task. You can also select an existing task and copy elements of the task (such as the description, checklist, attachments, and labels) to create a new task. To copy a task, click the ellipsis [...] menu when editing the task that you want to copy, select the elements to copy, and give the copied task a new name.

A task can also be copied to another plan (even to plans owned by other groups). The person copying the task can select any plan they belong to and choose a target bucket in that plan. When a task is copied between plans, only the progress, dates, description, and checklist are copied. You'll have to assign the task after it is copied to the target plan and add attachments and labels.

Although each task must have a name, the names do not have to be unique. You can create as many tasks as you want with the same name and assign them all to the same person, which might be a little confusing. Task names can be up to 254 characters long. If you try to use a longer name, Planner trims the name back to the limit. Special characters are fully supported and a task name such as "1"£\$%^&*()_+{};:@'~#><.,?/|\\" is possible, even if it doesn't mean very much to anyone. On the upside, plenty of opportunities exists to dream up some interesting code names for tasks, especially because you can also use emoji in task titles.

Adding Tasks from Teams

Microsoft lets you quickly add a task from within Teams, which is immensely useful as a way to quickly capture things that you need to do. The "More actions" context menu for any personal or group chat message will contain a "Create task" item; when you select it, it takes the selected message text and uses it as the title of the new task. The notes for the task will contain a link to the thread. You can also create tasks from channel conversations, in which case you can select whether the task should be stored as a personal task for you or in a plan associated with one of the teams that you're a member of. Keep in mind that an individual Team may have more than one plan associated with it.

Assigning Tasks

You can assign a task to one or more people. Planner populates the drop-down list used for task assignment, with the Group membership divided into those assigned to the task and those who are not (yet). If needed, you can leave tasks unassigned until the right person is available to take on a task. As already noted, if someone leaves a Group, their tasks stay assigned to them until someone reassigns the tasks to another team member. No bulk reassignment function is available to move a set of tasks to someone else within one plan or across all plans in a tenant, such as when someone leaves the company, and the need arises for others to take over this work. For this reason, it is sensible to check whether an individual has any assigned tasks when they leave the company.

Like the other applications which use Microsoft 365 Groups to manage their membership, everyone in a Group shares equal access to the plan. Anyone can create or edit a task. Anyone can assign a task to another member or reassign a task that they have received to someone else. And they can remove a task or update the progress of a task. It's all very self-liberating and empowering if you're prepared for this mode of working.

If you need a more hierarchical form of management where only defined members can add, change, or assign tasks, then you need to use traditional project management software such as Project Online. Another option is to use [the “Project” template for SharePoint Online](#) to create a site to hold tasks for a project. Out of the box, this will not deliver the same kind of user interface that Planner provides, nor will it have the same close connection to the Group, but because it is based on SharePoint Online, it is possible to customize and organize the site to meet your requirements.

Task Notifications and Comments

When you assign a task to someone, Planner can notify them of the assignment, depending on what notification settings are in effect. By default, Planner will email a notification to the Group that the plan lives in to tell the assignee about their new task. If you use Outlook to access the Group mailbox, these notifications can serve as the starting point for conversations about the task. Any comments made about the task become part of this conversation. Planner adds the comments to the conversation in the Group mailbox and circulates copies of the comments to members who have previously commented on the task.

The comments shown on the Planner task itself are loaded from the Group mailbox and displayed on the task. The integration of the Group mailbox and the comments feature leads to some unwanted side effects. First, when a user's assigned to a task, she'll get a notification, but other changes to the task won't trigger notifications until someone posts the first comment on the task. The second is that editing the conversations in the underlying Group mailbox will change what appears on the task—if you delete comments from the mailbox, they will no longer be visible on the card.

In addition to notification emails through the Group mailbox, Planner will default to sending push notifications to the targeted user through the Planner mobile app and in Teams. Notification settings are at the plan level. You access them through the plan settings interface (click the [...] menu and select **Plan settings**). You can't control which methods are used to send notifications, but users can still turn task assignment notifications off in the Teams or Planner apps themselves, which will override the plan settings value.

Fleshing Out Task Details

Newly created tasks won't usually contain much information, just enough to be able to populate the card. This might be enough for some plans but not for others. To add more details to a task, select it to reveal the task dialog box (Figure 8-7), which allows you to view and update the task metadata. The task is relatively complete, including:

- A title describing the task.
- Progress is set to In Progress.
- Priority is set to Urgent.
- A desired end date.
- Notes describing the task.
- Any attachments added by the task creator or subsequently by the task owner.
- Planner displays “suggested attachments” at the bottom of the task card. These attachments are documents available to the task owner selected by the Microsoft Graph based on the task content.

Examples of changes you might want to make include:

- Set the expected end date for the task. As discussed earlier, the start and end dates are important if you plan to use the Schedule view to manage tasks.
- Assign a task recurrence using the “Repeat” dropdown. You can repeat tasks daily, weekly, monthly, or yearly; repeat it only during weekdays; or choose a custom recurrence pattern.
- Assign the task to Group members.
- Add more attachments.

- Add checklist items.
- Use the 25 colored labels to give a visual marker to the task. To assign a label, click Add label. You can then pick a label or give a new name to a label.
- Decide what to show on the task card.
- Mark the task as complete or in progress.
- Set a different priority.

The screenshot shows the details of a task named "Office 365 for IT Pros Update 92".

Task Details:

- Bucket:** New Notifications
- Progress:** In progress
- Priority:** Urgent
- Start date:** Start anytime
- Due date:** 01/02/2023
- Repeat:** Does not repeat

Notes: Generate PDF and EPUB versions of Office 365 for IT Pros (update #92). Update due for release to subscribers on 1 Feb 2023.

Checklist: 0 / 4

- Generate book files
- Upload PDF and EPUB to Gumroad
- Upload EPUB to Amazon
- Notify users
- Add an item

Attachments:

- <https://gum.co/O365IT/> ... Show on card
- <https://redmondassociates.share> ... Show on card

Add attachment

Comments: Type your message here

Figure 8-7: Details of a task

Microsoft previously announced, twice, that the task notes and comments fields will gain support for rich text and images, which is useful both to emphasize or highlight certain parts of a task but also when pasting notes into a task from another source. This capability depends on a new Microsoft Graph API, which is initially supported only in the Tasks app for Teams and the Planner web app. Behind the scenes, two task note fields exist: one for plain text and one for rich text. Rich text notes are converted to plain text and synced to the plain text field, but the reverse is not true; for now, if you edit the plain-text version, its changes will overwrite the contents of the rich-text version. That means if you add rich text to a task note in the Planner web client, then edit that task note on (say) the iOS version, the edits you make in iOS will overwrite the existing content and formatting in the rich text note you see in Planner. Somewhat confusingly, the web version of Planner

doesn't show any rich text controls—so you can select text and make it bold with **ctrl+B**, but there's no UI to show you that you can do that.

You cannot customize or otherwise change the metadata available for tasks. In other words, you cannot add new fields for users to complete to describe or categorize a task. This is one key advantage that Microsoft Lists offers as you can customize the fields available for the items in each list.

The task name is the default information shown in the card, but if you prefer, you can display other elements in task cards. For instance, it is often easier to pick out a specific item by scanning a list for an image, so Planner allows you to use graphic files added as attachments to tasks on the task card.

Checklist items (such as those listed in Figure 8-7) allow task owners to note activities and things to do for a task. In one way, you could consider checklist items to be sub-tasks. However, checklist items have no formal connection to the outcome of a task because you can mark a task as complete even if many checklist items are unfinished. The idea here is that a checklist item is not a formal activity to complete before a task can finish. Instead, it is a free-form reminder of something that should happen, and tasks can complete with incomplete checklists. However, to encourage a sense of achievement, Planner displays a progress bar to reflect the completion of checklist items. Also, Planner displays "confetti" (an animation) when the last checklist item is complete. Unlike comments, checklist items are part of the plan metadata and Planner doesn't generate email updates to Group members when checklists change.

You can add the following attachments to a task:

- A file from your computer. This includes files stored in any network location available to the PC, such as the OneDrive and SharePoint sites synchronized to the PC.
- A file from the SharePoint document library associated with the Group that owns the plan.
- A URL.

Planner stores the files uploaded as attachments for a task in the Documents folder of the Group document library (you cannot select a different folder). The same folder is used for attachments uploaded to tasks for any plan belonging to the Group. You cannot upload the same file twice as it would cause a duplicate file in the folder, but once you upload a file to the library, you can attach it to multiple tasks. If you try to create a link attachment that points to a link already attached to the task, Planner overwrites the original link. You can attach up to nine files or links to a task.

Task cards with graphic previews take up more screen real estate than text-only cards, but sometimes you want to highlight a specific item and a graphic can be an effective way of doing this. The task card can also display checklist items or the free-form text description of the task. You can add up to 20 checklist items to a task.

The different elements of a task show up in the user interface for the task cards too. The visual hints that you can add to cards give a quick insight into the tasks within a plan, bucket, or assigned to a specific user. A big difference exists between a card that displays a simple line of text when compared to one which uses graphics. What you add to a card in terms of comments, attachments, and checklist items help plan members understand the full context of a task, including the task owner and their progress towards completion. A lot of information about a task is therefore available at a glance.

Unlike Project, Planner tasks have no dependencies on each other. You cannot link one task to another in any way except by making sure that they are arranged in display order so that one follows another as needed. This situation is problematic for some, but it reflects the general "let's make it simple" design philosophy followed throughout Planner.

Task Status

Managing tasks effectively requires you to update task status as the work unfolds. At any time, you can mark a task status as complete or incomplete, edit the dates associated with the tasks, or add or remove new tasks. Eventually, everything will come together and all the tasks on a board will be complete. And then, when all the tasks across all boards are complete, the plan is complete.

Planner allows a task to be in just three states – not started, in progress, and completed. There is none of the precision and exactitude of measuring a task to be say 87% complete. On the other hand, the simplicity is appealing as it is easy to know whether a task has started, is being worked on, or has finished.

No Recycle Bin

Once you mark a task as completed, Planner draws a line through it and leaves the task in a completed state. You can delete the task if you want by selecting it and using the Delete option in the [...] menu. But be aware that once you delete a task it's gone for good and can't be recovered. Planner doesn't have a recycle bin and there's no way, even for Microsoft, to restore a deleted task.

Assigning Labels to Tasks

To highlight tasks, you can assign one or more of the 25 labels (sometimes called categories or tags) available for a plan. Colors (Blue, Purple, etc.) corresponding to the label color are used as the default names. Planner displays the assigned labels in the task card. Because you can use labels to group or filter tasks, they are a useful way to flag high-priority tasks or tasks that may need specific attention from someone.

You can't change the colors used for labels, but you can change the display name for labels to assign more appropriate names for the plan such as Urgent, Action, or Critical with these steps:

- Access a task.
- Select Add label to expose the current set of labels.
- Select the pencil icon alongside the label you want to change and input the new name.

Labels can be renamed using the web or mobile clients by any member of a plan. This aspect of the user interface encourages freedom of operation but seems a little odd in the context of an application designed to help people organize work. For instance, if I name the red label *Important*, I am not sure that I want someone else to rename it to *Can be ignored* without asking why the label name is currently *Important*. These customizations are specific to the individual plan.

Comments and Conversations

While the work is ongoing to complete tasks, some communication between the Group members is likely, and that's where conversations come in. Or rather, "comments" that Group members make about tasks, for this is how Planner refers to them.

As tasks are created and assigned to people, conversation items are created in the Group mailbox associated with the plan. People who choose to follow the Group Inbox receive these items in their mailbox, meaning that when you create a new plan for an existing Group that has a large set of existing subscribers, a certain amount of message traffic is likely to be generated as tasks are created, assigned, and perhaps reassigned. The email notifications help members keep track of task assignments as well as to know when tasks are complete without having to open the plan. These email notifications appear to come from the task assigner.

The text editor used for comments is rudimentary and does not support common text formatting shortcuts such as CTRL+B to bold selected words. If you want to emphasize text in comments, you will have to use another client.

The comment about task creation is one thread in the Group mailbox; the other comments form a threaded conversation for the task. Unlike task notifications, members don't receive copies of comments in email unless they have commented on a task. Members who receive comments in email can either reply directly to the message, or they can use the link embedded in the message to open Planner and go to the task and add a comment there. Posts added to the conversation through email appear as comments for the task. And, as you'd expect, if you delete a conversation, all the comments for the associated task disappear.

Behind the scenes, Planner uses the [Graph API](#) to post comments to the Group mailbox. When a user contributes to a conversation, the item is submitted through the Exchange Online transport system to apply transport rules before the comment shows up in conversations. For example, a rule might block someone from posting sensitive data such as credit card information. Another might stop the posting of any text holding an offensive term.

Printing Planner Data

Planner includes no method to print information about a plan such as a list of tasks assigned to a user or a schedule view of tasks due in the coming week. This is a much-requested feature that is partially provided by the ability to send tasks to Outlook (see below), from where users can print the information as needed. Alternatively, you can export tasks to an Excel worksheet and format and print task information from Excel.

Synchronizing Tasks to Outlook Calendars

Outlook calendar synchronization is automatically enabled for tenants with Planner as part of their subscription (to disable the feature, follow the [instructions in this article](#)). When a user wants to connect Planner to Outlook, they select **Assigned to me** in the navigation pane and click the ellipsis menu to reveal the choice to **Add "Assigned to me" to Outlook calendar**. Click the button and then select **Publish**. Planner generates an iCalendar link to the All Tasks view. The link looks something like this:

https://tasks.office.com/b662313f-14fc-43a2-9a7a-d2e27f4f3478/Calendar/User/Qi6exSZeQkC737py0An6HpYAAZ1X?t=0_95716443-a6d2-425b-a936-27fc76a889be_2018-05-10T12%3a29%3a13.4330492%2b00%3a00

Now click **Add to Outlook**. Planner launches OWA at the Calendar subscription window, copies the iCalendar link from Planner, and creates a default name for the new calendar (you can overwrite the name if you wish). By default, the calendar is created in the "Other calendars" section, but you can move it to one of the other sections. Click **Import** to continue. OWA creates a new calendar folder in the user's mailbox and synchronizes details of "Not Started" and "In Progress" tasks assigned to the user. You can't filter the tasks as the connector is configured to fetch all open tasks assigned to the user.

Synchronization is one-way from Planner to Outlook. New items do not synchronize at once because Outlook refreshes Planner data via the connector every three to four hours. You can't force synchronization to happen. The information synchronized to the calendar for a task includes:

- **Date:** Planner items are scheduled for all-day calendar slots as Planner bases task assignments on days rather than hours. If a task has a due date, the calendar item is scheduled for that day. If it has both start and due dates, the item is scheduled for that period.
- **Location:** None added as Planner does not capture this data.
- **Progress:** The status of the task in Planner.
- **Checklist:** A note about how many checklist items exist and are complete.

Calendar entries created through the connector do not tell you what plan or bucket within a plan a task belongs to, but each entry has a link to Planner to bring the user back to the original task, where whatever changes are necessary can be made. Changes are then synchronized back to Outlook. Although the user cannot edit details of the planner task, they can add a reminder to a task.

If you prefer not to use the iCalendar connector, you can also link Outlook to Planner using [several standard Power Automate templates](#) published by Microsoft. Power Automate is good at inserting items into a calendar. It is less successful at tracking changes made to tasks such as completing tasks or synchronizing changes made to a task like changing its name, due date, or status. This is probably because the [set of triggers](#) supported by Planner for the connector available to Power Automate only covers task creation, assignment, and completion, and not task updates.

Working with Planner Tasks in To Do

The To Do clients will show you all your assigned tasks from all plans. That is, the To Do category labeled *Assigned to Me* will include Planner tasks in shared plans or your own plans. There's bi-directional synchronization support so some actions performed in To Do will propagate to Planner. You can:

- Update the completion date for the task.
- Mark a task as completed or incomplete (but not mark a task as in progress).
- Add checklist items.
- Update the task description.
- Hide completed tasks.

You must enable this integration from the To Do client; there's currently no way to do so from within the Planner interface. Open the settings page for your To Do client (the exact location will depend on whether you're using Windows, the web, or macOS), then find the "Connected apps" section, then toggle the "Tasks assigned to you" control.

You can't change assignees, add attachments, or change the tabs for tasks from within To Do. You also can't create new tasks. However, an Open in Planner link is available to open the task in Planner if a user needs to perform one of these actions.

Using Planner Offline

The Planner iOS client can display tasks when offline but cannot update anything unless the client is connected. However, the Planner browser app includes more extensive offline capability. While you can't connect to Planner without a network connection, if the connection becomes unavailable during a session, you can continue working with tasks. When offline, you can:

- Add a new task to a plan.
- Update task properties like progress (not started, completed), start and due dates, notes, comments, and priority.
- Add or remove a web link or file attachment.
- Add or remove checklist items for a task.
- Move tasks between buckets.
- Assign tasks to team members.

You cannot:

- Start Planner when offline.
- Add a SharePoint item to a task.
- Create a new plan for an existing Group or with a new Group.

Using the cached data, Planner charts and the schedule view are both available when offline. When the network link is restored, Planner synchronizes any changes made offline to the server.

Planner and Guest Users

Planner supports the Azure B2B Collaboration model for guest access. As explained in the Groups chapter, to join a Group, external users receive and redeem an invitation. During the redemption process, if the external user doesn't already have a guest account, Entra ID creates one for them in the tenant directory. The same membership as used for Microsoft 365 Groups and Teams controls access to Planner, and a guest can be added to a Group through Outlook or Teams. Once a guest user becomes a member, their membership automatically allows access to the plans associated with the Group, including any plans created in channels belonging to a team. If a guest user already exists in the tenant directory, an owner can add them to a plan by assigning them a task.

To access Planner, guest users must specify the service domain for the tenant to which they want to connect. Planner can't switch guests between tenants, so the connection is always to a specific tenant. For example, to access plans in the office365itpros.com tenant, a guest connects to the URL

<https://tasks.office.com/office365itpros.onmicrosoft.com>. If you're already signed into Planner in your browser, you should use a private browser session to connect to Planner in another tenant. After successful authentication, the Planner browser client displays the set of plans available to the guest. These plans include those created before Planner supported external access.

Planner displays a restricted user interface to guest users by removing choices they cannot use. Guests can create, assign, and edit tasks, change task status, post comments, add checklist items and even update a plan's background. However, guests cannot create new plans because they cannot create new Microsoft 365 Groups. Likewise, they cannot remove a plan. Guests can edit a plan's name, but they cannot change other plan settings, like its privacy level (which a sensitivity label might control). Finally, guests cannot browse the host tenant to look for plans (and Groups) to join.

Using Planner in Teams

Microsoft has integrated Planner (and the underlying task data) with several other Microsoft 365 services.

Planner, Tasks, and Teams

Teams can be used with Planner in most enterprise, government, and education plans. One point to consider during any implementation that includes frontline workers is that Teams is available for frontline (F1) licenses while Planner is not.

Teams and Planner share two points of integration. First, a user can open the Planner app to access all their tasks, including personal tasks created in Outlook or To Do and tasks assigned to them through their membership in a team or Group. The Planner app for Teams and continues the [overall Microsoft strategy](#) of providing multiple endpoints for creating and managing tasks that all end up working against the same data store.

The second point of integration is when Planner is added through a channel tab to access the tasks in a plan belonging to a team. We'll discuss this method shortly.

Planner in Teams

The Planner app in Teams delivers an integrated view of personal and team tasks. Its functionality is still quite limited compared to the Planner web app. For example, as of July 2024, the Teams app can't show you the members of a plan whilst you're viewing it, and it doesn't allow editing of all the same items that can be edited in the web application.

As shown in Figure 8-8, the current release of the Planner app divides tasks into:

- **My Day:** this view summarizes your tasks that are due during the current day, plus any tasks you chose to add to the view.
- **My Tasks:** this view shows your personal (not shared with anyone else) and include tasks created in Planner, Planner Premium, To Do, and Outlook, as well as any organizational tasks published to you. Pivots at the top of the view let you see private tasks, tasks assigned to you, and flagged emails.
- **My Plans:** this list contains the To Do lists, basic plans, and premium plans that the user has access to.

The screenshot shows the Microsoft Planner 'My Tasks' page. At the top, there are filters: 'All' (selected), 'Private tasks', 'Assigned to me', and 'Flagged emails'. Below the filters are columns: 'Title', 'Plan', 'Due date', 'Priority', 'Progress', and 'Quick look'. A red box highlights the 'Due date' column header. The table lists various tasks, each with a small icon, the task title, the plan it belongs to, its due date (e.g., '6/15/2024'), its priority (e.g., 'Medium'), its progress status (e.g., 'Completed', 'Not started', 'In progress'), and a 'Quick look' button.

Title	Plan	Due date	Priority	Progress	Quick look
Tony: A couple of questions; Please?	Flagged Emails		Medium	Completed	1
Please review your Azure billing statement for MVP he...	Flagged Emails		Medium	Not started	1
Ticket Number : 13195822	Flagged Emails		Medium	Not started	1
Update 1099s	Private Tasks		! Important	Not started	
Get updated sponsor chapter	Private Tasks	6/15/2024	Medium	Not started	
[Exchange Online, Microsoft 365 Apps, Microsoft 365 ...	MT MAC Tasks		Medium	Not started	
[Microsoft Copilot (Microsoft 365)] Updates to Securi...	MT MAC Tasks		Medium	Not started	
[Microsoft Copilot (Microsoft 365)] Microsoft Copilot f...	MT MAC Tasks		Medium	Not started	
[Microsoft Viva] Microsoft Viva Insights: Delegate acce...	MT MAC Tasks		Medium	Not started	
[Microsoft 365 suite, Microsoft Purview] Endpoint Dat...	MT MAC Tasks		Medium	Not started	
[Microsoft 365 suite] Microsoft Purview Generative A...	MT MAC Tasks		Medium	Not started	
[Microsoft 365 suite] Product transitions to the cloud...	MT MAC Tasks		Medium	Not started	
[Microsoft Viva] (Updated) Managing Microsoft Viva E...	MT MAC Tasks		Medium	In progress	
[Microsoft 365 Apps] (Updated) Microsoft Outlook for...	MT MAC Tasks		Medium	In progress	
[Microsoft Teams] (Updated) Microsoft Teams: Access ...	MT MAC Tasks		Medium	In progress	
[Microsoft 365 suite, Microsoft Copilot (Microsoft 365...)	MT MAC Tasks		Medium	In progress	
[Microsoft 365 suite] (Updated) Microsoft 365 admin ...	MT MAC Tasks		Medium	In progress	

Figure 8-8: Planner and To Do Tasks are available in the Planner app for Teams

Working with a task happens in the same way as in the web app and Teams writes any changes made through the app back to the native repository using Graph APIs. Due to the need to refresh client-side caches, a slight delay occurs before the change appears in the native app, but this shouldn't be a problem because people don't usually rush to check To Do or Planner after updating a task in Teams. One minor difference between the Planner browser app and the app in Teams is that Teams doesn't send email notifications about task updates or closures. Instead, status changes for tasks (such as someone assigning a task to you, or a task being marked as complete) appear as Teams notifications.

Accessing Plans Through Teams Channel Tabs

Sometimes people need to concentrate on work items belonging to a single plan. This is best accomplished by adding a Planner tab to a team channel. As it turns out, according to Microsoft's telemetry, Planner is the most popular channel tab in Teams.

If a plan hasn't already been created for the underlying Group, Teams creates it and attaches the plan to the tab. If one or more plans already exist for the Group, you can select one and attach it to the tab. You can then work with the tasks in the plan through Teams or click the **Go to website** (globe) icon in the set of options at the top right-hand corner of the pane. This launches Planner and loads the tasks for the plan into a browser tab.

Tasks in the Teams Feed

When someone assigns a task to a user, the user will see that assignment in the Teams activity feed. Starting in April 2023, in organizations that use [task publishing](#), when someone publishes an urgent task using the task publishing feature, the owner and members of the team that the task is assigned to will see the notification in their activity feed too.

Removing a Plan from a Channel

To remove a plan accessed through a channel tab, open the plan, select the arrow next to the tab, and then **Remove**. You now have a choice:

- **Remove the plan from Teams:** This is the default and leaves the plan accessible through the Planner browser interface. If needed, you can add the plan back to Teams.
- **Permanently remove the plan:** To do this, select the checkbox *Permanently delete this plan and all its tasks*. This removes the plan data from the Planner Azure service. The plan is then irrecoverable through any interface.

Unlike removing a plan through the Planner browser interface, removing a plan through Teams does not affect the Group or any other resource attached to the Group or team.

Using Planner Premium

Planner Premium is Microsoft's attempt to merge Planner (originally meant for lightweight task management) with the more capable parts of Project for the web. Users with a Planner Premium license get access to several additional project management features:

- A timeline view for seeing when tasks begin and end, including support for dependencies between tasks and the ability to see tasks on the critical path.
- Goals that can be linked to tasks. That is, you can define a goal and then have tasks that represent actions that must be taken to reach the goal; as the actions are completed, the goal progress updates.
- A "people view" that shows tasks assigned to specific team members. This is prettier than, but conceptually very similar to, using the board view in the Planner web app, then selecting **Group by bucket > Assigned to**.
- The ability to assign tasks to sprints, useful for projects that are using a methodology (such as Agile) that focuses on sprints.
- Copilot features for asking questions about tasks or instructing Copilot to take actions on tasks.
- Task-linked conversations, so that you can have a Teams conversation tied specifically to a task. If you have ever wanted to use @-mentions in comments on Planner items, this is Microsoft's answer to that desire.
- Revision history for task changes, showing changes such as editing the effort duration, adding or removing attachments, or changing labels assigned to a task.
- Custom fields in tasks.
- The ability to create summary tasks that have subtasks.

Many of these features are taken directly from the Project family, but many of them also exist in competing project management tools such as Monday or Trello. Microsoft allows users to start their own self-service trials of the Planner Premium license (unless you block them from doing so; see Chapter 4) but it remains to be seen whether organizations will be willing to buy a premium license to add these capabilities to their users.

Chapter 9: Managing Video

Paul Robichaux

Given the proliferation of consumer video-sharing apps like YouTube and the preference of some users to consume information through videos, the role of video communications within businesses is growing. It is undeniable that many people are more accustomed to and prefer to learn from short-form videos than from reading memos and reports. Stream is Microsoft's enterprise video service; it allows users to upload, view, and share videos securely. Stream's role in Microsoft 365 is to enable the best possible playback of video and audio content stored by Microsoft 365 apps in SharePoint Online and OneDrive for Business.

Stream Architecture and Management

Stream is included in all enterprise plans (including DoD, GCC, and GCC High), the education plans, and the front-line worker plans. It is also included in the Business and Business Premium plans. See [this page](#) for more licensing information. The Stream functionality available to Office 365 E3 and E5 tenants includes advanced features like speech-to-text transcript and caption generation, support for closed captioning, and search support.

Stream Stores Data in SharePoint

Stream uses SharePoint Online and OneDrive for Business (ODSP) to store and manage video files. This arrangement ensures that:

- Video content is stored according to Microsoft's [data residency commitments](#).
- Video content and transcripts are included in information governance (retention) and information protection policies.
- Transcripts of Teams meeting recordings are searchable in eDiscovery cases.
- Standard SharePoint Online external access and sharing controls provide consistent access control for external users.
- Backups and archives for SharePoint Online and OneDrive for Business includes videos.
- Video content is available through the Graph API.
- Programmable access to video content through the Graph API.

Stream on SharePoint doesn't have a Stream portal in the same way that Stream classic or the older Office 365 Video application did. Recordings are individually accessible and shareable. Instead, if you want to have a video portal (for example, to allow access to videos about the business), you'll need to take a different approach. You could:

- Build a SharePoint site tailored to highlight and feature selected videos.
- Create a channel in a team dedicated to video sharing.
- Publish organization videos through [Viva Learning](#).
- Use a Viva Engage community to disseminate videos.

Stream Building Blocks

Like many other Microsoft 365 apps, Stream uses components from across Microsoft 365 and contributes functionality to other apps. Examples of how Stream integrates with other applications and services include:

- Stream stores videos in the SharePoint Online sites, including those managed by Microsoft 365 groups and used by applications such as Viva Engage and Teams.

- Users can copy links for Stream videos generated by the Stream browser app and paste the link into Teams chats and channel conversations. When accessed, the video plays inline without any need to open a browser. Playback includes access to video comments, transcript, and chapters.
- Viva Engage can also playback Stream videos inline.
- The SharePoint web part for Stream can highlight a video or set of videos on a page.
- [Forms can collect feedback](#) through quizzes, polls, and surveys for videos through the *Interactivity* tab for a video. This functionality is only available in the classic client.

Other apps can use [Stream's implementation of oEmbed](#) to display videos or channels.

Stream Storage Quotas

The classic version of Stream had a separate quota for video storage; the current version uses the tenant's existing quotas. The storage consumed by video files is charged:

- For videos stored in SharePoint Online (for example, videos generated and shared in Teams channels): The file size is charged against the tenant storage quota for SharePoint.
- For videos stored in OneDrive for Business: The file size is charged against the storage quota for the owner's OneDrive for Business account. Files generated for Teams meeting recordings are stored in OneDrive for Business if the meeting is personal.

OneDrive for Business offers an [initial 5 TB of storage for Microsoft 365 accounts](#). This amount can be increased by making a request to Microsoft Support. The impact of storing Teams meeting recordings is moderated by the application of an automatic expiration policy. Videos expire after 120 days unless the video owner overrides the expiration period by changing it (or removing the expiration) or applying a retention label to the file. Upon expiration, video files follow the normal OneDrive for Business recycle process.

The exact size of a video file depends on its format, quality, and length. As a guide, expect to use approximately 7.5 MB per minute of 1080p MP4 video with smaller amounts consumed for lower-quality video (the storage required per minute doesn't vary for Teams meeting recordings saved to One Drive for Business). Stream counts the original file size of the uploaded video against the quota and doesn't take other factors such as the size of transcoded videos and caption files into account.

The original implementation of Stream on SharePoint used the standard ODSP versioning mechanism, meaning that any change to video metadata would create a new version of the file. Microsoft has changed this behavior. Changes to the chapters, transcripts, or transcript settings no longer cause Stream to create a new version, if you make those changes within the Stream app itself. Changes to audio tracks, the video title or description, or changes to the column metadata for the video file from within SharePoint will still create new versions. Of course, changing the video itself (e.g. by adding a title graphic or trimming video from the beginning or end) will still create a new version, however. You can use the version trimming controls described in the SharePoint chapter to remove old versions of Stream files to reduce your overall storage usage in SharePoint.

The Stream Client

Stream itself only has a browser-based client, which supports video upload and viewing through a wide range of browsers, including Microsoft Edge and the current versions of Chrome, Brave, and Safari. Microsoft used to make iOS and Android mobile apps for Stream but deprecated those apps in July 2024 in favor of the built-in video viewer included in the OneDrive and Microsoft 365 mobile apps.

The Stream browser app is a composite of a browser interface ([stream.office.com](#), aka the "Stream start page") to manage videos and the standard OneDrive web audio and video player page (the Stream player) to play

videos and control their settings. The Stream start page and the player operate separately now, and Microsoft's stated direction is to create a much better connection between the two components over time.

The Stream player is used for video playback in Microsoft 365 apps, including the OneDrive and SharePoint browser clients and the Teams and Viva Engage apps. The Stream browser app uses Microsoft Search to find and display videos stored in Microsoft 365 apps, including those stored as attachments in user mailboxes. The information a user sees may include:

- Teams meeting recordings (both the user's recordings and those shared with the user).
- Videos uploaded by the user using the Stream browser app (or OneDrive for Business). This includes video files uploaded through applications like Viva Engage and Teams.
- Videos shared by other users.
- Video file attachments for emails found in the user's Exchange Online mailbox.
- Stories (short videos) created using the Viva Engage app.
- Videos created using the recording facilities (camera or screen) available in the Stream browser app.

The Stream client supports a wide range of features to manage video files. The only feature that was in the old client that's not available today is the ability to replace a video with another file. Although Stream includes a basic trim function to hide content in a video, but sometimes a video needs more post-production work to iron out imperfections, add titles, or improve the flow. Video owners can download a video, process it with a video editor like TechSmith Camtasia or Clipchamp for Work, and upload the updated version. However, editing a video creates a new file, which will be uploaded separately and thus have a different link. The ability to replace a video is important because this retains the link used for the original video and avoids the need to replace it in places like Teams channel tabs or SharePoint pages.

Managing Stream

The Stream browser app doesn't include any controls for administrative settings. The standard ODSP and Microsoft 365 settings provide administrative control for sharing, storage quotas, recovery of videos for deleted users, and retention. The ability to organize videos through Microsoft 365 Groups by storing videos in the SharePoint team site belonging to the groups is still there, even if a dedicated GUI to perform group-based video management is unavailable.

Controlling Automatic Transcript Generation

Stream automatically generates transcripts for videos uploaded to SharePoint Online using applications like Stream or Viva Engage. Two criteria must be satisfied for automatic transcript generation:

- The language set for the video must be supported by Stream for transcript generation.
- The SharePoint Online tenant-wide *MediaTranscriptionAutomaticFeatures* setting must be *Enabled* (this is the default value).

To disable automatic transcript generation, connect to SharePoint Online with PowerShell and run the *Set-SPOTenant* cmdlet:

```
Set-SPOTenant -MediaTranscriptionAutomaticFeatures Disabled
```

It can take several hours before SharePoint Online ceases automatic transcript generation.

Managing Stream Network Demand

Like any video application, Stream benefits from good network performance between servers and clients. Microsoft publishes articles to help administrators understand the characteristics of network performance for Stream, including video delivery and network overview.

Audit Events for Stream

Videos are processed just like any other file stored in a SharePoint site or OneDrive account, so the [audit events you'll see for Stream](#) video creation, modification, access, and deletion are identical to similar events for other SharePoint Online activities.

You can search audit data with the audit log search feature in the Microsoft Purview Compliance portal or using the PowerShell `Search-UnifiedAuditLog` cmdlet. The Auditing and Reporting chapter explains how to search using either method, but for illustration purposes, the code below shows how to search the audit log and return the count of videos upload and modification actions by individual users.

When a client uploads a video, it initially creates a file with a ~tmp prefix. For example, ~tmp7C_Microsoft 365 Track.mp4. A *FileUploaded* event captures this action. Stream processes the video, updates its settings, and renames the file (in the example above, the renamed file is Microsoft 365 Track.mp4). These actions generate two *FileModified* audit events. One logged for the video owner (rename the file), the other for app@sharepoint (update the video settings). One issue in Stream using the general-purpose events generated by SharePoint Online is that Stream activities are usually a small percentage of the overall set of audit events found by a search. For instance, SharePoint Online and OneDrive for Business generate many *FileModified* and *FileAccessed* events as users work with Office documents, especially if the AutoSave feature is used as this can generate multiple events when saving files periodically during a session.

[This script](#) retrieves the audit records logged for several SharePoint events, extracts the Stream events from the set, and reports them.

In addition to the general-purpose file events, several Stream-specific events are available such as actions logged for transcript creation, deletion, and access and for comment creation and deletion. This code finds those audit records.

```
$StartDate = (Get-Date).AddDays(-30); $EndDate = Get-Date
$Operations = "FileTranscriptContentAccessed", "FileTranscriptCreated", "FileTranscriptDeleted"
[array]$Records = (Search-UnifiedAuditLog -Operations $Operations -StartDate $StartDate -EndDate
$EndDate -Formatted -ResultSize 5000 -SessionCommand ReturnLargeSet)
$Records = $Records | Sort-Object Identity -Unique
```

Controlling Comments on Videos

Stream videos stored in OneDrive or SharePoint support the ability for users to comment on their content. Although users typically receive view-only permission for video and audio files, Stream makes an exception to allow users to post comments via a button included in the set of overlaid options available during video playback. People with edit permission for a video can remove comments or prevent the posting of comments by updating video settings.

Apart from the per-video control over comments, organizations can remove the ability for people with view-only permission to post comments through a tenant setting. To do this, run the `Set-SPOTenant` cmdlet from the SharePoint Online module and change the value of *ViewersCanCommentOnMediaDisabled* from the default (False) to True:

```
Set-SPOTenant -ViewersCanCommentOnMediaDisabled $True
```

Stream Information Protection

As you'll read in the compliance chapter, Microsoft has been on a journey to apply its compliance tools equally across all data types and workloads. Video content is more difficult for automated systems to interpret than documents, email, and so on, so the range of information protection controls applicable to Stream is smaller than for other data types. Here's the current state of Microsoft's information protection tools as applied to videos:

- Communications compliance: currently you cannot use Microsoft's [communications compliance tools](#) on video files, although Microsoft has a [roadmap item for using these tools](#) to monitor video content based on the content of the associated transcript. However, this feature will only work for Teams meetings, not for other video files.
- eDiscovery: Stream videos can be located, played back, and exported as part of eDiscovery processing. Administrators can identify and gather video files by searching specific locations in SharePoint or OneDrive, or by performing keyword searches against video titles, descriptions, chapters, or transcripts.
- Sensitivity labels are not yet supported for videos.
- Data loss prevention rules can find terms in the title, transcript, or video metadata; any DLP matches will trigger a tooltip in SharePoint or OneDrive where the video's displayed and may also trigger other actions, depending on how the DLP rule is written.

Managing Stream and Teams

Teams uses Stream to support several features:

- Recording of Teams meetings.
- Publishing Stream videos via a channel tab.
- Recording Teams Town Hall Events. After the end of a live event, the video stream automatically transitions from a live feed to an on-demand recording. The recording is available online and accessible to attendees and other users for 180 days. If the organizer of a live event wants to keep the recording for longer, they must download the video and upload it to Stream.

Managing Teams Meeting Recordings

Users can record Teams chats (including group chats and VOIP and PSTN calls), channel meetings, ad-hoc ("meet now") meetings, and Teams Town Hall events (see above). The organizer and participants of Teams meetings can record meetings if the Teams meeting policy assigned to their accounts enables recordings. Teams considers the person who starts a recording to be the owner of the recording file generated by Teams. Meeting organizers can update the options for individual meetings so that a recording starts automatically when a meeting commences (the first person with the presenter or owner role joins the call).

Important video settings in the Teams meeting policy include:

- **AllowCloudRecording:** Controls if the meeting organizer and presenters can record a meeting.
- **AllowTranscription:** Controls if the meeting organizer and presents can generate a meeting transcript.
- **ExplicitRecordingConsent:** Controls if participants in meetings created by a user must give explicit consent for recording. If they do not, Teams disables their microphone, camera, and ability to share information in the meeting.
- **NewMeetingRecordingExpirationDays:** Sets the number of days Teams keeps recordings for before deleting the files.

Transcript generation was originally available only for meetings held in U.S. English (or rather, meetings detected by Teams as being in U.S. English). Today, Teams supports an expanded range of languages for live caption and transcript generation including English, German, French, Italian, Spanish, Russian, Hindi, Arabic, Finnish, Danish, Swedish, Japanese, Korean, Chinese, and Dutch. In addition, Microsoft offers pay-as-you-go translation services for several dozen additional languages, [as described here](#). Holders of Teams Premium licenses can see when their name is mentioned in a transcribed recording and go to those points in the timeline. Teams personalizes these mentions so that a user can only see their mentions.

When Teams records a meeting, the service adds a bot to the call to capture the voice and video stream from participants (even if the meeting is voice-only). Recordings use a 3x3 view (the last nine speakers). Once the meeting ends or the recording is halted, the SharePoint app (app@sharepoint) creates the recording as an .MP4 file as follows:

- For **personal meetings**: in the Recordings folder of the OneDrive for Business account of the meeting organizer.
- For **channel meetings**: in the Recordings folder for the channel in the SharePoint document library belonging to the team. For example, General\Recordings. The exception is for meetings in private channels. The *ChannelRecordingDownload* setting in the Teams meeting policy assigned to user accounts controls if channel members can download recordings for meetings held in shared and standard channels. The default is *Allow*, meaning that channel members can download recordings just like any other file stored in the channel site. To block channel members from downloading recordings, update the setting to *Block*. Thereafter, when people who are assigned a meetings policy with channel recordings blocked record meetings, the SharePoint app creates the MP4 file in the *Recordings\View Only* folder. In addition, SharePoint limits full access rights for the folder to channel owners (or team owners for standard channels). Channel members receive read access without the ability to download. Even the organizers of channel meetings are blocked from downloading recordings of their meetings when the *ChannelRecordingDownload* setting in the meeting policy assigned to their accounts is *Block*. Updating the *ChannelRecordingDownload* setting is not supported by the Teams admin center and can only be done using PowerShell. Here are examples of updating a Teams meeting policy to block download access for channel meeting recordings and granting the policy to a user account:

```
Set-CsTeamsMeetingPolicy -Identity "Allow Meeting Recording" -ChannelRecordingDownload Block
```

```
Grant-CsTeamsMeetingPolicy -PolicyName "Allow Meeting Recording" -Identity
Ken.Bowers@office365itpros.com
```

- For **one-to-one calls and group chats**: the Recordings folder of the OneDrive for Business account of the person who records the meeting.

If the meeting is left active, the recording ceases after four hours. Access rights for recordings stored in OneDrive for Business do not include external meeting participants, including guest accounts. If external access is needed for a recording, the owner must grant access.

Teams also posts a link to the recording in the meeting chat or channel. The MP4 file can be edited or processed by whatever tools are available to trim or otherwise adjust the recording. If available, meeting transcripts are available in the same place.

Different processing rules apply to the recordings of one-to-one calls. These meetings can only be recorded if both participants use Teams clients and the meeting policy assigned to the person who schedules the meeting to allow them to record the meeting. Recordings are unsupported if one of the participants uses a dial-in number or connections through federation (external access). It's also important to understand that only participants from the host tenant have (read) access to the recordings by default. External participants, including guest users, cannot access the recording unless the meeting organizer shares the recording with them. Table 9-1 summarizes how meeting participants can access Teams meeting recordings.

Type of meeting	Who can view recording	Access to recording
Group chat	All chat participants from the host tenant.	Recording posted in meeting chat and in the OneDrive for Business account of the person who starts the recording.
Private or ad-hoc meeting	All participants from the host tenant.	Recording posted in the meeting chat and in the OneDrive for Business account of the person who

		schedules the meeting. The recording is also available in the meeting recap. Meeting participants from the same tenant have read-only access rights to the recording. External participants, including guest accounts, must be assigned permission to access the recording.
Channel meeting	Members of the team owning the channel.	Recording posted in the meeting chat in the channel and the Recording folder of the channel folder in the SharePoint site belonging to the team.
One-to-one meeting	Both participants (if in the same tenant).	Recording posted in the chat and in the OneDrive for Business account of the person who schedules the meeting. The other party has read-only access if they have a tenant account.
VOIP and PSTN calls	Call owner.	Recording and transcript are available in the call history and call details.

Table 9-1: Access to Teams recordings

No matter how a recording is made, only the owner can download or remove the video. The owner can upload the recording to Stream if they wish to share the content to a wider audience (except externally, as Stream doesn't support this type of sharing).

Sharing Permissions in OneDrive: Permissions to access meeting recordings stored in OneDrive are limited to internal users, even if guests participate in the call. If it is necessary to share a recording with an external user, the meeting owner must update the sharing list to include that user. Channel recordings stored in SharePoint can be accessed by any team member. Another thing to remember is that only the owner can download the recording from OneDrive. Other participants in personal meetings receive view-only permission and are blocked from downloading.

Managing Call Recordings for VoIP and PSTN Calls

Teams users who place calls to VOIP or PSTN recipients can record the call and generate a transcript if the calling policy assigned to their accounts have the following settings enabled:

- *AllowCloudRecordingForCalls*: Controls if the user can record PSTN and VOIP calls. By default, the setting is True.
- *AllowTranscriptionForCalling*: Controls if the user can generate a transcript of a call. By default, the setting is False.

For example, to update the default Teams calling policy to allow users to record calls and generate transcripts, the command is:

```
Set-CsTeamsCallingPolicy -Identity Global -AllowCloudRecordingForCalls $True  
-AllowTranscriptionForCalling $True
```

Meeting recordings are stored in the OneDrive for Business account of the user who starts the recording and is available with the transcript in the call history and call details.

Managing Teams Recording Retention

Most recordings of Teams meetings age rapidly. Time and activities overtake the matters discussed and the value of the recording diminishes over time. For this reason, many organizations want to remove Teams meeting recordings sooner than other content. Microsoft has committed to delivering a special retention policy to process Teams meeting recordings which can be used by all tenants with Teams licenses. This feature isn't yet available, so for now only tenants with the necessary Office 365 E5 or Microsoft 365 E5 compliance licenses can create an auto-label policy to apply retention labels to the recording files stored in SharePoint.

Online and OneDrive for Business. Alternatively, if you don't have the licenses for auto-label policies, you can train users to apply retention labels manually.

Background labeling processes find content identified by policy criteria (a keyword query, sensitive information type, or trainable classifier). In the case of Teams meeting recordings, a keyword query of (*ProgID:Media AND ProgID:Meeting*) locates the MP4 files. These are programmable identifiers set on recordings when Teams creates the files. You can test the effectiveness of the query by using it with SharePoint search to find Teams meeting recordings available to you.

When specifying the locations covered by the policy, make sure that you include all the locations where recordings might be found:

- OneDrive for Business (personal meetings).
- Microsoft 365 Groups (channel meetings). This includes the SharePoint sites connected to teams.
- SharePoint Online. This covers any copies of recordings moved from the SharePoint sites connected to teams.

When the auto-label policy matches the query against a file, it applies the retention label specified in the policy settings. The retention period in the label dictates how long the recording remains in place. Once the retention period (say, six months) lapses for recordings, background processes remove the files. See the Compliance chapter for more information about retention policies and labels.

Compliance administrators can track auto-label activity through the Activity Explorer in the Microsoft 365 compliance center. Another way to check the progress of auto-labeling is to run the PowerShell script [downloadable from GitHub](#) to report the recording files which receive a retention label together with information about how long it takes auto-labeling to happen after the creation of recordings.

Auto-Expiration of Teams Meeting Recordings

Microsoft says that 96% of Teams meeting recordings are not rewatched 60 days after the original meeting and 99% are not watched after 110 days. To help preserve storage quota, Teams marks an auto-expiration date on each recording. Unlike retention labels, which need Office 365 E3 or above, auto-expiration works for all SKUs which include Teams.

Originally, Teams used a 60-day retention period. Following customer feedback, Microsoft increased this to 120 days, which is the expiration period for recordings created by enterprise users. Recordings for users with Office 365 A1 licenses have a 30-day retention period. It doesn't matter if the recording is in SharePoint Online or OneDrive for Business. Users can change the expiration period for individual recordings by updating file properties through the file details pane (selecting preset values of 14, 30, or 60 days, a custom date, or *Never Expire*). Organizations can set a default expiration period for newly created recordings using the Teams meeting policy assigned to user accounts. The auto-expiration settings are managed by updating meeting policies in the Teams admin center. Alternatively, you can use PowerShell. For example, to set the default expiration period for recordings of meetings made by people assigned the *VIP User Meeting Policy*, run the command:

```
Set-CsTeamsMeetingPolicy -Identity "VIP User Meeting Policy" -NewMeetingRecordingExpirationDays 180
```

The minimum retention period is one day, and the maximum is 99,999 days (which should be enough for anyone). You can also set retention to -1, meaning that recordings of team meetings never expire. The expiration period for A1 users can only be reduced from the default 30 days.

Background processes run to evaluate recordings and check their expiration date. If the process detects an expired file, the process moves the file into the recycle bin and clears the expiration date field. Users receive email notifications when expired recordings move into the recycle bin. If necessary, they can rescue important

recordings from the recycle bin for up to 90 days after deletion. Once moved back from the recycle bin, the recording has no expiration date set and will therefore not be evaluated for deletion again.

To help users understand when a recording approaches expiration will see visual indications in:

- Beside the link to the meeting recording in the meeting chat. Anyone with view access to the recording sees the expiration notice.
- Two weeks before expiration, a red icon appears beside the MP4 files for files in the Recordings folder of OneDrive for Business accounts (personal meetings) or SharePoint Online sites (channel meetings).

Auto-expiration applies only to new recordings. Existing recordings do not have an expiration period. Auto-expiration is only available for meeting recordings and cannot be used with other file types held in OneDrive for Business and SharePoint Online.

If you move a file with an expiration date to another site, the expiration date stays with the file and remains active. Copying a file creates a new file without an expiration date. The same applies if you download a meeting recording and then upload it to a different site to create a new file.

Microsoft Purview retention labels that retain items for a set period take precedence over auto-expiration. In other words, if a recording has a retention label, that's what governs how it is kept (or removed). SharePoint Online evaluates retention labels that remove content differently because the shortest deletion date takes precedence. For instance, if a user assigns a recording a retention label that mandates deletion after a year and the Teams expiration date is 120 days, SharePoint Online removes the recording after 120 days. The user can recover the recording and the retention label settings will then apply, meaning that SharePoint Online deletes the recording after another 245 days (365-120).

For this reason, you should assign retention labels with retention periods to keep important recordings if you want to make sure that SharePoint Online will not remove recordings after the Teams-specified expiration period expires.

Using Stream

Stream's user functionality divides into these major sections:

- Uploading and creating video content (recording through screen captures or a workstation camera).
- Managing videos.
- Video playback.

The Stream browser app (Figure 9-1) uses the same design "language" as other Microsoft 365 apps. At the top of the client, the recommended list of videos contains files that you've worked with, recently watched, or those that Stream believes are of interest. Filters control the videos shown beneath the recommended set, including filters to find videos marked by the user as favorites, recordings of Teams meetings, or videos shared with other people. If the selected filter is set to All, Stream displays the full set of videos available to the user in Microsoft 365 locations, including any found in email attachments. The videos include those that the user owns and those that they can access because of access gained through a sharing link, Teams chat, or direct access.

No matter how someone accesses Stream content, Stream won't show them a video unless their account has the right to view it.

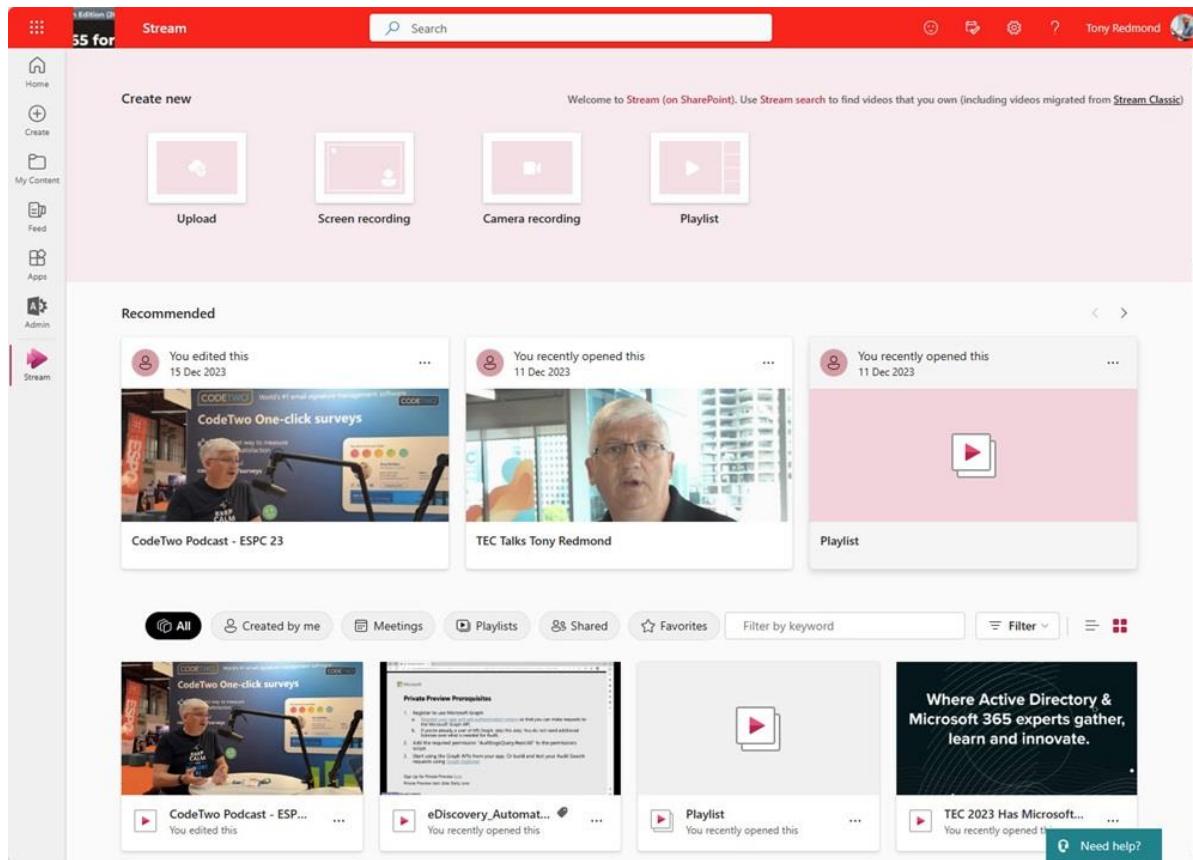


Figure 9-1: The Stream browser app

User Settings

The user settings available for the Stream browser app are minimal. Currently, they are limited to selecting a theme and deciding whether to use dark mode.

Uploading and Accessing Videos

To upload a video, click the upload link and select the source files (in the [supported file formats](#) – audio-only files are not supported). You can also drag and drop a file to the client. A newly-uploaded video receives the default permission in the target site or account. Recordings of Teams channel meetings are available to team members while recordings of Teams personal calls are available to the participants.

After uploading a video, the owner can:

- Play the video.
- Open the location of the video. This option opens a new browser tab positioned in the OneDrive or SharePoint folder where the file is located.
- Share the video via email, a link that you generate and share using other means, or to a Teams user, chat, or channel. The generated link can block users from downloading the video content.
- Create a new calendar meeting and include the link to the video in the meeting notes. Stream uses the OWA meeting request screen to compose the meeting invitation. Make sure that the recipients of the invitation have access to the video. The client uses meeting insights to highlight videos sent in meeting invitations before the event occurs to give the user the chance to review the content beforehand.
- Add a link to the video to To-Do. This action creates a bare-bones personal task in To Do.
- Mark the video as a favorite. This adds the video to the set listed through the Favorites link.

- Tag the video by adding a user-defined label (with a color) to the video. The colored tag is displayed in the list of videos and the tag name is revealed by hovering over the tag. To manage tags (remove, update the color, change the name), go to the [My Content page](#). This page also reveals tagged files.
- Hide the video. The Stream client doesn't show the video in its list.
- Download a copy of the video.
- Delete the video.

Opening a video with the Stream video player allows the owner to manage some settings for the video (Figure 9-2). People who watch the video use the same player, but they can't change the settings.

The options to interact with videos are available in an item in an overlaid menu on the video player. Options might be restricted depending on the permissions available to a user when they view a video. For example, someone with view-only permission can only see the transcript, analytics, and comments. The full set of menu items are:

- **Video settings:** Opens a pane to allow the video owner to turn on different options.
- **Transcript:** Opens a pane to show the transcript (and chapter markers, if used).
- **Analytics:** Displays view statistics for the video. Interactivity statistics are also available.
- **Comments:** Opens a pane to show any comments posted for the video. Stream uses the same commenting facilities available for Office documents stored in ODSP.
- **Copilot:** If the user has a Microsoft 365 Copilot license, Copilot can access the video transcript to perform actions such as summarizing what happened in the meeting or the action items assigned in the meeting.
- **Trim:** Remove some content from view. Unlike other trim mechanisms, Stream does not remove data from the video. Instead, it hides content between two timecodes.
- **Interactivity:** Add a callout or Microsoft form at specific timecodes during a video.

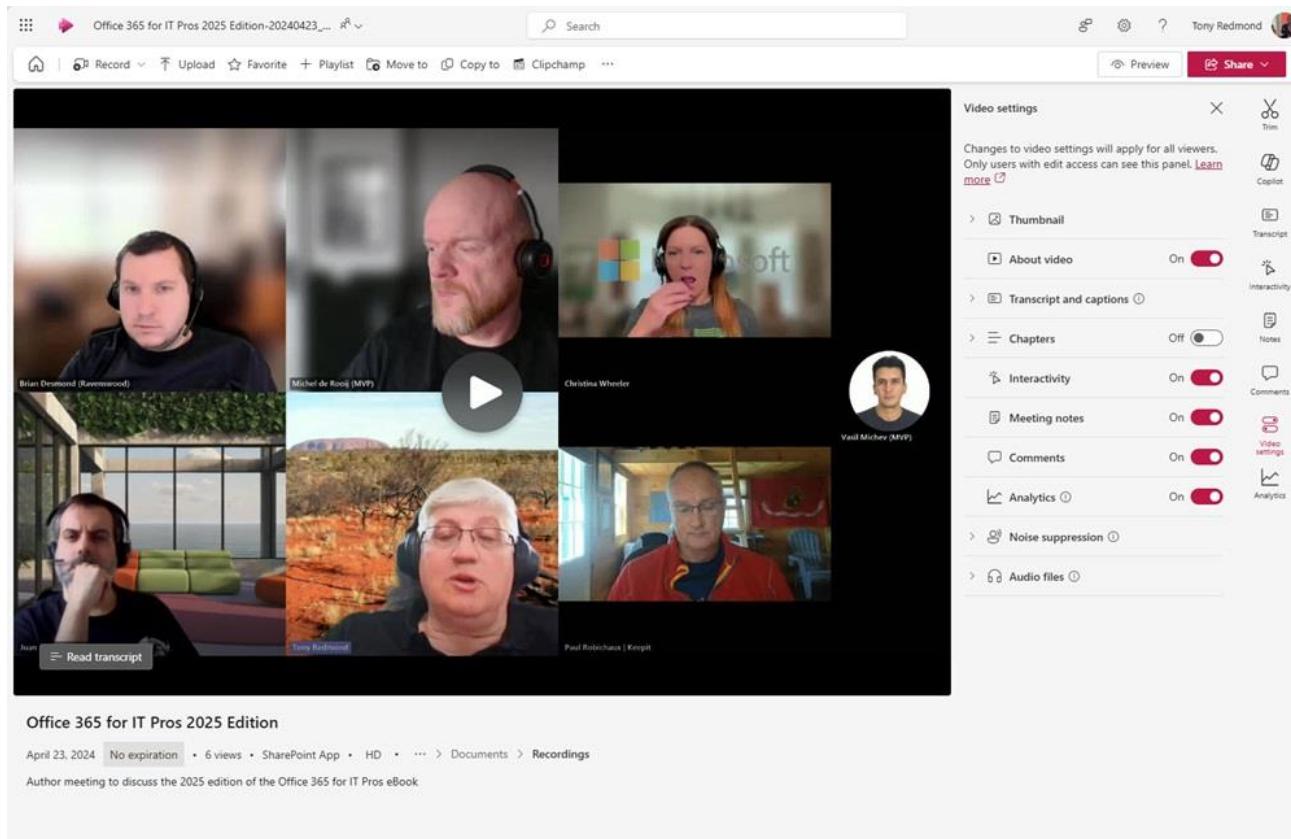


Figure 9-2: Options available in the Stream video player

The video settings are:

- **Thumbnail:** Select a frame from the video to use as the thumbnail displayed for the video by the Stream client. To select a frame, move the pointer in the seekbar (the time bar under the video) to select an appropriate frame.
- **About video:** Controls if any information is available for display to users when they watch the video. The text entered about a video is indexed and discoverable using SharePoint search. It's a good idea to include information about a video such as the time and place of the recording, important parts of the video, and perhaps some hyperlinks for users to find more information about the topic.
- **Transcript and captions:** Originally, Stream did not generate captions or a transcript for uploaded videos unless the owner requests a transcript. From June 2023, Stream automatically generates a transcript.
- **Chapters:** To help organize videos, creators can insert chapter markers in files to help users navigate within a video to find the information they're interested in. If the owner enables chapter markers, Stream displays the markers in the timeline shown by the player. See [this article](#) for more information.
- **Analytics:** See above...
- **Noise suppression:** Users can enable noise suppression if they want when playing a video. This control affects if noise suppression is the default for a video. It should be turned on if significant background noise is present.
- **Interactivity:** See above.
- **Comments:** Viewers can add comments to a video to create a discussion about its content. The Office commenting system is used.
- **Audio files:** Upload audio descriptions or language voiceovers that viewers can choose during playback.

Recording a Video with Stream

The Stream client supports the recording of videos of up to 15 minutes in length using the cameras available to the workstation (including software cameras like OBS VirtualCam) or a screen recording. Videos can record using any camera available to the workstation. To record a new video:

- Select either Camera recording or screen recording. This launches a new browser tab with the Stream camera.
- Add whatever video effects that you want to enhance the image. You can add a backdrop like those used in Teams meetings, including the ability to upload a custom backdrop or use background blur. You can also add text to the image.
- Click the record button. Stream starts a 3-second countdown and then begins to record.
- To finish recording, click the stop button and then Next. Stream allows you to review the captured video to decide if you want to keep the video. If you do, click Publish.
- Stream writes the video in [WebM format](#) into the top-level folder of the user's OneDrive for Business account. You can't choose another destination folder to use as the default for new videos, but you can move the video once it's in OneDrive.
- Edit the video properties to adjust settings such as adding a transcript, allowing comments, and so on. It's best to update the video to replace the default date-based name with something more descriptive.
- Share the video with other people.

Figure 9-3 shows a Stream video recording in progress. The backdrop is from a photo overlaid the user's image. You can drag and drop the user image to wherever you like on the slide (Stream includes quick keys to position the image to the left, right, and center), and you can resize the image too.

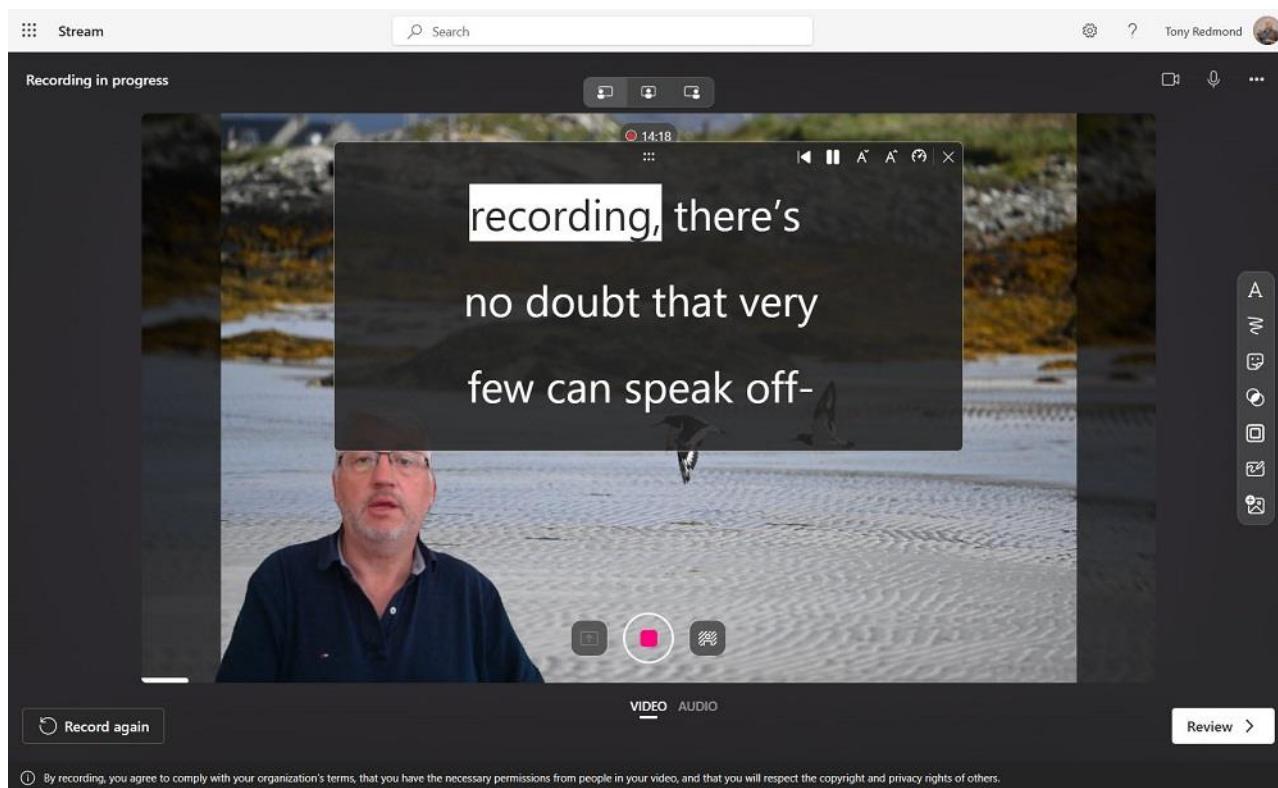


Figure 9-3: Recording a Stream video with the teleprompter turned on

The most important element in the picture is the teleprompter, which supports the timed playback of text input directly or copied from a source. The idea is that people deliver more confidently and require fewer retakes when they see the text they need to deliver in front of them. The teleprompter comes with a speed control to slow down or speed up the display of the words. The Interactivity option allows video creators to add hyperlinks, text callouts, and quizzes and surveys generated by Microsoft Forms to Stream videos by editing videos and inserting information at whatever timecode is most appropriate.

Microsoft 365 enterprise SKUs include Clipchamp for Work (the Office 365 enterprise SKUs do not include Clipchamp for Work), a version of the consumer product acquired by Microsoft in 2021. Clipchamp supports features like single sign-on and uses SharePoint Online and OneDrive for Business to store video files. Clipchamp is a very capable video editor that includes many filters, effects, transitions and functions for video postprocessing. Users with access to Clipchamp see a Clipchamp option in the menu bar. Clicking the option copies the video to Clipchamp for processing. When the edits are complete, you can export the video back to Stream. This creates a new version of the video, with new analytics, links, and so on. As noted earlier, it's not possible to replace a video and keep links, etc. intact.

Other Ways to Get Video Content into Stream

Apart from recording a new video with the Stream or Clipchamp apps, other ways exist for users to add video content to Stream, including:

- Mobile apps such as the OneDrive or Microsoft 365 apps.
- Recording a Teams meeting.
- Uploading a video file to a Teams chat or Viva Engage conversation.
- Uploading a file to OneDrive for Business or SharePoint Online that originates from some other source.
- Recording or playing back videos directly inside compatible apps. For example, you can record and play back videos inline within Outlook on the web and New Outlook.

In all cases, after a video is uploaded, Stream processes it to create the playback files, captions, and transcript. Stream generates automatic transcripts for uploaded videos. Transcripts include attribution, meaning that the text spoken by an individual is attributed to them as indicated by their initials or thumbnail photo.

Sharing Stream Videos

Because the new Stream stores its files in ODSP, sharing a video is very much like sharing any other SharePoint or OneDrive file. To share a video, select a video and select Share from the [...] menu to expose the following sharing mechanisms:

- **Email.** ODSP generates a sharing link and inserts it into an email addressed to the link recipients. The sharing link settings control what the recipients can do with the video. For instance, the settings can block downloads. Recipients of the sharing link can be inside or outside the organization.
- **Copy link.** The user can copy the sharing link to the clipboard and share the link elsewhere as needed. For example, you can create a Teams channel tab to point to a specific video. Make sure that the permissions set on the link allow the intended audience to access the file.
- **Teams.** ODSP uses the Share to Teams feature to post the link to the video to a personal chat, group chat, or channel. This is the only method supported to share a video file stored in a user mailbox. The process is the same as that used to share an item from Outlook to Teams (see the Teams chapter).

If you want to start a video playback at a specific point, you can add an instruction to the link. For example, this instruction tells Stream to start the video at the 180 second mark.

```
&nav={"playbackOptions":{"startTimeInSeconds":180}}
```

For instance, a link containing the instruction for a video stored in a user's OneDrive for Business account might look like this:

```
https://office365itpros-my.sharepoint.com/:v/g/personal/james_ryan_office365itpros.com/ETbXnV4vB-pMsfV9LK81d9MBtTS9KQiBnZaHNq9LxcrfMQ?e=qoCLkw&nav={"playbackOptions":{"startTimeInSeconds":180}}
```

When sharing a video, you can use the "Can view, but not download" option in the sharing dialog to prevent users who access the video from downloading it.

Playlists

Playlists are another way to share videos. A playlist is a personal list created in the user's OneDrive for Business account and managed using the Microsoft Lists app. Playlists are accessible through the Lists app or through Stream where they appear in the list of video and audio files.

When someone creates a playlist, they add video or audio files (from locations that they can access) stored in OneDrive for Business and SharePoint Online to the list. After building the list, they can then create a sharing link for the list and send it to whomever they wish to see the videos. Adding a video to a playlist does not update the sharing settings for the file. To make sure that the recipients of the sharing link can play the videos, the owner must update the sharing settings to permit access.

Transcripts

A video transcript is made up of individual timecoded captions in Web Video Text Tracks, or WebVTT (VTT) format. For videos recorded in any of its [supported languages](#), Stream generates a transcript by interpreting the voice track to create captions along with the corresponding timecode. For example, here are three segments from an English language transcript.

```
00:00:26.645 --> 00:00:30.965  
We'll talk about it. I  
have my viewpoint on it as well.
```

```

00:00:30.965 --> 00:00:35.015
OK, OK, so let's get things
going and what we might want to
00:00:35.015 --> 00:00:39.335
do is then if we can just take
some of the snippets out of this.

```

Stream offers the choice of downloading a transcript in VTT format (like shown above) or as a Word (docx) file. The latter is easier to work with if you want to edit the transcript to clarify places where the AI misunderstood what people said, or to add extra detail such as a link to reference sources.

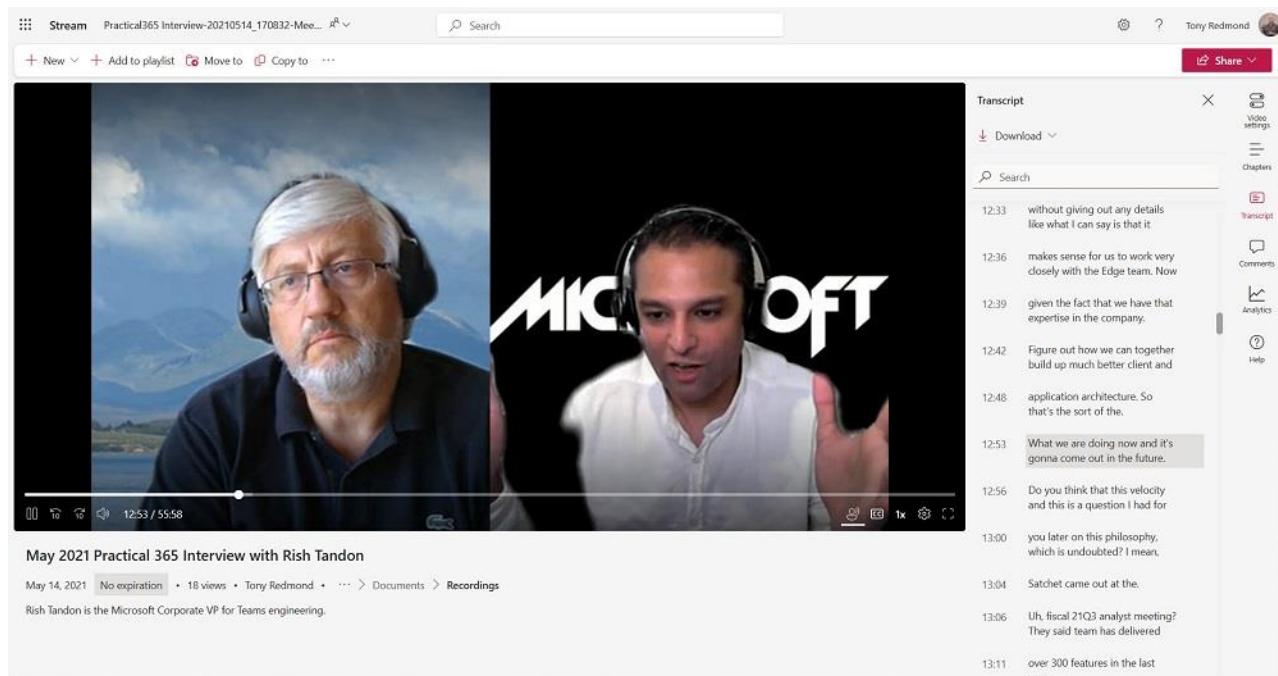


Figure 9-4: Playing a Stream video with its transcript

Figure 9-4 shows the transcript for a video as displayed in the Stream viewer. You can see how the individual captions appear in the transcript. Selecting a caption repositions the player at that point in the video. Stream displays the same text under the video when the user enables closed captions. Stream supports transcript searches to allow viewers to find and jump to a location in a video.

Transcript generation is available for videos with a maximum size of 4 GB (professional high-definition videos longer than 20 minutes or so can easily exceed this size). Being able to create and view an automatic transcript is very helpful, and users with Microsoft 365 Copilot licenses can interrogate the transcript to ask Copilot to summarize what happens in the video, locate the discussion of a specific topic, generate a set of action items, or report the contribution of a video participant on a certain point.

Generally, Stream does a reasonable job of interpreting the spoken words in a video. However, the nature of automatic text generation is that it can always do with a little help. If you want to improve the quality (accuracy) of the captions, you can either edit the transcript online (use the edit button that appears when you hover over a transcript entry), or you can:

- Download the transcript file and amend it with any text editor. Unless you use a VTT editor ([here's a free online example](#)), don't edit the time codes – just the text.
- Delete the existing transcript.
- Upload the amended file.

You can fix misunderstood words, add speaker attribution, or include other details that might be useful to the watcher. Editing a transcript online is a good way to fix obvious errors; downloading and reviewing the complete transcript is a better approach when the need exists to ensure the highest quality transcript.

Noise Suppression

Noise suppression isolates speech from background noise in the audio feed to make it clearer and more distinct. Video owners can enable noise suppression by editing the properties of specific videos. When noise suppression is enabled, viewers have the option to keep noise suppression on or disable it during video playback.

Most videos qualify to be processed for noise suppression. The criteria include:

- The video is two hours or shorter, and no larger than 3 GB.
- An audio track is available, but not when multiple audio tracks in different languages exist in a video.
- The video is not a recording of a Teams meeting. This is because noise suppression is automatically done when Teams meetings are recorded.

Noise suppression is not available for recordings of Live Events. You can't disable noise suppression on a tenant-wide level.

Viewership Statistics

When people view videos using the web player, Microsoft 365 captures statistics to help video owners understand how engaged viewers are with the content. Not everyone watches a video from end to end, and it can be important to know what parts of a video attract the most engagement or where viewers begin to drop off. To see the viewership statistics for a video, use the Analytics link in the video properties. You'll see the number of views per week, who viewed the video, and its ability to retain viewers (Figure 9-5) over time.

Viewership retention is different from the number of viewers. If someone opens a video at any point, they count as part of the total viewership. Retention depends on how many of the total viewers saw a specific point in the video. To make it easy for video owners to understand the effectiveness of getting their message across, Stream superimposes analytics on the screen to show the retention of users as the video progresses. For instance, Figure 9-5 reports that 75% of the viewership saw the video at the 25-second mark with a gradual tail-off of interest thereafter.

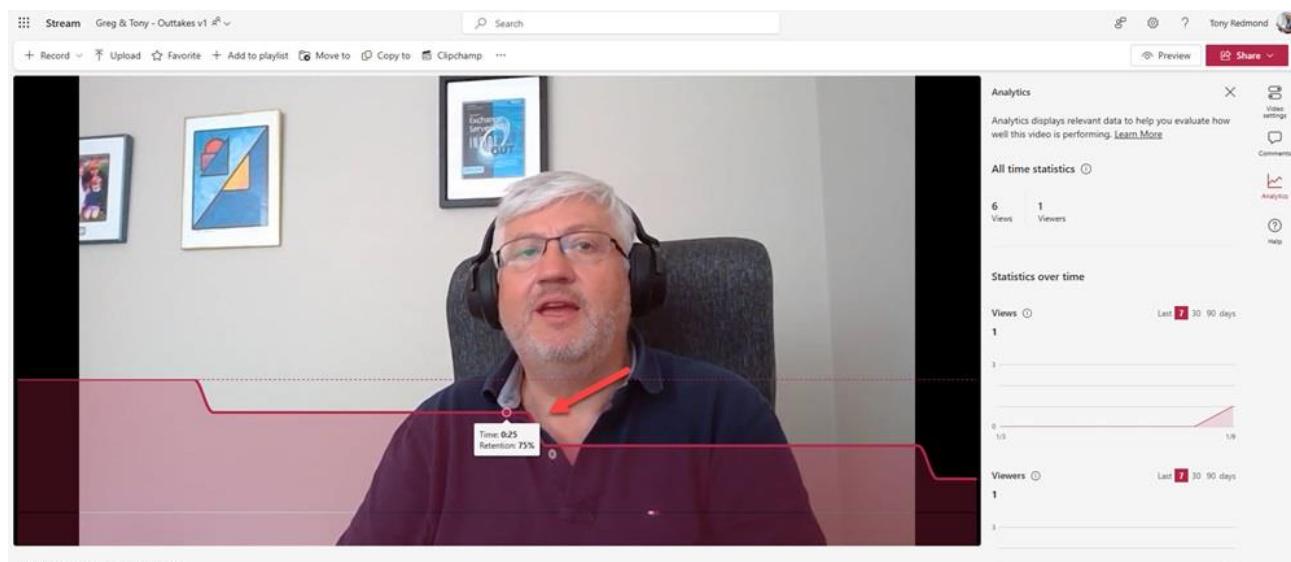


Figure 9-5: Displaying viewer retention statistics for a video

The number of views includes “rewatches,” or occasions when someone goes back and reviews a part of a video again. The statistics include these events when someone goes back to a part of a video during a viewing session. Usually (as seen in this case), viewership drops off toward the end of a video but it’s more unusual to see a dip at the start. This is probably caused by people skipping ahead to avoid the opening credits. The viewership chart aggregates data for the entire lifetime of a video: you cannot choose to view data for specific periods.

Viewership data is tied to a specific version of a file. If you edit a video and upload the new content to Stream, statistics accrue for that version and don’t inherit the data for the older video. Stream adjusts the data points in the time chart depending on a video’s duration. If a video is short (under 200 seconds), a data point appears for each second. For longer videos, Stream adjusts the graph by aggregating data over longer periods. For example, a 10-minute video uses 3-second data points.

Video Trimming

The Stream player supports the ability to trim videos in a very specific manner: instead of removing parts of a video from the start, end, or middle, Stream hides content based on time codes. For example, you can tell Stream to hide the first fifteen seconds of a Teams meeting recording to avoid viewers having to watch the Teams recording introduction screen. Stream stores details of the trimmed sections in the video metadata. Trimming a video in this manner avoids the need to regenerate an edited video without the trimmed sections. When the time comes to play the video, Stream simply ignores the trimmed sections.

Hidden content is always available to video owners and others with full access. The trimmed sections are viewable if someone downloads and plays a copy of the video. In addition, trimming doesn’t affect the transcript and although Stream doesn’t display the parts of the transcript for trimmed section, the full text is available for eDiscovery and for Copilot to process. For these reasons, if you want a video where it is impossible for viewers to access removed content, use a tool like Clipchamp to regenerate a new version of the video after removing the parts you don’t want people to see. Stream should then produce a transcript for the new video that reflects the edited content.

Video Interactivity

The interactivity feature of the Stream player supports the addition of elements at specific time codes within a video. You can add:

1. **Forms.** Insert a link to a Microsoft form (created beforehand) for display to viewers starting at a timecode. A form can conduct a survey, poll viewers, or quiz the viewers about the content of the video.
2. **Callouts.** Add a callout containing simple text (including emojis), a hyperlink, or both to display in a colored box to viewers between two timecodes. This feature is used to highlight important points in a video. The callout text editor is rudimentary and supports the selection of a limited range of colors. When you add a callout, the Stream editor will attempt to suggest relevant documents from Microsoft 365. You can insert multiple callouts in a video.

You can see statistics about the number of unique viewers and the percentage of viewers that used interactive elements. Given the usefulness of being able to add interactive elements to a video, it’s reasonable to expect that Microsoft will add new elements to this feature over time.

Searching Teams Meeting Transcripts

When Teams generates a transcript for a meeting, it stores the transcript along with the meeting recording in the OneDrive for Business account of the meeting organizer (private meetings) or the SharePoint Online site

(for channel meetings). When the Stream player displays a meeting recording, the transcript appears in a separate pane. This process is the same as happens when someone uploads a video to Stream.

Microsoft Search indexes the spoken words from the transcript to make it possible for users to search based on words spoken during meetings. Transcripts can be searched from any application that offers access to Microsoft Search, including SharePoint Online search or in OneDrive for Business. In both cases, the search is scoped to only reveal words from meetings the user is entitled to access. Including spoken words from meetings in Microsoft Search indexes also means the data is available for eDiscovery searches.

Including Stream in a Teams Channel Tab

To make it easy for people to find videos, team owners and administrators can create channel tabs to connect to a video. To create the connection, enter the URL (retrieved with the Share option in Stream or from the browser address bar) for the video into the Teams dialog screen. The tab name is set to be the name of the video, but you can rename the tab if necessary.

Chapter 10: Managing Groups

Tony Redmond

Microsoft has used different names for modern groups since their introduction in November 2014, including Office 365 Groups, Outlook Groups, Groups in Outlook, and now [Microsoft 365 Groups](#). To simplify matters, we use “Groups” unless we need to refer specifically to another type of group found within Microsoft 365, such as a mail-enabled security group.

Groups started out with the intention of delivering a “better distribution list” for the email-centric community. Today, the most important role for Groups is in membership management. Teams is the best example of a Microsoft 365 app that uses Groups for membership management. Planner is another.

An Identity and Membership Service

The basic idea behind Groups is to bring people, information, and applications together to enable better communication and collaboration. We can summarize how Groups work in three steps:

1. Users create and manage groups using their client of choice. The client depends on the purpose for which they want to use the group. For instance, if they believe that group members prefer to communicate via email, they should create the group with Outlook. If they prefer using chat or threaded conversations, they might choose Teams.
2. The new group object exists in both Entra ID and Exchange Online. Entra ID is the *system of record* and is responsible for synchronizing information about the new group to other workloads across Microsoft 365 (for example, Planner and SharePoint Online) to make those applications aware that a new group is available. In some respects, because both types of group control access to resources, you can think of a Microsoft 365 group as having some of the same characteristics as a security group. The big difference is that a workload must recognize Groups as a valid security mechanism before Groups can control access to resources.
The Exchange Online directory holds email-related information about Microsoft 365 Groups, including their proxy addresses. When you use Exchange clients or cmdlets from the Exchange Online PowerShell module to update Groups, a dual-write mechanism commits the updates simultaneously in Entra ID and Exchange Online. Following a successful update, Entra ID synchronizes the changes with other application directories.
3. Group members select the tools they need to get work done from the range of applications that support Groups. For example, a team might choose to connect a plan via a channel tab.

We will explore how these steps work in practice through the rest of this chapter.

Applications that use Microsoft 365 Groups

A wide range of Microsoft 365 applications uses Groups as a membership service. Table 10-1 lists some of the major applications which use the Groups service.

Group	Focus	Storage
Outlook	Email-based conversations within public or private groups. Limited to “more than” 1,000 members. Dynamic membership supported.	Exchange Online mailbox

Microsoft Teams	Personal chats and channel-based conversations. The membership limit for an individual team is 25,000.	Azure Cosmos DB
Microsoft Planner	Task-based plans used by public or private teams. Shares the same limit as Teams.	Azure data service
Viva Engage (Yammer) Communities	Open, idea sharing, collaboration at scale. The membership limit for these groups is up to 50K if synchronized to an on-premises AD and higher if not.	Viva Engage
SharePoint sites	Structured document and information management.	SharePoint
Stream	Controls access to video content in the Microsoft Stream service.	Stream (moving to OneDrive for Business and SharePoint Online)
Power BI	Controls access to workspaces.	Power BI

Table 10-1: The various kinds of groups available within Microsoft 365

The only real limit for groups is imposed by [Entra ID](#), where “any number of objects can be members of a single group,” or, if you synchronize with an on-premises directory, an Entra ID group object is limited to 50,000 members.

Core Principles

Figure 10-1 illustrates how three core principles combine to form the architecture of Microsoft 365 Groups. These are:

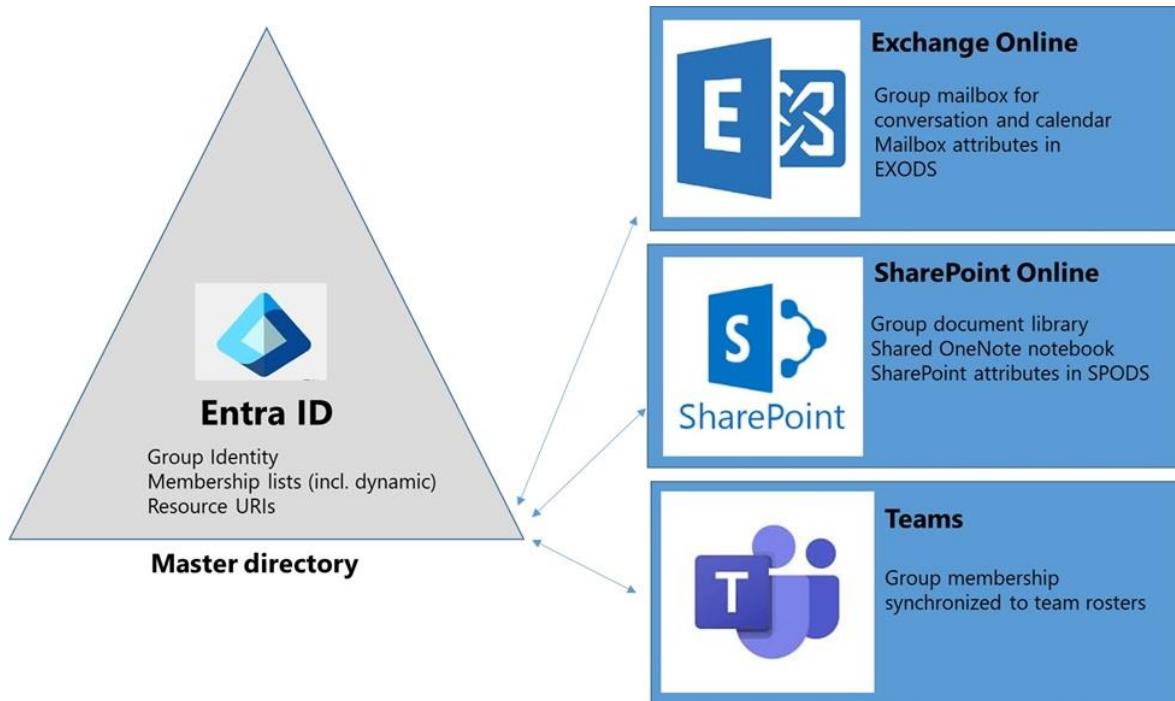


Figure 10-1: The loosely coupled Groups architecture

Entra ID is the directory of record. When you create a new group, two writes occur in tandem. The first is to Entra ID to create the object that becomes the definitive identity for the new group. The second is to the EXODS directory to create the group mailbox. This process ensures that the new group can begin to function immediately. After Exchange Online creates the new group mailbox, it updates the group object in Entra ID with information such as its email address. Provisioning processes create other components like the SharePoint Online document library and the shared OneNote notebook.

Entra ID propagates information about group properties and members using a “forward synchronization” process to the directories used by individual applications to enable those applications to recognize and respect the membership of groups. For instance, if a user updates the membership of a group using OWA, writes occur to update the membership information held in Entra ID and EXODS. Notifications occur to make other group-enabled applications aware of the change. You can think of group membership as a form of “access all areas” pass that is valid for access to all the resources available to the group.

Although notifications are the primary mechanism used to inform workloads of changes to which they should respond, applications might not respond at once to the notifications as they might have other items to process. The forward synchronization process, which runs in the background on a timed basis, acts as a backstop by making sure that all workloads apply any outstanding updates consistently. The focus of the synchronization process is scale rather than immediacy. In other words, a change might take one or two minutes (or sometimes much longer, depending on the load on the service) before replication fully occurs across all directories. Although the change might not be immediate, it will happen. This is important because as more applications use Groups as a membership service, the interaction between those applications and Entra ID becomes more complex. Typically, if an application has a separate directory (like Exchange Online), the application updates both directories and relies on synchronization to spread the change to other workloads.

Viewed in the context of Entra ID, Microsoft 365 groups are mail-enabled groups that have members and owners. Groups can optionally be security-enabled. The Groups service manages membership for apps like Teams and Planner and therefore controls access to the resources available through these apps, some compare Groups to security groups (in the loosest sense).

Federated resources are drawn from multiple applications. Microsoft 365 spans a growing set of applications, each of which delivers specific functionality. Each application controls its data stores. Federation allows Microsoft to select from the functionality available in existing applications and expose that functionality to users through new applications and their clients. Thus, a group has the following components:

- A mailbox to store threaded conversations from Exchange Online. The Microsoft 365 substrate uses the group mailbox for other purposes, such as holding compliance records generated for other apps, including Teams and Planner. The group mailbox includes a shared calendar, which Teams uses for both the team and channel calendars.
- A SharePoint Online team site, including a document library to allow group users to share documents and other files.
- A shared OneNote Online notebook. The notebook is in the Site Assets document library of the SharePoint site.
- Other applications can add components to the mix. For example, Teams adds several Azure-based data services to hold its conversations, chats, and graphics.

A Viva Engage community uses similar components, with the difference being that the group mailbox holds only compliance and substrate data. When Teams creates a group, members communicate through chats and only use the group mailbox for the calendar. Stream uses groups to control what videos are available to group members. Likewise, Power BI can use a group to control the workspaces that are available to users.

The single identity for the group means that members automatically gain access to all the application resources available to the group to create an integrated end-to-end user experience across Microsoft 365. Federation allows Microsoft to introduce new applications to Microsoft 365 more easily and with less disruption to other applications than would be the case if each application depends on its resources. Members of the group can then use whatever functionality is available in an application. The functionality and its data remain under the control of each application.

Loose coupling with groups and applications. Apart from their dependency on membership and identity services, applications that use Groups to manage their membership operate independently of each other. Applications are aware of each other because they share the common linkage through Groups and respect the common identity represented by a group. When changes occur in an application, other applications become aware of the changes through a synchronization process. For example, if a user creates a new group with Outlook, the notification signaled from Entra ID to Exchange Online forces the provisioning of a new group mailbox to hold group conversations and the calendar. The presence of a new group object in Entra ID makes SharePoint Online aware that some work is necessary to update itself when someone tries to use the new group.

The fact that a group has a single identity with a single set of permissions is a major part of the value of Groups. It means that groups can act as a means of access to different Microsoft 365 applications, which is how applications like [Forms](#) and Power BI use Groups. Forms, for instance, uses Groups as the way to share forms between users in what it calls "Group forms." Because a group is a single identity, when members join a group, they gain access to all the components available to that group with the same rights to the content as other members. If you need to implement granular access to information, you should use whatever mechanisms are in individual applications rather than trying to transform the team identity of a group into a set of individual custom permissions.

Groups Basics

Before we examine the details of how Groups work, we should first consider some of the basic ideas behind how Microsoft views these objects and how this affects their evolution as a major Microsoft 365 component. Here are some of those ideas:

A focus on self-service: Microsoft wants Groups to be easy for users to set up on an on-demand basis. By default, anyone can create a new group (as we will discuss later, you can control this through settings in the Entra ID Groups policy). Users creating objects that consume system resources without oversight fly in the face of traditional IT practices where IT exerts control over what a user can and cannot do. The idea is that by making groups easy to create, users can collaborate as they see fit and work together in ad-hoc or formal teams. Remember that resources are more abundant inside Microsoft 365 than is the case in most on-premises deployments, so a reduced focus on the need to control resources is an understandable position to take.

Private by default: Originally, Microsoft made groups public by default to encourage people to join and take part in as many groups as possible. It seemed like a good idea in 2015. After several years, the experience of deployments and customer feedback moved Microsoft to believe that groups should be private by default. The change aligns Groups with Teams as both apps use private as the default access type. It has the side effect of making groups less discoverable, but it is easy to set a group to be public after creation if you want to follow the original philosophy.

Simple permissions: The history of IT is full of stories about people getting into trouble with permissions. Either they do not have the right permissions to do the job, or their account has permissions that are unnecessary, which means that the user ends up accessing data that they should not. Once a user is a member of a group, they have full access to the contents available to that group, no matter what application provides and manages that content. If someone leaves the group, they lose access to the information belonging to the group. It is as simple as that. The downside of this approach is that non-members have complete access to some information held in public groups.

Sharing is easy: Users can share personal documents stored in their OneDrive for Business account with other people, including external users (if allowed by the tenant sharing policy). Members of groups can share documents from the group document library with other users and other groups just as easily. Thus, you

should never put a document into a group document library unless you want to grant full control over that information to every other member of the group.

A shared memory: In the past, administrators often bolted public folders to distribution lists to record contributions. Groups incorporate a shared memory from the start in that once someone joins a group, they enjoy full access to all the information accumulated in the group since its initiation. Nothing is secret or hidden from group members. The shared memory makes it easy for new members to quickly familiarize themselves with the work of the group without the need for an existing member to send them messages or documents or update them with details of group meetings. Everything is present for the new member to explore.

A growing experience: Members might begin by taking part in group conversations, just as they have used distribution lists for decades. Over time they can become more fully involved in the work of the group and begin to use the other facilities to interact with other people. Since their introduction, Microsoft has steadily added new features to Groups. More importantly, as shown in their use by the Teams and Planner applications, Groups have become the keystone for Microsoft 365 collaboration.

Group Components

The functionality enabled through Groups is based on the single identity represented by the group objects stored in Entra ID. The single identity and simple permissions model create a low-touch need for administration. Membership information exists as sets of links that connect back to user accounts. Three types of members exist:

- **Owners:** These users can update group properties and add members and owners to the group. A user must be a group member before they can be an owner.
- **Members:** These users have full access to all the resources of the group. Users must connect to the group to access Outlook conversations. Members can add new members to a public group or request that an owner adds someone to a private group.
- **Subscribers:** These are members who have opted to receive copies of conversations and group calendar events via email. A group does not have to have any subscribers, which is the normal case for the groups used by Microsoft Teams where conversations occur through chats rather than email. To ensure that they can participate in group conversations, Exchange adds guest accounts to the subscriber list when they join a group. This also applies to groups enabled for Teams.

Group membership can be dynamic or static. You can create dynamic Groups through the Entra admin center, PowerShell, or the Graph API. Entra ID supports two types of group membership:

- **Dynamic user:** Entra ID uses membership rules (queries) to compute group membership. When you create a dynamic group, you specify the rules used to find group members. Dynamic groups can include the membership of other groups, including Microsoft 365 groups with assigned or dynamic membership and distribution lists.
- **Assigned:** The membership is static. To change the membership, administrators add or remove members.

You can change the membership type for a group from dynamic to static afterward. When this happens, Entra ID updates the group to add the objects found by the dynamic query as static members.

User accounts can be owners, members, and subscribers. Guests can only be Members and Subscribers and cannot be group owners. Members can elect to take part in conversations via email, in which case they join the set of subscribers. Except for dynamic groups, administrators and group owners manage the three types of members by manipulating the links belonging to the group through group-enabled applications like OWA

or Teams, the Outlook mobile apps, or by running the set of PowerShell `*-UnifiedGroupLinks` cmdlets as discussed in the PowerShell book.

No way to Print Group Membership: No Microsoft application includes a method to print or report the details of the membership of a group. As [explained in this article](#), it's easy to create a report with PowerShell.

Ownerless Groups Policy

Most Microsoft 365 apps prevent the removal of a group's last owner. However, the deletion of an account (for example, when someone leaves the company) might result in some groups falling into an ownerless state. Although this is not a good condition, the group continues to function. New members can continue to join if the group is public but membership requests to join private groups stay unapproved because no owner exists to process requests.

You can check for ownerless groups with PowerShell.

```
[array]$Groups = (Get-UnifiedGroup -ResultSize Unlimited | Select-Object DisplayName, ManagedBy)  
$Groups | Where-Object {$_.ManagedBy.Count -eq 0}
```

After finding an ownerless group, administrators can add a new owner by updating the group through the Microsoft 365 admin center or EAC or by running the `Add-UnifiedGroupLinks` cmdlet.

The Group Ownership Governance policy (aka the ownerless group policy) automates the process of finding and fixing ownerless groups. Configured in the Microsoft 365 Groups section in Org settings in the Microsoft 365 admin center, the policy uses background processes to periodically check for ownerless groups. For each ownerless group, Microsoft 365:

- Examines the group membership and makes a random selection from the active tenant accounts in the membership to become potential group owners. The administrator sets the number of accounts that Groups can invite to become the group owner. This number can be from 1 to 90. Active means that the account performs some activity in the group in the last 90 days.
- Sends an invitation by email to the potential group owners to ask them to take on the role.
- Actions the response of those invited to become group owners.
- Continues the process for the number of weeks (up to 7) set in the policy.

Microsoft 365 captures audit records for all the actions involved in sending out and processing responses to invitations to become group owners.

The governance policy can process all or selected groups. It can also constrain the selection of new group owners to the members of a security group. This feature allows an organization to restrict group ownership to specific accounts instead of having random people chosen (potentially to become owners of very important groups). No special license is necessary if the policy allows random selection, but if opt for restricted selection, all the members of the groups which come within the scope of the policy require Entra ID P1 licenses. See [this article](#) for more information.

Group Privacy (Access Type)

A group can be private or public (the default for a new group is private). A private group is one where the group owners control the membership. This is the most suitable group to use when group content is confidential. If a group's membership is open, anyone can view its membership, but not the content unless they join the group. Users can ask to join a private group, and their request is routed to the group owners. Any of the group owners can allow or deny a request to join.

You can change the default access type for groups created by Outlook clients by updating the organization configuration. This setting does not affect groups created from non-Outlook endpoints.

Set-OrganizationConfig -DefaultGroupAccessType Public

Public groups are open to any user in the tenant. Anyone can join a public group if they wish. A user can enroll other users into public groups without their permission (the newly enrolled users can then decide whether they want to take part in the group).

You can change the access type for a group using the following methods:

1. **OWA:** Select the group, edit its properties, and switch the type. For more details, see the section about creating and updating groups with OWA later.
2. **Outlook:** Select the group, then **Edit Group** and update the setting.
3. **Teams:** Select a team and use **Manage Team** to change the setting.
4. **Outlook mobile:** Expand the Groups section in resources and select the group, edit its properties, and change the privacy setting.
5. **Planner:** Select a plan and then **Plan Details**, then choose the Privacy setting in the **Group** tab.
6. **EAC or Microsoft 365 admin center:** Select the group and edit its settings.
7. **PowerShell:** Run the *Set-UnifiedGroup* cmdlet and set the *AccessType* property to be either Private or Public.

Set-UnifiedGroup -Identity TestGroup -AccessType Private

If your tenant uses sensitivity labels for container management, the sensitivity label assigned to the group controls its privacy setting and you can only update the privacy setting by changing the sensitivity label.

Conversations

Aside from sharing documents, the basic way members communicate within a group is through threaded conversations. The individual items in message threads exist in the Inbox folder of the group mailbox for Outlook Groups or the Yammer data store for Viva Engage communities. In either case, clients present messages sent to the group as threaded conversations. Users can reply to conversations by posting a response using a client or by sending email.

The calendar is the other major folder used in a group mailbox. It functions much like any other calendar in a personal or shared mailbox, with the notable exception that you can't use granular permissions with group calendars.

Access to Other Folders in the Group Mailbox

Although group mailboxes contain a complete set of default folders, clients usually only expose the Inbox and Calendar folders. The other default folders function in much the same way as happens in user mailboxes. For instance, junk mail sent to a group goes into the Junk Email folder, and the Sent Items folder stores copies of messages generated by clients, such as notifications to users that someone has assigned them a task using Planner. If a group is team-enabled, compliance records for standard channel conversations are in the TeamsMessagesData folder. If the group is subject to a hold, the Recoverable Items folder retains copies of items until the hold lapses. You can retrieve details about the complete set of folders in a group mailbox by running this command:

Get-MailboxFolderStatistics -Identity GroupName | Format-Table Name, ItemsInFolder

To access all the folders in a group mailbox, you can add the mailbox as a shared folder to OWA. This action makes OWA treat the group mailbox like a shared mailbox. Alternatively, you can enable folder and rules support for group mailboxes. This feature only works for OWA. It allows group members and owners to:

- Create subfolders of the Inbox in group mailboxes.
- Access some non-Inbox folders (but only non-default folders) created by group owners and members.
- Move, copy, and delete items in folders in group mailboxes.
- Add and manage inbox rules for group mailboxes.

Three settings in the Exchange Online organization configuration control how group members use these features (group owners can always delete, move, and copy items). The settings are:

- *IsGroupFoldersAndRulesEnabled*: Defines if folders and rules are enabled for group mailboxes. The default is True, meaning that OWA exposes the support for folders and rules in Outlook groups.
- *IsGroupMemberAllowedToEditContent*: Controls if group owners see a permissions toggle when editing group settings to control the ability of group members to move, copy, and delete messages and create and manage rules. The default is True, meaning that the toggle is available. If set to False, group owners don't see the toggle and group members cannot move, copy, and delete items.
- *BlockMoveMessagesForGroupFolders*: Controls if the move option is available to group members. If True, they can move items to other folders. If False, they cannot. The reason why you might prevent group members moving items is to keep all received messages in the Inbox where they can be accessed by people using Outlook desktop and mobile clients.

At an individual group level, group owners must set the permissions toggle in group settings (if the organization *IsGroupMemberAllowedToEditContent* setting is True) to allow group members to copy, move, and delete items. It can take up to 20 minutes before a change to enable or disable permissions takes effect.

Rules management for group inboxes uses the same interface as rules management for personal mailboxes. The important point to remember is that group inbox rules apply to inbound messages delivered to the group. They do not affect the copies of messages delivered to group members who subscribe to the inbox.

Assigning Send As and Send On Behalf Of Permissions to Groups

How to assign the *Send As* and the *Send On Behalf Of* permissions to mailboxes is explained in the Exchange Online chapter. You can also grant these permissions to Groups, or rather to the group mailboxes, to let group members (and non-group members) send messages as if they were the group (*Send As*) or on behalf of the group (*Send On Behalf Of*).

You can assign permissions by editing the group properties in EAC or through PowerShell. With EAC, edit the group and go to the group delegation settings. Enter the names of the users to whom you wish to assign the *Send As* and *Send On Behalf Of* permissions and then **Save**. Two cmdlets manage the permissions through PowerShell. The *Add-RecipientPermission* cmdlet assigns the *SendAs* permission and the *Set-UnifiedGroup* cmdlet assigns the *Send On Behalf Of* permission. Here is an example of how to set the two permissions:

```
Add-RecipientPermission Microsoft365Gurus@Office365ITPros.com -AccessRights SendAs -Trustee  
Kim.Akers@Office365ITPros.com  
  
Set-UnifiedGroup -Identity "Microsoft 365 Gurus" -GrantSendOnBehalfTo  
@{Add="John.Smith@Office365ITPros.com"}
```

After users have been assigned permissions, they can use [OWA or Outlook to send messages](#) as if they were the group.

Auto-Reply for Group Mailboxes

Group mailboxes support the ability to set an auto-reply. This is useful when the need exists to inform people about some special processing for messages that arrive in a group mailbox. For example, to tell:

- Customers about the procedure to process messages sent to a group.

- Internal people to inform them that a group is team-enabled, and all conversations occur in the team. Although most team-enabled groups are hidden from Exchange clients and are not included in Exchange address lists like the GAL, this doesn't stop people sending emails to the SMTP addresses of the groups.
- People when a group (or team) is not in active use or archived.

Setting an auto-reply for a group mailbox is just like setting one for a user mailbox. In this example, we use the *Set-MailboxAutoReplyConfiguration* cmdlet to create an auto-reply. The message sent to external people tells them that the mailbox is not in use. Because the group is team-enabled, the message used for internal people includes a mailto: link to the email address for a team channel. The recipient can click on the link to send their message to Teams.

```
Set-MailboxAutoReplyConfiguration -Identity "Office 365 for IT Pros" -ExternalMessage "Sorry, this
mailbox doesn't accept email" -AutoReplyState Enabled -InternalMessage 'Please! We use Teams for
communication, so send your message to <a href = "mailto:
943a5091.office365itpros.com@emea.teams.ms">Teams</a> and it will be dealt with there.'
```

Moving Personal Email to Groups

Users can move items from personal mailboxes to Groups using drag and drop in either OWA or Outlook. You can move items from any mailbox to which you have access. The moved items go into the inbox folder in the group mailbox. If you reply to the item, the recipient list includes all the recipients from the original message plus the group.

Group Document Libraries

Apart from conversations and the shared calendar, the most obvious difference between Groups and traditional email distribution lists is the Files functionality available through the SharePoint team site owned by a group. When you create a new group, the provisioning process uses a site template called **GROUP#0** to create a SharePoint Online site for the team site. You cannot change the template to apply other settings, such as assigning a storage quota (which you can update afterward using the *Set-SPOSite* cmdlet). All the limits applied to SharePoint sites apply to the sites used by Groups.

Users can add content to document libraries using the following methods:

- Drag and drop files from any location accessible to your PC (local drives, OneDrive, file servers, etc.). You cannot drag and drop files from another SharePoint Online site or group document library. We will discuss later how to move files from a SharePoint Online site to a group document library.
- Upload files or the contents of entire folders.
- Create files from scratch using Office Online applications.
- Save files into the document library from desktop Office applications.
- Save attachments received by email into the document library using Outlook or OWA.
- Use the OneDrive Sync client to upload and manage files.

When a file is in a Group's document library, the group controls its permissions. All documents in the library inherit the permissions to allow group members equal access to the content. SharePoint checks permissions when a user requests access to a file by checking the group membership. The storage used by group document libraries counts against the overall allocation for the tenant.

If the group is public, any user in a tenant can join the group and access the files in the document library. It is also important to remember that the group owns the content in the group document library rather than the original authors. If someone leaves a group, all the content they authored or amended remains behind.

Document Library Regional Settings: The regional settings for document libraries created for Groups inherit their time zone and locale (country) from the account which creates the group. Group members see date and timestamps for documents as if they were in that time zone. You can change the site's time zone and locale (country) by updating the Regional Settings (in Site Information). Sites created in the SharePoint admin center use the regional settings defined in the Site creation settings.

Implementing Groups

Microsoft 365 Groups are a platform for user-driven collaboration. In an ideal world, or a small tenant, this approach works, and users create the right number of groups, each used for its assigned purpose. Allowing everyone to create new groups in larger organizations is more problematic because the potential then exists that underused or unwanted groups will linger in the directory and absorb resources. The latter point is debatable because Microsoft controls the resources and tenants do not incur any cost when a user creates a group. In general, it is better to set out a well-defined set of rules to govern the creation of groups and communicate them to users upfront than to attempt to apply rules retrospectively and control a sprawl of unwanted groups.

Here are some simple questions to help show the need for a new group:

- **What purpose will the group serve?** If the person who wants to create a group cannot say why the group is necessary and how it differs from existing groups, then there is a fair chance that the new group is unnecessary. Sometimes you cannot avoid creating a new group, as in the case when a Planner creates a new plan (from scratch or by copying an existing plan), which results in the automatic creation of a group to support the membership and conversations for the plan. See the Tasks chapter for more information about Microsoft Planner.
- **Who is the intended audience for the group?** Is the group to be public (anyone can join it) or private (restricted to a defined set of users)? Does the group need to support guest access?
- **What app will people use to access the group?** The available options include Outlook, Teams, and Viva Engage. Each app brings its own set of advantages and disadvantages to the table. The best answer depends on factors like the organization's culture, strategic direction for collaboration, and above all, the desired functionality. For example, an Outlook-based group is a good choice for a team that needs to receive and process inbound communications from customers. A team is a good choice for small working groups who need to work on projects. A Viva Engage community works well for cross-organization communication, especially when the organization is very large. The thing to remember is that it is important to select the right technology to meet the needs of those who will use it instead of trying to force one answer for all.

Group Controls

The default situation is that anyone in a tenant can create a new group. In the following pages, we'll get into the details of how to apply different levels of controls to restrict the creation of groups. For now, we can summarize by saying that controls over group creation are available at these levels.

Entra ID (directory): the Groups section of the Entra admin center has a setting to control if users can create new Microsoft 365 groups. The *Users can create Microsoft 365 groups in Azure portals, API or PowerShell* setting is in the General settings section for Groups in the Entra admin center. By default, the setting is On. If it is turned off, users won't be able to create new Microsoft 365 groups even if allowed by the Entra ID Groups policy. A similar setting in the Entra admin center controls the ability of users to create new security groups.

Microsoft 365 (all workloads): The Entra ID Groups policy contains settings to control different aspects of groups, one of which is to disable the ability of all users to create new groups and replace this with a

restricted set of people permitted to create groups. A security group is usually the best method to define the set of users. Restricting group creation is an Entra ID P1 feature.

App-level: Outlook clients use a setting in the OWA mailbox policy to define if a user can create a new group through Outlook (including OWA and Outlook mobile). This control does not require any additional licenses.

It's up to each organization to decide what level of control they wish to exert over group control, including the use of third-party software to impose group creation request and approval workflows. You can also implement a group creation workflow using a Power Apps flow (many templates exist for this task).

Entra ID Groups Policy

The Entra ID Groups policy (or rather, a directory setting object) stores settings in an array of name-value pairs. The settings control different aspects of Groups such as the ability to create new Microsoft 365 groups. Applications retrieve settings from the policy to know how they should interact with Groups. Table 10-2 lists the policy settings.

Policy setting	Use
<i>AllowToAddGuests</i>	Controls whether users can invite external accounts to become guest members of Groups (and Teams). By default, this setting is <i>True</i> , meaning that group owners can add guests.
<i>AllowGuestsToAccessGroups</i>	Controls whether guests can access content held in the SharePoint site belonging to Groups. By default, the value is <i>True</i> .
<i>AllowGuestsToBeGroupOwner</i>	Controls whether guests can be group owners. This setting is not operational.
<i>ClassificationDescriptions</i>	Comma-separated descriptive pairs for the classifications available in the tenant.
<i>ClassificationList</i>	Stores a comma-separated list of valid classification values to give users a visual indication of what is stored in different Groups.
<i>CustomBlockedWordsList</i>	A list of words that the tenant does not wish group owners to use in the names of new groups.
<i>DefaultClassification</i>	Sets the default classification to apply to new groups.
<i>EnableGroupCreation</i>	Controls whether users can create groups. By default, this value is <i>True</i> and any user can create a new group.
<i>GroupCreationAllowedGroupId</i>	Points to the object identifier (GUID) of a security, distribution, or Microsoft 365 group whose members can create new Groups. This group is used if the <i>EnableGroupCreation</i> setting is <i>False</i> .
<i>GuestUsageGuidelinesUrl</i>	Defines a URL displayed in client user interfaces to remind users about guidelines for how to share company information with guests. For example, http://mydomain.com/GuestUserAccessO365Groups.html .
<i>PrefixSuffixNamingRequirement</i>	Used by the group naming policy to define if it should apply a prefix and a suffix to the display names of new groups.
<i>UsageGuidelinesUrl</i>	Defines a URL displayed in client user interfaces to give guidelines about the creation and usage of Groups. For example: http://mydomain.com/HowtoUseO365Groups.html .
<i>EnableMIPLabels</i>	Tells Groups to use sensitivity labels instead of text-based classifications.

Table 10-2: Settings in the Entra ID Groups policy

While you can configure the *AllowGuestsToBeGroupOwner* setting to *True* to allow guests to become owners of groups, this capability is not exposed in the Groups or Teams user interfaces.

Get Entra ID Right Too: It's amazing how often you need to look up Entra ID for something to do with a group. For instance, you might want to know where the owner of a group works or who their manager is. If

the directory isn't populated accurately, you'll get bad results. It is always best to ensure that the information held in the directory is as accurate as possible (it will never be 100%) before building any script or other procedure that depends on a directory lookup.

Licensing Groups Functionality

If you use Groups or Teams without changing any setting in the Entra ID Groups policy, the only license needed is the one included in plans like Exchange Online, Teams, or Office 365 E3. Things become more complex if you decide to utilize some of the more advanced features enabled and controlled through policy settings because Microsoft requires accounts to have Entra ID P1 licenses to benefit from the added functionality. Microsoft's view is that these features reduce administrative effort or make groups more productive for organizations, so they price the features accordingly as extensions of the basic Entra ID capabilities bundled with every tenant.

The general rule is that any account that benefits from a feature must be licensed. Sometimes this rule is easy to understand, as in the case of dynamic groups where the requirement is to license the accounts found by the queries used to populate group membership. For instance, if you create a dynamic group based on a query that finds all users with mailboxes in the tenant, it means that you need licenses for all those accounts. In other cases, the logic is harder to follow. For example, if you implement a policy to control the creation of new groups, you must license every account in the group allowed to create new groups plus the administrators who manage the policy. On the other hand, if you use the expiration policy to control how long groups function before their owners must reconfirm that the groups are needed, you only need licenses for the members belonging to the groups to which you apply the expiration policy.

Table 10-3 summarizes the licensing requirement for the features you can activate or control through the Entra ID Groups policy. See this [support article](#) for more information.

Feature controlled by a group policy setting	Requires Entra ID P1
Allow non-admin users to create groups	No
Restrict the ability to create new groups to a defined set of accounts	Yes
Use the expiration policy to force the renewal of groups after a set period	Yes
Create and use dynamic groups	Yes
Apply group naming policy	Yes
Apply default classification to new groups	Yes
Provide URL with usage guidelines to internal users	Yes
Provide URL with usage guidelines to guests	Yes
Allow guests to access groups	No
Force new groups to have classification selected from a predefined list	Yes

Table 10-3: License requirements for features controlled by group policy settings

The requirement for Entra ID P1 licenses to use certain features makes them less attractive than if Microsoft bundled the functionality into the standard plans as it does for Microsoft 365 Business Premium plan. Entra ID premium licenses are included in the Enterprise Security and Mobility suite and the Microsoft 365 enterprise SKUs.

Guest Access Licenses

[Guest access to Microsoft 365 applications](#) is included in all Microsoft 365 Business Standard and Premium plans and Enterprise subscriptions, which means that you do not need to assign licenses to guest users to access applications like Groups, Teams, and Planner. Microsoft's [guidance for B2B collaboration licensing](#) sets

out the rules for guest access to “paid” (premium) Entra ID features like conditional access policies. Briefly, Microsoft allows tenants 50,000 free authentication activities for premium activities monthly. Access past this threshold is charged against an Azure subscription taken out by the tenant. See [this article](#) for more information.

Creating and Updating the Groups Policy

By default, a tenant does not have an active Groups policy, and applications use default settings. To change any settings, we first create a directory setting object to hold the policy settings from the correct template. Entra ID loads default values into the new policy and you can then update those settings.

Several directory settings templates exist in Entra ID, including one to hold group policy settings. A different template is available to control guest access for specific groups (explained later). To see the available templates in a tenant, use the `Get-MgBetaDirectorySettingTemplate` cmdlet (use the /beta endpoint) to query the templates API. Access to update directory settings requires the `Directory.ReadWrite.All` permission.

```
Get-MgBetaDirectorySettingTemplate | Where-Object {$_._.DisplayName -like "*group*"} | Format-List
 DisplayName, Values, Id

DisplayName : Group.Unified
Values      : {NewUnifiedGroupWritebackDefault, EnableMIPLabels, CustomBlockedWordsList,
              EnableMSStandardBlockedWords...}
Id         : 62375ab9-6b52-47ed-826b-58e47e0e304b

DisplayName : Group.Unified.Guest
Values      : {AllowToAddGuests}
Id         : 08d542b9-071f-4e16-94b0-74abb372e3d9
```

The directory settings template used to create the Groups policy for the tenant has the display name *“Group.Unified”* while the one used to amend settings for a specific group is called *“Group.Unified.Guest.”* The templates have identifiers *62375ab9-6b52-47ed-826b-58e47e0e304b* and *08d542b9-071f-4e16-94b0-74abb372e3d9* respectively. These identifiers are the same in all tenants.

To create a new directory settings object to hold the tenant-specific settings for the Groups policy, run the `New-MgBetaDirectorySetting` cmdlet to create the new directory settings object from the template.

```
$PolicyId = (Get-MgBetaDirectorySettingTemplate | Where-Object {$_._.DisplayName -eq
"Group.Unified"}).Id
New-MgBetaDirectorySetting -TemplateId $PolicyId
```

When the `New-MgBetaDirectorySetting` cmdlet runs, it creates a new directory settings object. Any application that can access Entra ID can check the settings to know what it needs to do to respect the policy. For example, when a user tries to create a new group, the client can verify that the user can take this action. To view the policy settings, run the `Get-MgBetaDirectorySetting` cmdlet. In this case, many of the settings have non-default values.

```
Get-MgBetaDirectorySetting | Where-Object {$_._.DisplayName -eq "Group.Unified"} | ForEach Values

Name          Value
----          -----
EnableMIPLabels          true
CustomBlockedWordsList
ClassificationDescriptions General Usage:Anyone can access,External Access:Available outside
                           the company,Internal Only:Must not be shared with external people,Confidential: Can only be
                           disclosed with management permission
DefaultClassification      General Usage
PrefixSuffixNamingRequirement
AllowGuestsToBeGroupOwner   False
AllowGuestsToAccessGroups   True
GuestUsageGuidelinesUrl
```

GroupCreationAllowedGroupId	A3c13e4d-7083-4448-9224-287f10f23e10
AllowToAddGuests	True
UsageGuidelinesUrl	http://office365itpros.com/GroupGuidelines.html
ClassificationList	General Usage, External Access, Internal Only, Confidential
EnableGroupCreation	False

We will discuss how to update individual settings in the Groups policy using the *Update-MgBetaDirectorySetting* cmdlet over the next few pages. Remember that the names of policy settings are case-sensitive, so be sure to type the names exactly as shown here (for example, "AllowToAddGuests" rather than "Allowtoaddguests"). If you use the wrong name, Entra ID cannot update the policy. Another thing to consider is that Exchange Online distributes mailboxes for a tenant across multiple servers that can run inside different Microsoft data centers, so it can take an hour or so before new or updated settings are active across a tenant. Finally, if you make a mistake and want to start over with a new group policy, you can do so by removing the directory settings object and then creating a new directory settings object from the template as described above.

```
$PolicyId = (Get-MgBetaDirectorySetting | Where-Object {$_.DisplayName -eq "Group.Unified"}).Id
Remove-MgBetaDirectorySetting -DirectorySettingId $PolicyId
```

In the rest of this section, we cover how to update the settings in the Groups policy to control classifications, group creation, naming, and group guidelines.

Container Management for Groups, Sites, and Teams

Groups, Teams, and SharePoint sites are *containers* for information associated with Groups. Some host internal discussions, some hold confidential information that the tenant wants to keep restricted within the organization, and some exist to share information with guests. To help users understand how sensitive or confidential the information stored within a container is, Groups introduced classifications. A classification is a text-only marker (like "Secret" or "Confidential") assigned to a group and displayed by applications. A text-only marker can deliver a visual reminder to users when they work with important data, but the marker is no more useful than a sticker applied to a paper document.

If sensitivity labels are available in the tenant, you can replace classifications with "container management" sensitivity labels. Container management labels contain management settings that Entra ID stamps onto groups when they receive a label. These settings include:

- **Privacy:** The group is private or public.
- **Guest access:** Whether the group owner can add guests to the membership.
- **Unmanaged devices:** Controls how group members can access content in the group's SharePoint site when they connect with an unmanaged device.
- **Sharing settings** controlling what can be shared externally.
- **For Private Teams:** if the team is visible to users when they browse for teams to join.

A tenant can choose to use classifications or sensitivity labels to mark groups. They cannot use both. In either case, when you apply a classification or sensitivity label to a group, the marking is synchronized across workloads. Clients connecting to the workloads display the marking prominently in their user interfaces (Figure 10-2).

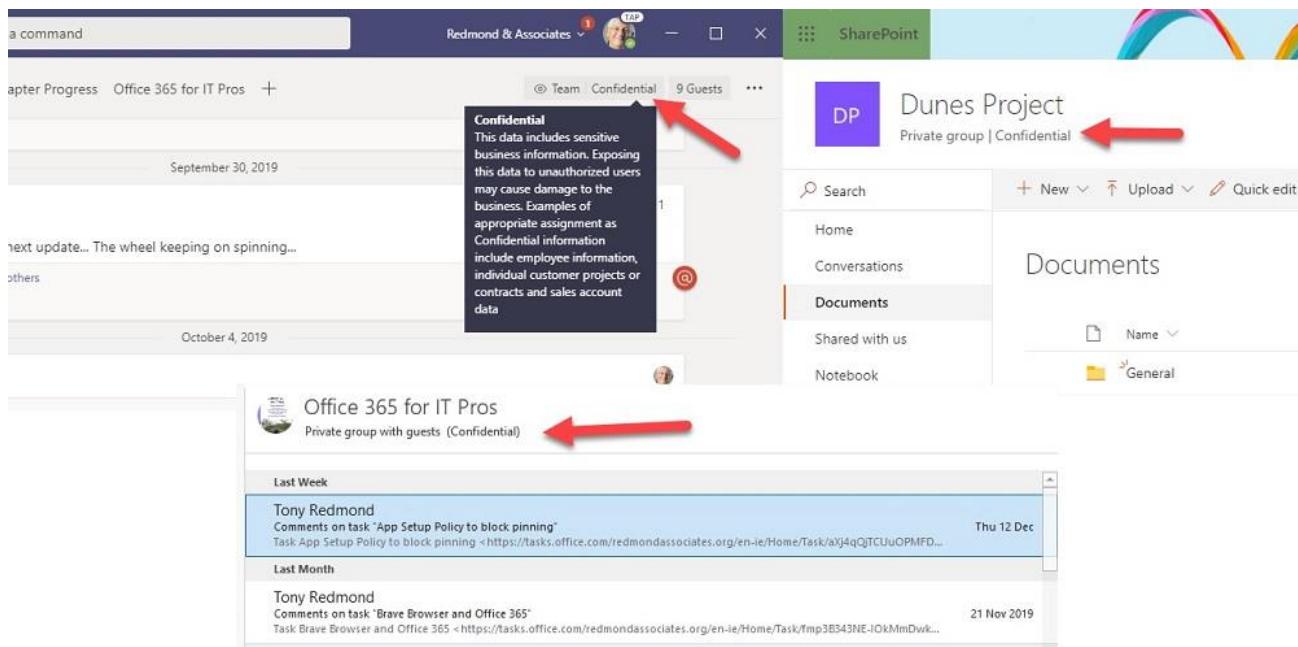


Figure 10-2: Sensitivity markings in Teams, SharePoint, and Outlook

To assign or update sensitivity labels for groups you can use:

- **Client applications:** OWA, Outlook, Outlook mobile, Teams, Teams mobile, SharePoint browser client. User interfaces refer to both sensitivity labels and classifications as "Sensitivity."
- **Administrative portals:** SharePoint admin center (you can add a sensitivity column to see the labels applied to sites), Entra admin center, or the Teams admin center.
- **APIs:** PowerShell (`Set-UnifiedGroup` and `Set-SPOSite`). Support is also available to [assign sensitivity labels to Groups via the Graph API](#).

To use sensitivity labels instead of classifications, follow the directions in the Information Protection chapter to enable sensitivity label support for SharePoint Online and SSeSD update the groups policy to enable sensitivity labels.

See [this article](#) for more information about using classifications and how to switch to sensitivity labels.

Like updates to any policy, changes can take some time to become active in all applications. Before making the switch, make sure that you have defined an appropriate set of sensitivity labels to use with groups.

Controlling Group Creation

If a tenant allows unrestricted creation of Groups, each licensed user in the tenant can exploit over twenty separate ways available across a spectrum of clients and applications to create up to 250 groups. A thousand-user tenant therefore might end up with 250,000 user-created groups to add to the groups created by administrators. Allowing people to create the groups they think they need through a self-service model is in line with Microsoft's original view that control over groups should be user-led. Although the model gives users the power to decide what groups they need to collaborate with their colleagues, it's easy to see how chaos can result and why, in most cases, it is better when administrators put some thought and planning into the process of group creation and maintenance. This is especially true in large enterprises.

Previous experience with user-controlled creation of shared objects, such as the mayhem that often occurred in public folder hierarchies when anyone could create top-level folders in the early versions of Exchange, proves that if you allow users free rein to create new objects, you can expect a rapid expansion of those objects, many of which duplicate the purpose of other objects. The usual upshot of creating many groups for no good reason is user confusion. People do not know which groups to use for what reason, especially if you

do not implement a naming policy and apps create groups with duplicate names. This can lead to chaos in the GAL with groups scattered amongst other mail-enabled recipients. Creating groups often leads to groups used for a period and then left to decay. It is to impose order on potential madness that tenants decide to exert control over who can create new groups. The group expiration policy helps to clean up unused groups and should be used whenever possible. We discuss how this policy works later.

Administrative interfaces are not subject to the same controls over group creation as imposed on clients. Accounts holding administrative roles for the tenant (see below) can create new groups using PowerShell or an administrator portal even when blocked by application-level controls. On the other hand, those holding administrative roles cannot create groups using clients like OWA or Teams unless they are allowed by policy. The administrative roles allowed to create new groups are:

- Global Administrator.
- Team Service Administrator (in the Teams admin center or Entra admin center).
- User Administrator (in the Microsoft 365 admin center or Entra admin center).
- Exchange Administrator (in the Exchange admin center or Entra admin center).
- SharePoint Administrator (in the SharePoint admin center or Entra admin center).
- Directory Writers (in the Entra admin center).
- Groups admins (in the Microsoft 365 admin center and Entra admin center).

In addition, groups created through administrative interfaces (like the admin centers, PowerShell, and Graph APIs) do not come within the scope of the group naming policy.

When group creation is controlled, users cannot create new teams unless they're allowed by policy. However, if they are owners of Microsoft 365 Groups that are not team-enabled, they can create new teams from those groups.

Steps to Control Group Creation

Follow these steps to create the settings to control the creation of new groups through the Groups policy.

Create a group for the set of authorized users: You need to know the set of users who can create new Groups. To define the set of authorized users, you create a group to hold their names. This can be a distribution list, a security group, or a Microsoft 365 group. A security group is the best choice for two reasons. First, if you create new groups through SharePoint, you must use a security group to control creation. Second, unless you mail-enable the group, a security group does not appear in the GAL and is therefore less likely to be known to users. If you restrict group creation and do not specify a group for authorized users, only administrators can create new groups.

Add the set of authorized users to the security group: Because Groups only exist in the cloud, the users who create new groups must have accounts homed in the cloud. Make sure that you add all the people you want to be able to create new groups as members of the security group. Being an owner of the group is insufficient. Include those who hold administrative roles so that they can create new groups from applications and be sure to consider the needs of applications to use groups. For example, the Viva Amplify app uses groups for its communication campaigns. Make sure that all the members of the security group have Entra ID P1 licenses.

Prepare to edit the policy: Because no user interface exists for this purpose, you must create the policy and populate its settings using PowerShell. The first step is to retrieve the object identifier for the group that you just created to hold the set of authorized users. This can be done by checking the group object in the Entra admin center or by running the `Get-MgGroup` cmdlet:

```
(Get-MgGroup -Filter "displayName eq 'GroupCreationControl'").Id
```

```
12cb915b-2365-4bed-baf6-6257b3543273
```

The group identifier (*Id*) returned by the `Get-MgGroup` command identifies the group whose members can create new Microsoft 365 groups and is needed to update the policy. If you use the Entra admin center to find the group identifier, copy it to the clipboard and store it safely for reuse with PowerShell cmdlets.

Use PowerShell to update the policy: Two controls are used for group creation:

- Set the **`EnableGroupCreation`** setting to *False* to show that only authorized users can create groups. To reset and allow anyone to create groups, update the setting to *True*.
- Populate the **`GroupCreationAllowedGroupId`** setting with the identifier of the group holding the list of authorized users. This is the *Id* property retrieved using the `Get-MgGroup` cmdlet as described above. No check is done to establish what the identifier points to when you use it in a policy setting, so it is easy to make a mistake and end up in a situation where only an administrator can create a group. For this reason, you should avoid typing the identifier manually and instead copy the value from the group properties shown in the Entra admin center or use PowerShell to retrieve the value.

Members Only! It's critical to understand that only the members of the nominated control group can create new Microsoft 365 groups. A common mistake is for an administrator to create the control group (and so become the owner) and then assume that they can create new groups. Administrators can create new groups, but only through administrative interfaces. They will be unable to create new groups using applications like Teams because they are not a member of the control group.

Together, the two policy settings tell applications that only the members of the authorized group can create new groups. In this example, we fetch the object identifier for the group (as explained above) used to control group creation and the current settings of the Groups policy. The current values are extracted into an array, and we update the two settings with the necessary values. We then write the new values for the settings back into the policy.

```
$GroupId = (Get-MgGroup -Filter "displayName eq 'GroupCreationControl'").Id
$TenantSettings = Get-MgBetaDirectorySetting | Where-Object {$_.DisplayName -eq "Group.Unified"}
$Values = $TenantSettings.Values
($Values | Where-Object Name -eq 'EnableGroupCreation').Value = "false"
($Values | Where-Object Name -eq 'GroupCreationAllowedGroupId').Value = $GroupId
Update-MgBetaDirectorySetting -DirectorySettingId $TenantSettings.Id -Values $Values
```

After making the changes, you can check that the settings are as you expect. This code retrieves the name, identifier, owners, and current membership of the group used to control group creation.

```
$Values = (Get-MgBetaDirectorySetting | Where-Object {$_.DisplayName -eq "Group.Unified"}).Values
$GroupId = $Values | Where-Object {$_.Name -eq "GroupCreationAllowedGroupId" } | Select -
ExpandProperty Value
[array]$Owners = (Get-MgGroupOwner -GroupId $GroupId)
[array]$OwnerNames = $Null
ForEach ($Owner in $Owners) {
    $OwnerNames += (Get-MgUser -UserId $Owner.Id).DisplayName }
[string]$OwnerNames = $OwnerNames -join ", "
Write-Host ("The name of the group defined to control group creation is {0} and its identifier is {1}. Its owners are {2}." -f (Get-MgGroup -GroupId $GroupId).DisplayName, $GroupId, $OwnerNames)
Write-Host ""
Write-Host "The accounts allowed to create new Microsoft 365 groups are:"
(Get-MgGroupMember -GroupId $GroupId).additionalProperties.displayName
```

Exchange Online stores details of some group policy settings in its organization configuration, so the following command also reveals who can create new groups:

```
[array]$Members = Get-MgGroupMember -GroupId (Get-OrganizationConfig).GroupsCreationWhiteListedId
ForEach ($Member in $Members) {(Get-MgUser -UserId $Member.Id).DisplayName }
```

Test that the new policy works: A user included in the membership of the authorized user group should be able to create new groups from any application that supports the policy, including OWA, Planner, Teams,

Dynamics, Stream, SharePoint Online, and OneDrive for Business as well as the Outlook and Teams mobile apps. Applications signal errors when a user who is not allowed to create a group tries to create a new group (something like “*The group couldn’t be created. Your admin hasn’t given you permission to create a new group*”).

Lack of Granularity in the Creation Policy: The use of a single policy to control group creation makes things simple. The downside is that once you restrict creation, the decision applies to all applications that use Groups for membership services. For instance, you might want to control the creation of new Plans but not Teams, but the same policy applies to both applications, as it does to Stream, SharePoint, and the other group-enabled applications. You should consider this point when you decide to apply restrictions to group creation.

A script demonstrating how to control the group creation settings in the Entra ID policy [is downloadable from GitHub](#).

Changing the Group for Authorized Group Creators

Over time, you might want to swap the group specifying the set of users allowed to create groups for another group, perhaps for testing purposes. You can change the group specified in the policy by updating the *GroupCreationAllowedGroupId* setting in the policy with the identifier for the group. Like the code used to establish a group to control creation, we retrieve the identifier for a group called “Authorized Users” and use it to update the policy.

```
$GroupId = (Get-MgGroup -Filter "displayName eq 'Authorized Users").Id
$TenantSettings = Get-MgBetaDirectorySetting | Where-Object {$_.DisplayName -eq "Group.Unified"}
$Values = $TenantSettings.Values
($Values | Where-Object Name -eq 'GroupCreationAllowedGroupId').Value = $GroupId
Update-MgBetaDirectorySetting -DirectorySettingId $TenantSettings.Id -Values $Values
```

The Groups Admin Role and Group Creation

The *GroupCreationAllowedGroupId* setting in the Entra ID Groups policy allows tenants to control which users can create new groups. Being able to create new groups by policy does nothing to allow people to manage groups thereafter, so tenant administrators had to do this work. The situation is manageable in small tenants but becomes more problematic as the number of groups grows.

The Groups admin role is designed to solve the problem. This is a standard Microsoft 365 administrative role that can be assigned to user accounts through the Microsoft 365 admin center, the Entra admin center (where the role is called Groups Administrator), or PowerShell. When assigned, the Groups Admin role allows the holder to manage the following actions for Groups:

- Create, edit, delete, and restore Microsoft 365 groups and security groups.
- Create, edit, and delete group creation, expiration, and naming policies.

Groups admins can manage groups and group policies through administrative interfaces such as the Microsoft 365 admin center, PowerShell, or Graph APIs. Holding an administrative role does not allow users to create new groups through client interfaces like OWA. If you want administrators to be able to create groups using all applications, you must add them to the membership of the group used to control group creation in the Entra ID Groups policy.

An [Entra ID custom role](#) can also be used for fine-grained control over group creation.

Entra ID Group Naming Policy

Exchange Online has a naming policy that applies to distribution lists. Settings in the Entra ID Groups policy can similarly control the display name generated for new groups created by applications. You can update the

policy with the Microsoft Graph or with PowerShell (see below) or you can use the Entra admin center (Figure 10-3).

The screenshot shows the 'Groups | Naming policy' page in the Azure AD for workforce section of the Entra admin center. The 'Group naming policy' tab is active. A message box says 'Learn more about group naming policies.' Below it, the 'Group naming policy' section explains that it allows adding a specific prefix and/or suffix to group names. The 'Current policy' is shown as '<Group name>M365'. There are two sections for modifying the policy: 'Add prefix' (with a dropdown menu 'Select the type of prefix') and 'Add suffix' (with a dropdown menu 'String' containing 'M365' and a link 'Select another suffix')).

Figure 10-3: Working with the Entra ID Groups naming policy in the Entra admin center

Settings for the Groups Naming Policy

Two settings in the Groups policy control the form of display names users can give to groups when they create new groups or update the display name of existing groups:

- The **PrefixSuffixNamingRequirement** setting is a pattern controlling whether the group name has a prefix and suffix. The pattern can include fixed strings or reference user attributes such as the department, company, or office of the user who creates the group. Attribute values come from the information held in Entra ID for the account of the user creating the group. You can combine multiple attributes in a display name. Although combining multiple attributes to create a display name might seem like a good idea, it is best to favor simplicity over complexity when selecting which attributes to use to construct a display name. The policy ignores values that are missing in the directory. If the tenant uses a naming policy for Exchange distribution lists, it is wise to use different prefixes for the two types of groups. Finally, the display name created for a group can be up to 256 characters. If you tend to use very long names for groups, you must ensure that the application of prefixes and/or suffixes to display names does not exceed the 256-character limit.
- The **CustomBlockedWordsList** holds a set of words that users cannot include in group names. These might be words that you consider offensive or have other reasons to exclude. Companies often include business terms that they do not want people to use in group names such as "CEO" to avoid the possibility that users communicate with the wrong person or group. The check against blocked words is case-insensitive and you do not have to enter the blocked words alphabetically. For practical

purposes, you can enter as many words as you like in the list as Entra ID sets no upper limit. The Azure Active Portal allows you to upload a CSV containing blocked words to add to the policy.

The naming policy does not apply when administrators create groups. The assumption is that these users know what kind of display name to give to a group.

Deciding on a Prefix or Suffix for Group Names

The original thinking about group names followed that of Exchange distribution lists and largely preferred using a prefix instead of a suffix to mark groups. The logic behind the choice is that this allowed users to find all the groups together in the Global Address List (GAL) and other address lists.

Useful as this approach is for applications that use the GAL, the reasons for using a prefix are less valid for applications that create groups but don't use the GAL (like Teams). A suffix is often a better approach for these applications because it is less visually intrusive as the marking moves to the end of the screen space reserved by the application to list group names (like the list of teams shown to the left of the Teams client). The choice to use a prefix or suffix is heavily influenced by what applications are in use within the tenant.

Naming Policy in Action

Here is an example of how to update the settings used for the group naming policy. In this case, we want to add the prefix "O365Grp-" to the names of newly-created groups (and existing groups when a group owner updates their properties). We also specify a set of custom blocked words.

```
$TenantSettings = Get-MgBetaDirectorySetting | Where-Object {$_.DisplayName -eq "Group.Unified"}  
$Values = $TenantSettings.Values  
($Values | Where-Object Name -eq 'PrefixSuffixNamingRequirement').Value = "O365Grp-[GroupName]"  
($Values | Where-Object Name -eq 'CustomBlockedWordsList').Value =  
"Sexy,Stupid,Giggles,Funny,CFO,CEO,Shit,Payroll"  
Update-MgBetaDirectorySetting -DirectorySettingId $TenantSettings.Id -Values $Values
```

A small change is made to use a suffix instead of a prefix. For example, let's assume that we want to add the suffix "(Team)" to the display names of new groups. The *PrefixSuffixNamingRequirement* setting for the policy is then:

```
$Settings["PrefixSuffixNamingRequirement"] = "[GroupName] (Team)"
```

After a naming policy is in effect, clients apply the policy when users create new groups or edit the display name for an existing group. [Many of the applications](#) which create Groups support the naming policy. Clients check the name entered by the user rather than the name as it will be after the application of the prefix and/or suffix dictated by the policy (what Microsoft refers to as the "decorated" name). Another point to remember is that the check for blocked words is for complete words rather than substrings. This is to avoid problems where a blocked word is part of another legitimate word (think "ass" as part of "class").

Some differences exist in the detail of how a client applies the naming policy. In general, web-based clients like OWA and Teams generate a preview of the group name after the application of the policy together with warnings when a user types in a blocked word for a group name. Other clients, like Outlook desktop and Outlook mobile clients, enforce the policy without giving so many visual clues as users type in names. Instead, these clients flag errors when they check the policy before trying to create or edit a group.

Updating Group Display Names with PowerShell

When you implement a naming policy for groups, its effect is not retrospective, and the naming policy will not apply to existing groups. If you want to bring those groups into line with the policy, you must update the display name for older groups. One solution is to use PowerShell to make a one-time pass to find and update non-compliant group names. The example [script available on GitHub](#) extracts the group naming policy for the organization and uses it to figure out the display names for groups that don't currently follow the policy. The

example works when either a prefix or suffix is used to create the display names for groups. Because it's PowerShell code, you can include other conditional processing. For instance, team-enabled groups might use one form of display names while those not used with Teams might have another.

Group Policy Settings in Exchange Organization Configuration

For convenience (mostly for OWA), copies of some group policy settings are held in the Exchange Online organization configuration. You can view these settings by running the *Get-OrganizationConfig* cmdlet:

```
Get-OrganizationConfig | Format-List Group*,Data*
```

```
GroupsCreationEnabled      : False
GroupsCreationWhitelistedId : 12cb915b-2365-4bed-baf6-6257b3543273
GroupsUsageGuidelinesLink  : Http://office365exchange.com/GroupGuidelines.html
GroupsNamingPolicy          : 0365Grp-[GroupName]
DataClassifications         : <DataClassifications
Default="Confidential"><Classifications><Classification Name="General Use"
Description="Anyone can access" /><Classification Name="External Access" Description="Available
outside the company" /><Classification Name="Internal Only" Description="Must not be shared with
external people" /><Classification Name="Confidential" Description="Can only be disclosed with
management permission" /></Classifications></DataClassifications>
```

The group settings in the organization configuration are read-only and cannot be updated with the *Set-OrganizationConfig* cmdlet.

Creating Microsoft 365 Groups

If permitted by policy, a user can create new Microsoft 365 Groups through the following interfaces:

- **Admin portals:** The Microsoft 365 admin center, Exchange admin center (which also includes the option to upgrade a distribution list), Teams admin center (create a new team), and the Entra admin center.
- **Email clients:** OWA, Outlook for Windows or Mac (Microsoft 365 Apps), Outlook for iOS and Android.
- **Applications integrated with Groups:** These applications include Power BI, Dynamics 365, Teams, Stream, Viva Engage, Flow, and Microsoft Planner.
- **SharePoint Online:** Create a new team site or link an existing team site to a Group; you also have the option to create a group from a hub site.
- **OneDrive for Business:** Create a new group-enabled site.
- **Programmatically:** With PowerShell using the *New-UnifiedGroup* (Exchange Online module), *New-MgGroup* (Microsoft Graph PowerShell SDK), or *New-Team* (Microsoft Teams module) cmdlets; or through the [Microsoft Graph Groups API](#).

The list of possible ways to create a group grows all the time. Depending on the apps and configuration used in your tenant, you might have other methods available for group creation than those listed above.

Administrators most likely create new groups through the Microsoft 365 admin center, EAC, or PowerShell while users are likely to use OWA or Outlook. To create a new Group from the Microsoft 365 admin center, navigate to the **Active teams and groups** page in the **Teams & Groups** section and select **Add a Microsoft 365 Group**. The group creation wizard then gathers basic properties for the new group. These properties are:

- **Group name.** This is the display name visible to users through the directory. Make sure that the name conveys the intention and purpose of the group because it is highly likely that this is the sole information people will use when they decide whether to join the group. It is sensible to check the directory beforehand to ensure that the name you want to use does not clash with an existing object such as another group, a team, a distribution list, or a shared mailbox. You can rename a group after creation by editing its properties or by running the *Set-UnifiedGroup* cmdlet to update the

- DisplayName* property. The display name for a group can be up to 256 characters and can contain periods.
- **Description.** A free-text description to inform users about the intended use of the group. You can add whatever you like here but the text should tell users and administrators why the group exists and its intended use. In a multi-lingual organization, you might like to include translations of a text explaining the group's purpose in multiple languages. If a group holds confidential information, it is wise to make that fact known to group members here.
 - **Owners and members.** You must add at least one owner to manage the group and its membership (it's generally better to have at least two owners in case one leaves the organization). You can add some group owners and members when you create the group or build out the group membership afterward by either adding new members or, for dynamic groups, by changing the rules used by Entra ID to calculate its membership. You cannot nest a group inside another Microsoft 365 group, nor can you add a traditional distribution list to become a group.
 - **Group settings.** Administrative interfaces such as the Microsoft 365 admin center allow administrators to assign an email address to a new group. User clients, such as OWA or Outlook, collect details of the group name for Exchange Online to create a unique SMTP email address and **Alias** (or mail nickname) for the new group. Exchange Online derives the alias by removing any spaces from the group name before checking against the directory to make sure that the value is unique. If not, the user must change something in the alias to make it unique (for instance, appending a number to its end). You can add periods to the alias if the period has other text on both sides. For example, "Sales.Group.1" is OK, while "Sales.Group.1." is not (see the documentation for the [New-UnifiedGroup](#) cmdlet for more information). Exchange Online then combines the default email domain for the tenant with the alias to form the SMTP address, which also must be unique. For example, if the alias is *SalesProfessionals* and the tenant's default email domain is *contoso.onmicrosoft.com*, the SMTP address will be *SalesProfessionals@contoso.onmicrosoft.com*. After creation, an administrator can add more email addresses to the group or change the primary email address. For instance, groups can have an address from a vanity domain.
Entra ID prohibits the use of certain well-known or "highly-privileged" reserved aliases to avoid any possibility that users create groups with these words. Prohibiting the assignment of reserved aliases to groups is not unique to Entra ID (Google Workspace also includes this restriction). The reserved aliases include "abuse", "admin", "administrator", "hostmaster", "majordomo", "postmaster", "root", "secure", "security", "ssl-admin", and "webmaster." Only administrators can create groups that include these terms in identifiers (the Microsoft 365 admin center and EAC won't allow administrators to create distribution lists or mail-enabled security groups with a reserved alias).
 - **Sensitivity.** If your organization uses sensitivity labels for container management, you can assign a label to the group. As explained in the Information protection chapter, the new group inherits several settings from the label to control aspects like privacy, guest access, and external sharing.
 - **Privacy.** A group can either be Public, which means that anyone can join a group and access the resources available to the group (notebook, mailbox, calendar, document library, plan, and so on), or Private (the default), in which case only nominated members can access the group resources. Entra ID does not mark private groups in any special way within the directory, so they appear alongside public groups. For this reason, it is a good idea to consider giving a confidential group a name that does not create interest (or gossip) on the part of users. For instance, a group called "Planning 2020 Layoffs" is likely to attract unwanted attention! If users want to join a private group, they can apply to do so. A request then goes via email to the group owners, who then decide whether to add the user to the group membership. After creating a private group that needs to remain confidential, you can hide its existence from address lists to prevent the group from appearing in the GAL. Remember that you can change a group access type later.

- **Team-Enabled.** The Settings section includes the option to create a team for the new group. Use this option when a group's function is to manage the membership of a team rather than hosting Outlook conversations, so you should choose it to make the group available in Teams. It's entirely possible to access a group through Outlook and Teams, but it's more usual to choose one or the other. If you choose to team-enable a new group, make sure that the chosen group owners have Teams licenses as otherwise, they won't be able to access Teams. To help, when you come to assign group owners, the owner picker shows you which accounts have Teams licenses.
- **Role assignment:** You can [assign an administrative role](#) to the group. Only private groups should hold administrative roles. Role Assignment is a permanent state, meaning that once assigned, you can't remove the role from a group. If a mistake is made, you must remove the group and recreate it. Although Microsoft 365 Groups support role assignments, in many cases it's best to use security groups instead to avoid the chance that sensitive groups appear in address lists.

Click **Next** to review the settings for the new group and then **Create group** to complete the process. After a short pause, the new group is ready for use.

Managing Groups in the Microsoft 365 Admin Center

Some group settings are updatable only after the creation of a new group. These include:

- **Language.** The default language is the one for the user who creates the group. You can change the language at any time. Exchange Online uses the selected language in messages sent to group members, such as in the footer of copies of conversations. It has no impact on the content of group discussions or anything else belonging to the group.
- **Send copies of group conversations to members' inboxes.** The default is "On" for groups created using the Microsoft 365 admin center or an Outlook client. This means that the group adds new members automatically to its subscriber list. Subscribers receive copies of conversations and meetings via email and do not need to access the group mailbox unless they want to. Members can contribute to conversations by replying to the messages they receive. Individual users can disable or enable this setting as they like. Groups do not generate daily or weekly digests of conversations. Apart from guest members, groups used with Teams do not add new members to the subscriber list because their conversations are in Teams.

You can update settings through the Microsoft 365 admin center, Exchange admin center, Outlook clients, or PowerShell. In the Groups section of the Microsoft 365 admin center, you can do the following:

- Filter to only show all groups, team-enabled groups, or dynamic groups.
- Add group owners and members.
- Edit group settings, such as a group's display name, description, and whether to hide it from Exchange address lists.
- Allow external addresses to send emails to a group.
- Assign a new primary SMTP address for a group.
- Enable a group for Teams.
- Recover deleted groups.
- Export details of the groups to a CSV file. If a filter is applied, only the filtered groups are included in the export file.

Updating Group Membership

After making sure that the new group is set up correctly, the next step is to build the group membership. To do this in the Microsoft 365 admin center, go to the Groups section, and select the group. Under the *Members* tab, you can add group owners and members, including guests.

Using a GUI works well when you need to add a small number of users. Scrolling up and down within a large list to find the right person to add to a group can lead to mistakes, as can searching the GAL to find the right person when they have a common surname. For instance, many organizations have multiple users named "John Smith" or "Tom Jones." The Microsoft 365 admin center shows the user principal names for group members, but these can also be similar and hard to decipher. Large tenants often solve the problem by including organizational prefixes like departments in display names to help people find the right user.

OWA automates the process somewhat by allowing group owners to import members from distribution lists or other groups. When this happens, Exchange Online expands the membership of the input group, and adds eligible accounts to the group membership, so it is an effective way to add many members quickly. It is possible to add members to groups programmatically, including the conversion of some types of traditional email distribution lists to become Groups. Updating group membership through PowerShell is not to everyone's taste, but it can be the most efficient way to approach the task.

Limits: All software has limits and Groups are no different. Apart from the limits imposed by the underlying applications such as SharePoint Online storage quotas or the number of items that a folder can store in an Exchange Online mailbox (well over 100,000), Microsoft documents some specific limits for Groups. The most important are:

- A group can have up to 100 owners. The client user interfaces (including PowerShell) will prevent an attempt to add more. If you hit the limit, you must demote an existing owner before you can add a new one.
- An individual user cannot create more than 250 groups. This limit exists to speed up retrieval of the groups owned by an account from Entra ID. The limit could become a factor in large tenants where central control governs the creation of new groups. The simple workaround is to make sure that you reassign ownership for newly-created groups to a different user and remove the account that created the group from its owner list. The limit does not apply to global tenant administrators.
- Microsoft supports Outlook Groups with more than 1,000 users with the caveat that access to the group mailbox (for conversations and calendar) will be slow. By contrast, the reduced number of connections to the group mailbox allows team-enabled groups to support 25,000 members.

A tenant can support up to 500,000 Groups. These limits apply to all Groups, including those used by group-dependent apps. Microsoft can increase the number if necessary.

Checking Membership Changes to Sensitive Groups

Sometimes organizations want to monitor changes made to the membership of specific Microsoft 365 groups to make sure that unauthorized access to confidential information doesn't happen. One method to do this is to mark the selected groups with a value in a custom attribute and monitor the audit events captured in the event log when administrators or group owners update the memberships of the marked groups. A [PowerShell script can find and report the membership updates](#). To ensure that the check happens regularly, the script could run as a scheduled Azure Automation task with email sent to administrators to verify membership changes.

Welcome Notifications

When you add a member to a group using the Outlook apps or the admin tools (including PowerShell), Exchange Online generates a welcome notification and sends it to the user via email. The notification tells the person that they are now a member of the group, whether the group is public or private, how many other members are in the group, and contains a link to the group. A different form of the message is created for team-enabled groups, but the same principle holds.

Generation of the welcome message is governed by a property called *WelcomeMessageEnabled*. To disable the welcome message, update this property to False.

```
Set-UnifiedGroup -UnifiedGroupWelcomeMessageEnabled:$false -Identity 'U.S. Employees'
```

To revert and send welcome messages again, run Set-UnifiedGroup to reset the property:

```
Set-UnifiedGroup -UnifiedGroupWelcomeMessageEnabled -Identity 'U.S. Employees'
```

Creating Microsoft 365 Groups from the Entra Admin Center

To create a Microsoft 365 group from the [Entra admin center](#), select Identity, then All Groups, and then create a new group. Set the membership type to Assigned and the group type to Microsoft 365. After you add members, Entra ID signals Exchange Online to create the new group mailbox and SharePoint Online to create the new team site. The process of fully-provisioning group resources takes longer than it does when creating groups elsewhere too.

The synchronization process eventually completes, and the new group is available. Because the Entra admin center focuses exclusively on managing directory objects, it does not update the email-related properties managed in the Exchange Online directory. For example, you cannot assign the primary SMTP address for a new group to anything but the service domain for the tenant. By comparison, when you create a new group with OWA, Outlook, or EAC, you can populate those attributes (like if members receive updates via email) to create a fully-functional group.

Updating Group Properties

Once the group exists, you can update its properties. Group maintenance operations like updating properties or membership usually occur through the Microsoft 365 admin center or EAC. However, the admin centers don't support access to some group properties. For instance, you cannot add a MailTip or change the property which hides team-enabled groups from Exchange clients. You can manage these properties through PowerShell, which is one reason why some administrators script the creation of groups to ensure that their properties comply with the standards set for the tenant. For example, this command updates several properties for a new group, including a new primary SMTP address based on a vanity domain, a new alias, modification of the access type for the group, notes about the purpose of the group and allowing external users to contribute to group conversations by sending emails to the group.

```
Set-UnifiedGroup -Identity ProductMarketingGurus -PrimarySmtpAddress ProductMarketigGurus@Office365ITPros.com -Alias ProductGurus -AccessType Private -Notes "Product Marketing Discussions - Private Group" -RequireSenderAuthenticationEnabled $False
```

Non-Latin Group Names

Exchange Online generates the primary email address for new groups based on the group identifier (alias), which is in turn based on the group name. When clients run in non-English languages, group owners can input non-Latin characters in the group name. Behind the scenes, clients generate the identifier and primary email address from the group name. Some clients use the [internationalized domain name](#) (IDN) standard to deal with non-Latin characters. Although this is generally a good thing and creates valid identifiers and email addresses, it can result in the creation of email addresses that are not user-friendly. To avoid the problem, use a group identifier (alias) that only includes basic Latin characters. Alternatively, you can assign a new primary SMTP address to the group post-creation.

Email Address Policies and Groups

By default, Exchange Online assigns a newly created Group a primary SMTP address belonging to the tenant's default domain plus a secondary address for the service domain (the one ending in onmicrosoft.com). You can assign extra SMTP addresses to groups after creation, but you might want to assign SMTP addresses from separate domains depending on who creates the group.

Email address policies control the primary SMTP addresses Exchange Online assigns to new groups. Any of the known domains for the tenant are usable for this purpose. For example, this email address policy dictates that all new groups receive their primary SMTP address from the Office365itpros.com domain. The groups also receive a secondary proxy address from the service domain:

```
New-EmailAddressPolicy -Name Groups -IncludeUnifiedGroupRecipients  
-EnabledEmailAddressTemplates "SMTP:@office365itpros.com" -Priority 1
```

See [this page](#) for more information.

Controlling Group Email Traffic

For new groups created with OWA, the default setting is to subscribe members to the group. This means that Exchange Online distributes copies of any message sent to the group to all members, including tenant users and guests. Members can control the communications they wish to receive through **Manage Group Email** in the cogwheel menu, selecting whether to receive all messages, replies to their posts, calendar events, or no messages. They can also subscribe using the link in the group card displayed by Outlook.

The group's *AutoSubscribeNewMembers* property is *True* to subscribe members or *False* if not. You can change the *AutoSubscribeNewMembers* settings by:

- Editing the group properties with OWA or Outlook
- Updating the **Subscribe members** setting for the group in the Microsoft 365 admin center
- Running the *Set-UnifiedGroup* cmdlet. For example:

```
Set-UnifiedGroup -Identity Office365ITPros -AutoSubscribeNewMembers:$False
```

Groups created by Teams set the *AutoSubscribeNewMembers* property to *\$False* because members of these groups don't communicate via emails. To see a list of groups that do not distribute copies of conversations and events to members, use the command:

```
Get-UnifiedGroup | Where-Object {$_._AutoSubscribeNewMembers -eq $False } | Select DisplayName
```

To receive copies of group conversations and events, members join the group's subscribers list. The *Get-UnifiedGroupLinks* cmdlet can report the subscriber list for a group:

```
Get-UnifiedGroupLinks -Identity Office365ITPros -LinkType Subscribers
```

No way exists to view the subscribers of a group except via PowerShell. The membership view presented by Outlook clients lists individual users as either an owner or a member and doesn't display any information about subscribers.

When a group is "chatty" with many conversations, some members might decide that they do not wish to receive updates via email and are quite happy to access the conversations in the group mailbox instead. Tenant users can control the updates they receive for a group through email through settings available in OWA, Outlook for Windows, Outlook for Mac, and Outlook mobile. Guests can ask a group owner to remove them from the group's subscriber list if they do not want to receive updates. Even after removing a group member from the subscriber list, they continue to receive any conversations or replies posted to the group where replies include the special @ mention in the text (for instance, @Tony). The same is true when you explicitly add someone to the TO: or CC: list of a message sent to a group. Remember that the settings to control updates sent by email are specific to a group. If you want to stop updates arriving in your Inbox for every group you belong to, you must remove your account from the subscriber list for each group.

In OWA, the group card allows users quick access to different group resources (like conversations and files) and settings including the ability to control subscriptions. To access a group's card, find a message sent to the group and click on the group name in the message header. You can then move the **Follow in inbox** slider in

the group card from **Off** to **On** (Figure 10-4) to control whether you receive updates via email. Behind the scenes, moving the slider to **Off** removes your account from the group's subscriber list while moving it to **On** adds your account to the subscriber list. Outlook for Mac and Outlook for iOS also support group cards with the **Follow in Inbox** setting for a group.

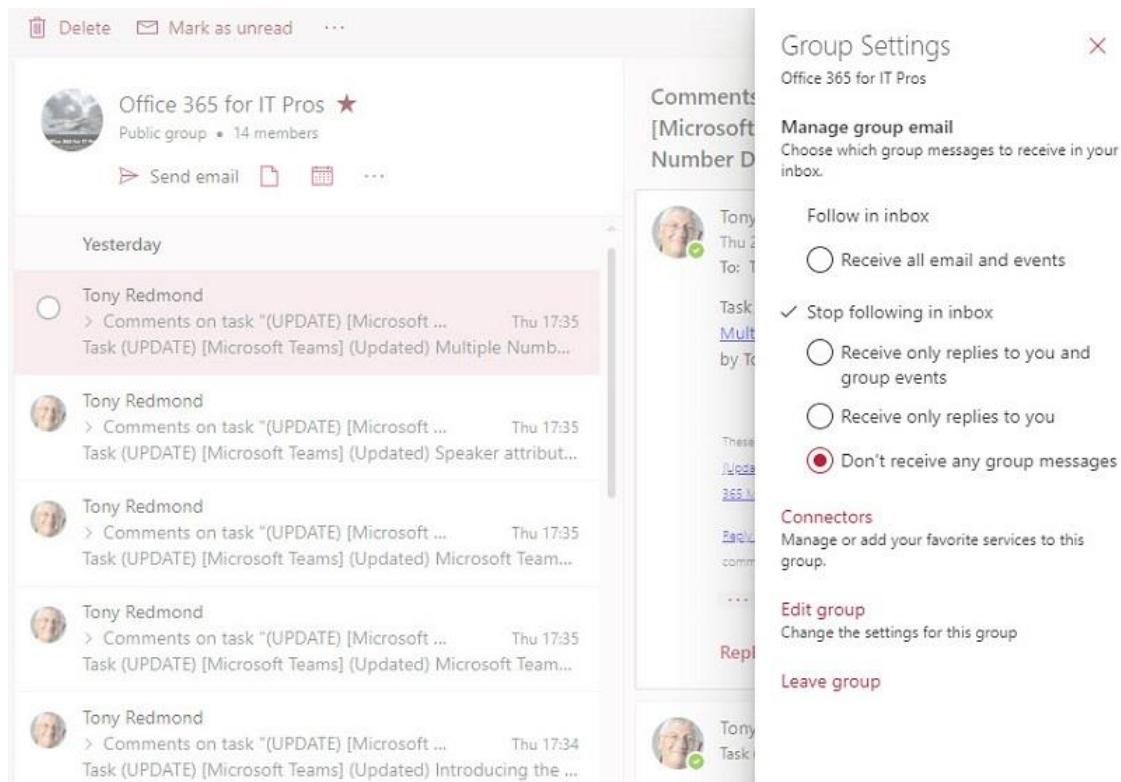


Figure 10-4: The Follow in Inbox setting controls if a user receives updates for a group by email

Groups and Transport

Every group has an SMTP email address. Members and others (if allowed by the group settings) can use that address to route email to groups just like any other recipient. The messages eventually arrive at the Exchange Online mailbox server that hosts the active copy of the group mailbox. At this point, the Exchange transport service processes the messages before delivery to the group mailbox. All messages are subject to whatever processing the tenant implements through transport rules.

In addition to sending emails to groups, clients can post new conversations and reply to existing conversations. Depending on the client, the mechanism to post to a group is slightly different. Outlook handles a message posted to a group conversation much like any other message. Upon submission, the normal Outlook synchronization mechanism picks up the change in the local folder and dispatches the message to the Exchange Online transport service. Eventually, Exchange delivers the message to the group mailbox where it shows up in a conversation. The item posted to the group stays in the user's Sent Items folder.

By default, the Exchange Online transport service does not deliver copies of messages posted by a user to their Inbox. If users want to receive copies of messages, they can either:

- Add their email address as a CC or BCC recipient.
- Use OWA settings to enable the *Send me a copy of email I send to a group* option (in the Groups section). An administrator can do this for a user by running the *Set-MailboxMessageConfiguration* cmdlet to set *EchoGroupMessageBackToSubscribedSender* to True. For instance:

```
Set-MailboxMessageConfiguration -EchoGroupMessageBackToSubscribedSender $True -Identity  
Jane.Sixsmith
```

The first approach works on an on-demand basis. In other words, the user receives copies of messages they post when they add their email address as a recipient. The second works for all groups where the user is a member of the group's subscriber list. Selecting *Receive all email and events* in the Follow in Inbox option described above adds a user to the subscriber list for a group.

OWA and mobile clients do not support offline working as the Outlook desktop clients do. Because all posts must go through the transport service, the possibility exists that a short delay might be obvious between the time when a user sends a post to the group and the post showing up in a conversation. The delay comes about through the need for the transport system to process the message through its pipeline to allow rules and routing to occur. To give the user confidence that their post succeeded, OWA and mobile clients create a "fake" post in the conversation that is only visible to the submitter. Behind the scenes, email processing continues and if a transport rule decides for some reason to reject the post, it does not deliver it to the group mailbox. The submitter will receive a non-delivery notification to tell them that an administrative rule blocked their contribution. At this point, OWA removes the fake post so that it no longer appears in the conversation. The transport service usually processes messages very quickly and the time elapsed between submission and removal is very short, but if delays occur, users might report a "disappearing item" if they ignore the non-delivery notification. It is all by design.

Managing Groups with Outlook Clients

Users allowed to create new Groups can do this with Outlook (desktop, OWA, and mobile). Group owners can also update the settings of their groups through these clients. In this section, we review how to create a new group using Outlook desktop and the management options available in OWA.

The dependency on the group mailbox for conversation storage means that Outlook Groups have a lower membership limit than other applications which use the Microsoft 365 Groups membership model. The limit is soft and based on practice, and Outlook groups don't break if they have larger memberships. The limit exists because we know that concurrent access to a shared mailbox becomes problematic as the number of connections grows. Not every member will access the mailbox (to read conversations or look at the calendar) at the same time, so 2,500 members is a "safe" limit, assuming normal usage patterns. If you have groups where members seldom access the mailbox, you can have more members. There are groups in production today that surpass this number of members by a considerable margin because their owners know only a small percentage of the membership ever access the group concurrently.

Creating and Editing Microsoft 365 Groups with Outlook (for Windows)

Three methods exist to create a new group with Outlook:

- Right-click on **Groups** in Outlook's resource navigation tree and then **New Group**.
- Click the **New** drop-down list in the **Home** section of Outlook's ribbon and then select **Group**.
- Click **New Group** in the group ribbon.

You can select public or private for the new group's privacy setting and select a value from the set of classifications defined in the Entra ID Groups policy (if set). If the tenant uses sensitivity labels for container management, the selected label controls group settings like privacy and guest access. You can update the group to change the settings afterward. When all details are input, click **Create** to create the new group. After Outlook creates the group, you can add members by inputting the names of individual users, guest accounts, or groups. If you add a group as a member, Outlook expands its membership and adds any cloud mailboxes

found in the membership to the membership of the new group. The account used to create an Outlook group joins the group automatically as an owner. Later, you can add or remove group members by selecting **Group Settings**.

Group owners can update the properties of a group. You can change the name of the group, its description, its membership, privacy setting, the language used in messages generated by the group, and whether people from outside the group can send emails to the group to take part in group conversations. Other properties, like the primary SMTP address, are either invisible or you cannot change through Outlook. The component used to edit group settings is shared with OWA.

OWA Group Management

The Manage Groups section at the bottom of the OWA's folder list and the Groups section in OWA's People section allow group members and owners to see details of the groups they belong to (including group membership), perform actions like leaving the group, and access the different resources associated with a group. A [new Outlook Groups experience](#) is also available that will likely become the default at some point (Figure 10-5).

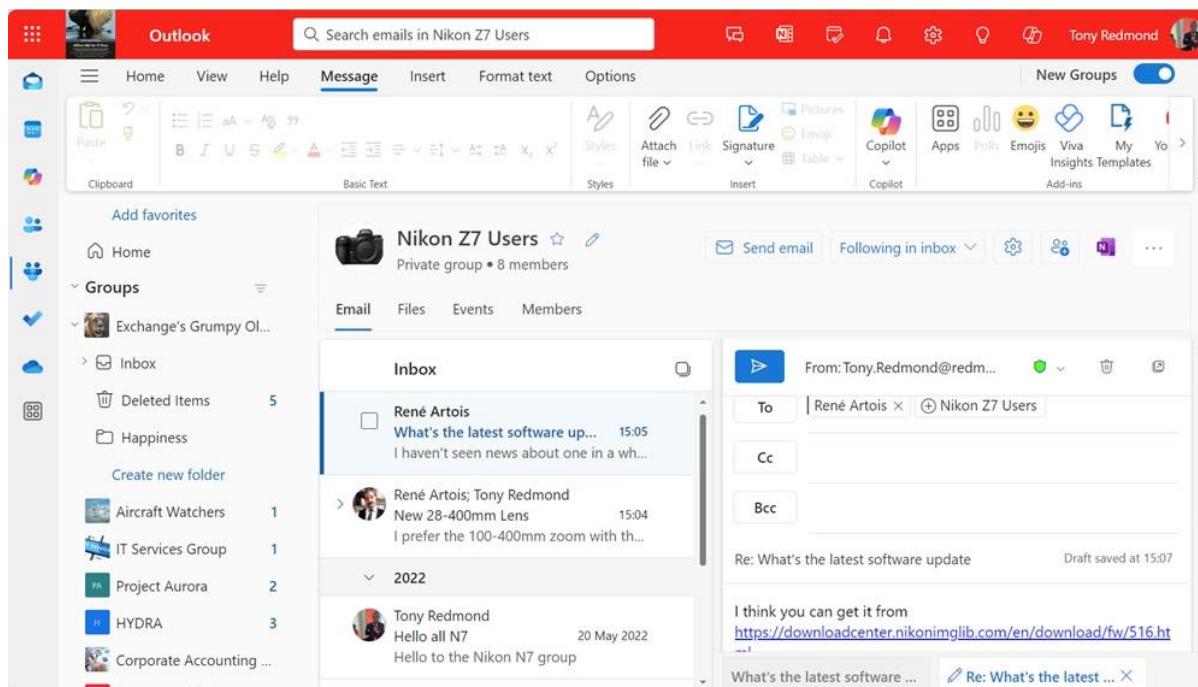


Figure 10-5: The new Outlook Groups experience

Owners can edit the settings of a group by selecting the pencil icon beside the group name. This reveals the edit group dialog to allow the owner to change:

- Group email address (the new address must be available).
- The group description.
- The sensitivity label or classification assigned to the group. Settings like whether guests are allowed are inherited from the sensitivity label.
- The language used for group communications.
- Whether people outside the organization can send messages to the group.
- Whether group members receive all group messages and events. Individual members can override this setting.
- Whether group members can manage folders and rules for the group.

A filter in the group list allows the user to choose to view all groups or just those they are a member or owner of.

Guest Access to Microsoft 365 Groups

Microsoft 365 applications that support guest user access leverage the [B2B collaboration framework](#) to create and manage guest accounts. Microsoft 365 Groups use [guest accounts](#) to enable access for external people to resources controlled by the tenant. Groups, Teams, SharePoint, and Planner support guest access. If an organization's Viva Engage (Yammer) network runs in Microsoft 365 native mode, [guests can be added to Viva Engage communities](#) using B2B collaboration, but only if the guests have Microsoft accounts. A single guest account can be a member of multiple groups and teams. Any application that supports Azure B2B Collaboration can use existing guest accounts to grant access to their resources.

Apart from the membership limits that exist for different types of groups, there is no specific limit on the number of guests who can join a group (or team). For example, you can have a group with 1 local member (the owner) and 2,499 guests. See the Identities chapter for more information about the management of guest accounts in Entra ID.

Adding Guests to a Group

Apart from administrative interfaces, you can use OWA, Outlook, or the Outlook and Teams mobile apps to add guest members to groups. A group owner or a tenant administrator can add a guest while other group members can request an owner to add a guest. For public groups, members can add guests to the group unless barred by policy (for instance, the sensitivity label assigned to the group might not allow guest members). In either case, when you add a guest to a group, an invitation is generated and sent to the guest to join the group. To start, open the group and click the *members* link (which shows the current number of members) to display the complete group membership, including any guests. Now click the **Add Members** icon and enter the email address of the guest you want to add. If the group settings allow guest access, the email address is checked against the tenant directory and your email address autocomplete list.

You are not restricted to using addresses already known to the directory as any valid email address is acceptable. If you input the email address of an account belonging to the tenant, they join the group as a regular member instead of a guest. Entra ID adds the guest to the group's membership and generates the email invitation after you click **Add**.

If group settings (for the tenant or a specific group) block guest access, OWA displays an error to say that you must contact an administrator to add a guest. OWA also flags an error if you try to add an email address for a guest that already exists for an unsupported object (like an email-enabled public folder).

Guests and the Microsoft 365 admin center: You can edit the membership of a group via the Microsoft 365 admin center and can add a guest to a group's membership there, providing that the guest account already exists in the directory. You can create new guest accounts in the Entra admin center or with an application that supports Azure B2B Collaboration, such as Groups or Microsoft Teams.

When OWA lists group members, it adds a "Guest" suffix to the display name of guest members as a visual reminder that this member is external. OWA also displays MailTips to warn users whenever they post new conversations. These visual indications serve as a warning that members should not share or discuss confidential material within the group.

How Guests Join Groups

When a group owner or administrator adds a guest to a group's membership of a group (or team), Entra ID checks if a guest account for the email address exists in the tenant. If not, Entra ID creates a new guest

account and sends an invitation to the guest's email address to let them know that they are now a member of the group. Should the guest wish to decline the invitation, the message has a link to allow the guest to leave the group. If not, they can click the link to access the group shared document library and confirm their membership. You can automate this process using the *New-MgInvitation* cmdlet from the Microsoft Graph PowerShell SDK. For example, this command creates and sends the invitation to the specified email address:

```
New-MgInvitation -InvitedUserDisplayName "Joni Sherman" -InvitedUserEmailAddress  
JoniS@o365maestro.onmicrosoft.com -InviteRedirectUrl "https://myapplications.microsoft.com"  
-SendInvitationMessage:$true
```

If you examine the properties of the guest account, you'll see that the external user state is "*PendingAcceptance*." This means that the guest has not redeemed their invitation. When they do, the state changes to "*Accepted*." The timestamp for the external user state change tells you when the last interaction occurred with the account:

```
Get-MgUser -Filter "Mail eq 'jonis@o365maestro.onmicrosoft.com'" | Format-List Mail, CreationType,  
ExternalUserState, ExternalUserStateChangeDateTime
```

Mail	:	JoniS@o365maestro.com
CreationType	:	Invitation
ExternalUserState	:	PendingAcceptance
ExternalUserStateChangeDateTime	:	2022-12-21T14:15:27Z

If a guest does not receive (or loses) the email notification to tell them about their new membership status, the group owner can send them the URL for the document library. The guest can input the URL into a private browser session and go through the sign-in process to connect to the group. The private session makes sure that existing cached credentials don't interfere with the process. The URL for a group document library is in this form:

https://mytenant.sharepoint.com/sites/groupalias/

Another method is to [reset the redemption status for a guest account](#) in the Entra admin center or with PowerShell:

```
$User = Get-MgUser -Filter "startsWith(mail, 'jonis@o365maestro.com')"  
  
New-MgInvitation -InvitedUserEmailAddress -SendInvitationMessage InvitedUser $User  
$User.Mail -InviteRedirectUrl "https://myapps.microsoft.com" -ResetRedemption
```

Some guests who receive invitations to join a group find that they cannot log into Microsoft 365 to access the group using the email address specified in the invitation. This might be because they have the same address registered elsewhere in Microsoft 365 (as a user in another tenant) and for a Microsoft consumer service, like OneDrive personal. In this case, the solution is to either use a different address to invite the guest or ask them to [rename their personal Microsoft consumer account](#).

An external user might receive an invitation to a file in a group document library if a group member shares a document from the library as a "cloudy attachment" (one where the attachment is a link to the content held in a OneDrive for Business or SharePoint Online library rather than a complete copy of the document). Clicking the attachment link invokes the invitation to access the document.

If the guest chooses to accept the invitation, two conditions can occur. First, they might already have a Microsoft (MSA) or Microsoft 365 account linked to the email address used for the invitation (including a consumer account for a service like Outlook.com). If so, they can use this account to authenticate with Microsoft 365 and access the group files.

If they do not have a Microsoft account, a redirect occurs to invitations.microsoft.com and the user can sign-up for a Microsoft account, including creating a password. Entra ID can then use the identity established by

the newly-created Microsoft account to create a guest account. Creating a fully functional guest account needs the guest to prove that they own the email address associated with the account. Entra ID sends a verification code to the email address specified by the person extending the invitation. When prompted, the user gives the code to authenticate their address and complete the activation process, the guest account can then access the group.

Finding group files: Guests who have accounts in other tenants cannot add external groups to their set of favorite groups. Instead, to ensure fast access, they should bookmark the link contained in the invitation message as a favorite in their browser. Clicking the bookmark will then bring the guest to the Files section of the group.

What Guests Can Access in Groups

Applications supporting the Azure B2B collaboration framework dictate what happens after someone accepts an invitation to access content managed by the application. In most cases, guests access group resources via browsers or mobile clients. Traditional desktop clients don't usually support guest access. You can't, for instance, configure Outlook to open a group in another tenant to see the conversations in the inbox or the group calendar. Instead, Exchange Online uses an indirect access model to allow guests to participate in group interactions via email. They send emails to the group to contribute to conversations and receive responses via email, including copies of calendar events posted to the group calendar. Guests can then decide if they want to add these events to their calendars.

External people who are not group members can participate in conversations via email if the group's *RequireSenderAuthenticationEnabled* property is *False*. Generally, it is a bad idea to allow open access to a group because it creates the possibility that an attacker who obtains the group's email address will use it to send malware to the group, which can end up being copied to group members.

The *RequireSenderAuthenticationEnabled* setting does not affect guest members because they authenticate through their guest accounts. The exception to this rule is where the primary SMTP address of a guest is different from the email address used for their invitation. When this happens, attempts to respond to a conversation fail because the email address on the inbound item does not match the address of a group member. An easy workaround is to set *RequireSenderAuthenticationEnabled* to *False*, which allows any external user to email the group. Alternatively, you can create a guest to allow the person to log in using their normal UPN and send messages to the group using their primary SMTP address.

Guests have access to the SharePoint Online sites for the groups to which they belong. They can use the SharePoint browser interface to open, add, edit, and remove items from the sites. In addition, people can share individual documents in document libraries from other SharePoint sites with guest accounts.

Table 10-4 summarizes the access available to guests to resources managed by Groups.

Workload	Feature	Guests can access?
Exchange Online	Contribute to conversations in the group mailbox	Yes (via email)
Exchange Online	View items in the group shared calendar	No direct access, but can receive updates via email
Exchange Online	Search group conversations	No
Exchange Online	Browse Global Address List for tenant (note: guests can use the Entra admin center to view directory information if enabled by the tenant)	No. (Note: Guests don't appear in any default Exchange address list)
SharePoint Online	Access a single document	Yes – via specific sharing invitation
SharePoint Online	Access the complete team site owned by the group/team	Yes

SharePoint Online	Search group documents	Yes
OneNote	Access group shared notebook	Yes
Information Protection	Members can post encrypted conversations to group conversations but cannot access messages protected with sensitivity labels. Guests cannot read files protected with sensitivity labels in the document library unless they are explicitly granted access by the labels.	No (apart from encryption)
Planner	Access plan associated with group	Yes
Teams	Access channel conversations in the team owned by the group and files stored in the group's SharePoint site. Conduct personal chats with other tenant members. Access private channels.	Yes
Power BI	Access Power BI workspace associated with group	Yes
Dynamics 365	Access customer data associated with group	No
Groups	Browse Entra ID for groups to join	No
Groups	Perform group management	No

Table 10-4: Group functionality available to guests

Restricting Guest Access to Confidential Material

A basic principle of the Microsoft 365 Groups membership model is that every member enjoys the same access to resources belonging to the group such as its document library, plans, and regular team channels. Owners maintain group membership and settings and have the same access to group resources as other members. The model is simple and easy to understand and manage, but some potential downsides exist that tenant administrators need to understand.

Consider files stored in a group's SharePoint document library. When a guest member joins a group, they receive the same access rights to documents and other files held in the document library. They can view, print, add, edit, check out, and perform all the file management actions available to other group members, including the ability to remove items. Two issues might occur:

- Guests remove information from libraries.
- Guests access confidential material.

The first issue is easily handled by using retention labels to prevent permanent deletion of important information. The second can be dealt with by using specific locations to store confidential information that external people should not access.

For instance, let's assume a project team needs some advice about a complex contract document from an external legal advisor. Three approaches are available:

- Allow the advisor full access to the group where the contract is stored along with other project files.
- Create a specially-defined group or team.
- Create a private or shared channel in a team and invite the external advisor to access the information through the channel.

The answer depends on the relationship with the external advisor and the need of the external advisor to access other supporting information that might not exist in a designated location.

If you store confidential material alongside other files in the document library, can you make sure that guests cannot access this content? The answer is yes, but you must apply sensitivity labels with encryption to protect the files from external access. As explained in the Information Protection chapter, a sensitivity label with encryption uses rights management to define the rights that users have over items. Users must be able to

authenticate their access before SharePoint Online will decrypt and expose the content. Authors always hold full rights over files while other users might only be able to read the material. If a label does not grant rights to external users, they cannot open files protected by that label.

Sensitivity labels do not encrypt document metadata, so guest users can see the title and author information for protected files in a document library, even if they cannot open the content. Protected files circulated as email attachments to external people will also be inaccessible if the external users do not have the rights to open the files.

In all cases, it's important to understand the reasons for granting access to guests to a group or team and what resources they have access to if they become members before issuing any invitations.

Giving Guests a Face

Given the collaborative nature of Groups and Teams, it makes sense to update guest accounts with suitable photos. It's much better when people get a visual reminder of whom they work with. Applications like Planner, OWA, SharePoint, Teams, and OneDrive display photos if they are available for guest accounts. For example, the left-hand screen in Figure 10-6 shows a conversation within Teams where a guest account has a photo. This is a much nicer visual reminder about the person than the anonymous circle with two letters used for guests without photos.

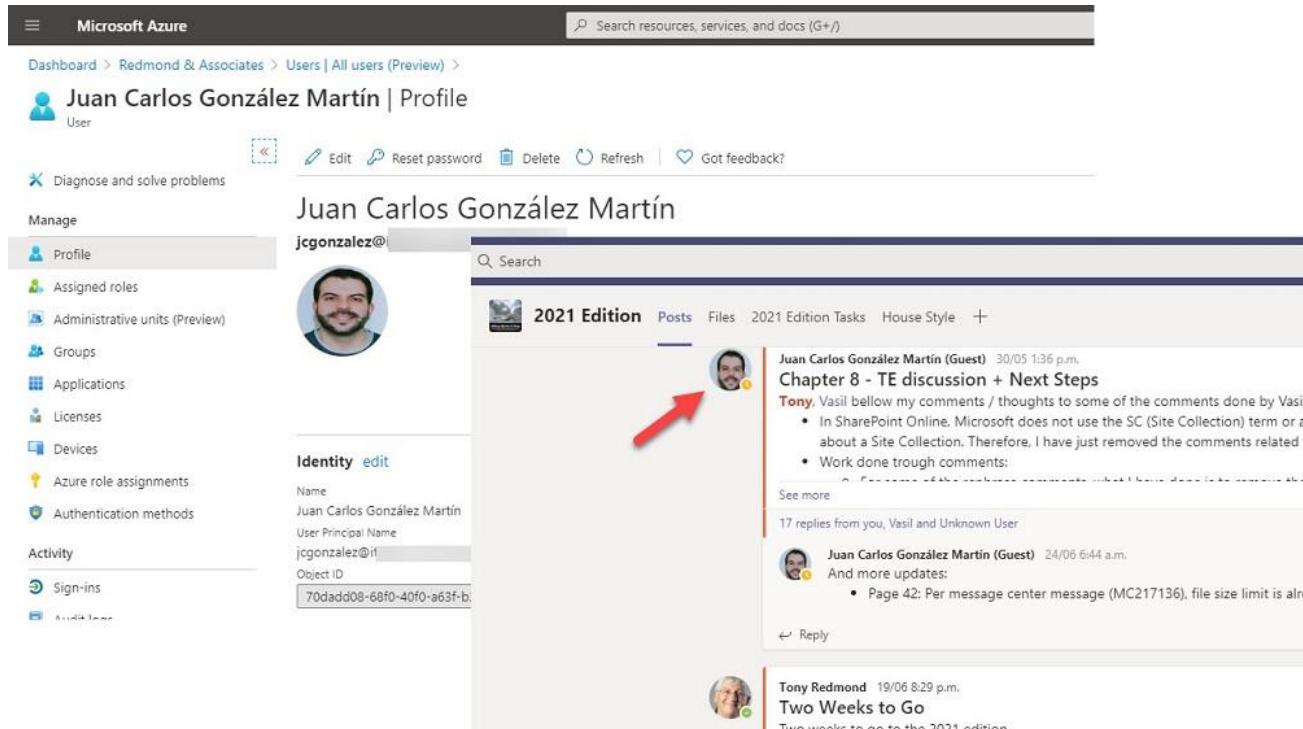


Figure 10-6: Using photos for Guest accounts

Administrators can't upload a photo to a user or guest account through the Microsoft 365 admin center, but you can through the Entra admin center. Go to the Users section, select the guest account, and upload a JPEG or PNG file, which should ideally be less than 1 MB and sized at 400 x 400 pixels. A high-definition photo is not necessary because applications only use thumbnails (small photos) when displaying information about guest accounts.

If users can't give you a suitable photo, using the profile picture from their LinkedIn.com account is usually a good option because these photos are reasonably small. To increase the usefulness of the directory, it is a good idea to update other information about the guest account at the same time, such as their first name, last

name, display name, job title, company name, and contact details. Applications can then include this information in contact cards.

After updating guest accounts with photos, the background jobs responsible for synchronizing Entra ID with Microsoft 365 applications will make the images available in apps. This process might take up to a day to complete. To force Teams to synchronize, always update another attribute of the account, like the display name. This “tickles” Teams to let the app know that it should synchronize the account. Browser clients pick up newly available photos first. Mobile and desktop clients must synchronize their local caches with the workload directory. This can add another day or so before new images appear.

Another advantage of adding photos to guest accounts is that Outlook Mobile displays the photos when displaying messages from guests. Outlook and OWA can retrieve thumbnails from LinkedIn based on a person’s email address, but Outlook Mobile depends on thumbnails stored in user and guest accounts.

Adding Guest Photos with PowerShell

You can also update the picture for user accounts using the *Set-MgUserPhotoContent* cmdlet. For example:

```
Set-MgUserPhotoContent -UserId a7eae252-3220-4254-91b2-c73918989a75 -InFile c:\temp\GuestPhoto.jpg
```

You can then take this technique further to update all guest accounts in the tenant. For instance, let’s say that you want to flag guest accounts with a special image unless a photo is already present for an account. The idea is that the image will give people a visual clue of the guest’s status. This code does the job, even if it’s not very fast.

```
[array]$Guests = Get-MgUser -Filter "Usertype eq 'Guest'" -All | Sort DisplayName
ForEach ($Guest in $Guests) {
    $PhotoExists = $Null
    $PhotoExists = Get-MgUserPhoto -UserId $Guest.Id -ErrorAction SilentlyContinue
    If (!$PhotoExists) {
        Write-Host "Photo does not exist for" $Guest.DisplayName "- updating with default guest logo"
        Set-MgUserPhotoContent -UserId $Guest.Id -Infile C:\Temp\DefaultGuestPicture.jpg
        Sleep -Seconds 3
    } Else { Write-Host "Photo found for" $Guest.DisplayName }
}
```

[This article](#) describes a more comprehensive script to find guest accounts without photos and update the accounts using files stored in a photo library.

Update Group Photos

You can also add photos to groups or teams. For much the same reasons as outlined above, it’s a good idea to assign an appropriate image to a group to help users identify the group in listings. The PowerShell book describes how to assign photos using the *Set-TeamPicture* and *Set-MgUserPhotoContent* cmdlets, and GUI methods exist to assign photos through OWA by editing group settings or Teams by managing the team and choosing settings.

Resetting Membership for Guests

Occasionally the creation process for a guest account does not complete as planned. The guest account is an Entra ID user object, and the guest shows up in a group’s membership list, but whenever the guest attempts to access the group files, they receive an error telling them that their account is not in the tenant directory.

The quickest and simplest solution is to recreate the guest account. To do this, you must remove the account through the Microsoft 365 admin center or with PowerShell. Here’s how to do the job with PowerShell:

```
Remove-MgUser -UserId t.redmond_live.com#EXT#@Office365ITPros.onmicrosoft.com
```

Now go back to a client and re-add the guest to force the creation of a new guest account. Everything should now work! The big downside with this method is that permanently removing a guest account also removes the membership for that user to all Groups and Teams and removes sharing permissions that the user might have in SharePoint and OneDrive for Business sites. For this reason, you should not remove a guest account without first thinking about the potential consequences.

Guests in SharePoint and OneDrive for Business Pickers

If you want guests to show up in the people pickers used by SharePoint Online and OneDrive for Business, you can run the `Set-SPOTenant` cmdlet to update behavior for the tenant or `Set-SPOSite` for a specific site. For example:

```
Set-SPOTenant -ShowPeoplePickerSuggestionsForGuestUsers $True
```

Guest Mail User Objects

Following the creation of a new guest account, a background process creates a linked guest mail user object. Guest mail user objects are like regular mail users, but:

- They are linked to an Entra ID guest account.
- They have `GuestMailUser` as their `RecipientTypeDetails` instead of `MailUser`.
- They are managed by updating the guest account (using the Entra admin center, Graph API, or PowerShell). Although guest mail users are visible in the Exchange admin center, they cannot be updated there. You can use the `Set-MailUser` cmdlet to update Exchange-specific settings for a guest mail user.

The intention is that guest mail user objects represent guest accounts within Exchange Online. The presence of the object allows Exchange Online to route email to the guest. It also supports:

- Participate in email-based conversations in Outlook groups.
- Appear in Exchange address lists like the GAL and OAB.
- Be a member of distribution lists.

Do not remove any of the special mail user objects. If you do, you'll also remove the associated guest user account and the guest will lose any access they have to resources within the tenant, including sharing links and memberships of teams and groups.

You can see the list of guest accounts with this command:

```
Get-ExoRecipient -RecipientTypeDetails GuestMailUser -PropertySet All | Format-Table DisplayName, HiddenFromAddressListsEnabled, PrimarySmtpAddress
```

DisplayName	HiddenFromAddressListsEnabled	PrimarySmtpAddress
Chris Burger	True	Chris@burger.com
Jon Vickers	False	flayosc32@outlook.com
Benjamin N Smith	True	benjamin.n.smith@contoso.com

By default, Exchange Online hides the mail user object for guest accounts from address lists by setting the `HiddenFromAddressListsEnabled` property to `$True`. To include guest mail users in Exchange address lists, set `HiddenFromAddressListsEnabled` to `$False`:

```
Set-MailUser -Identity vasil_michev.com#EXT# -HiddenFromAddressListsEnabled $False
```

Remember that it will take a day or so before newly unhidden objects appear in the OAB, but once unhidden, the objects show up in the online GAL and users can then address messages to the guest like any other recipient. Make sure that a mail contact for the guest isn't already present as unhiding the mail user object will

then create a duplicate in the GAL. The guest mail user appears in the offline GAL after Exchange Online generates the next set of OAB updates and Outlook clients download and process those updates.

Even if you do not update guest mail users so that they appear in address lists, you can include them in distribution lists by updating the group membership with PowerShell. Here's how to add a guest to a distribution list by specifying the user principal name of the

```
Add-DistributionGroupMember -Identity "External Suppliers List" -Member ExternalPerson@contoso.com
```

Instead of using the email address to identify the guest mail user, you can use the name, user principal name, or display name.

Mail user objects support the addition of guest accounts to groups using the *Add-UnifiedGroupLinks* cmdlet. In this example, we pass the alias created for the mail user object to tell Exchange Online which guest we want to add to the membership. As you can see, the alias is based on the UPN for the guest account.

```
Add-UnifiedGroupLinks -Identity MyGroup -LinkType Member -Links Julia.Foran_Contoso.com#EXT#
```

Alternatively, you can use the *New-MgGroupMember* cmdlet to add the guest to the group's membership.

```
$NewUser = (Get-MgUser -UserId John.Doe_outlook.com#EXT#@office365itpros.onmicrosoft.com).Id  
$GroupId = (Get-MgGroup -Filter "startsWith(displayname, 'Office 365 Adoption')").Id  
New-MgGroupMember -GroupId $GroupId -DirectoryObjectId $NewUser
```

Guests participate in group conversations via email, so we must make sure that they receive copies of group conversations via email. If the *AutoSubscribeNewMembers* property for the group is *\$True*, new members automatically join the subscriber list when they become a member. If not, we need to add them as a subscriber.

```
Add-UnifiedGroupLinks -Identity MyGroup -LinkType Subscriber -Links John.Doe_outlook.com#EXT#
```

Guest Accounts and Mail Contacts

A basic rule of email transport is that an addressable object must have a unique email address. In other words, you cannot have two objects in a directory that share the same email address. Guest accounts are an exception because they can share an email address with a mail contact. If you add a new guest account and give it the same email address as a mail contact, Groups creates the guest account based on the properties of the mail contact. You cannot do the reverse and create a mail contact using the email address of an existing guest account.

The need to support two objects with the same email address exists because the two objects serve different purposes. A mail contact exists to allow users to send emails to external contacts, individually or through a distribution list. A guest account allows an external user to access resources in the tenant.

Controlling Guest Access to Groups

Four distinct pieces come together to control guest access to Groups:

- Entra ID must allow invitations to external users to join groups.
- The settings for Microsoft 365 Groups in the Microsoft 365 admin center must allow people outside the organization to access group content (see below).
- SharePoint Online must allow sharing of content stored in SharePoint and OneDrive for Business sites with external users.
- The Entra ID Groups policy must allow guests to become members of groups.

These settings must be in place before Teams supports guest user access.

Because guest access for Outlook Groups primarily focuses on group document libraries, it follows that a prerequisite for sharing to occur is that SharePoint external sharing must be enabled for the tenant. This setting is available in the Sharing section of the SharePoint admin center. If a tenant does not allow sharing, guest access to Groups cannot work. SharePoint Online allows you to restrict sharing with users in specific domains (a whitelist). Applications ignore this whitelist when adding guests to groups. If you want to prevent guests from domains outside the whitelist from becoming members of groups, you should implement the block policy available for groups and conduct a periodic check of group memberships. We will get to these topics shortly.

The Entra ID tenant settings must also allow invitations to go to guests. For instance, if you disable the “Members can Invite” setting in the **User Settings** section in the Entra admin center, group owners cannot send invitations to people outside the organization.

Group Settings for Guests

By default, Microsoft 365 tenants support guest accounts as members of Microsoft 365 Groups. If you want to disable this capability, edit the Microsoft 365 Groups settings in the org-wide settings section of the Microsoft 365 admin center (Figure 10-7) and uncheck both:

- **Let group owners add people outside your organization to Microsoft 365 Groups as guests.** Unchecking this setting removes the ability of group owners to add new guests. Administrators can still add guests to groups.
- **Let guest group members access group content.** Unchecking this setting removes the ability of guest members to access any group resources which are not explicitly shared with them. Existing guest members of groups will lose access to group resources.

A separate Microsoft Teams setting (*Allow guest access in Teams*) controls if team owners can add guests. You can have a situation where the tenant supports guest access outside Teams. For instance, you might want to allow guests to share SharePoint Online documents but not permit guests to be members of Teams.



Figure 10-7: Microsoft 365 admin center settings for guest access to Groups

Optionally, you can use PowerShell or sensitivity labels to update the settings for a group to allow or deny guest access to that group.

Stopping Guests Joining Group Membership

Microsoft Graph PowerShell SDK cmdlets manage the settings in the Entra ID Groups policy. As an example, these commands update the *AllowToAddGuests* setting in the policy to *False* to stop owners from adding guest members. The organization-wide block on adding guest users set in the policy applies even when individual groups have a group-specific *AllowToAddGuests* setting of *\$True*. In other words, the organization-wide setting trumps an individual group setting.

```
$TenantSettings = Get-MgBetaDirectorySetting | Where-Object {$_.DisplayName -eq "Group.Unified"}
$Values = $TenantSettings.Values
($Values | Where-Object Name -eq 'AllowToAddGuests').Value = "false"
```

Update-MgBetaDirectorySetting -DirectorySettingId \$TenantSettings.Id -Values \$Values

Administrators can add guests to groups even if the *AllowToAddGuests* policy setting is False. The control applies only to owners. Administrators can add a guest using:

- **PowerShell:** By running *Add-UnifiedGroupLinks*, *Add-TeamUser*, or *New-MgGroupMember*.
- **Admin centers:** Through the Microsoft 365 admin center, the Entra admin center, the SharePoint admin center, or the Teams admin center.

Guest accounts that already exist in the tenant directory can join group membership immediately. If you need to add a new guest account to a group, you must create the guest account first. Once the guest account exists, it can be added to a group's membership. The guest won't be able to access any resources until they redeem their invitation to join the tenant.

Turning Off Guest Access

If you update the *AllowGuestsToAccessGroups* setting in the Entra ID Groups policy for Groups to *False*, guests lose access to the groups to which they belong after a brief period to allow cached directory settings to refresh. Think of this as "flipping a switch" to turn access on or off if the need suddenly arises to limit sharing for a tenant. You can restore access later by updating the Groups policy. Guests will continue to have access to individual files for which they have received sharing invitations.

Blocking Guest Access for Selected Groups

Individual groups inherit the settings of the organization policy and use these values unless overridden by settings for individual groups. When a group owner tries to add a new guest to the membership of a group or team, Groups checks the settings of the target group to check if it can proceed with the action. If allowed by the overall organization policy to control guest access to groups, the next check is against the setting for the target group to see if it supports guests. If both checks pass, Entra ID can add a guest to the group's membership.

Two methods exist to control guest access for individual groups:

- The method described below uses PowerShell to manipulate template settings for the group to block guest access.
- Container management sensitivity labels include a setting to control guest access. When an administrator or owner applies a sensitivity label to a group, the group inherits the container management settings, including that for guest access.

In both cases, the group's *AllowToAddGuests* setting is updated to block or allow guest access. After the block is in place, any attempt to add a guest generates an error. Existing guests remain in place and are unaffected by the block. To make sure that no guests have access to the group, you must remove existing guests from the group membership after you block guest access.

The Information Protection chapter contains an example of using PowerShell to find Microsoft 365 Groups with guest members and then check that the label assigned to each group is appropriate. In other words, groups with guests have labels that allow guest access.

Block Guest Access for an Individual Group with PowerShell

The *Get-MgGroupSetting* and *Update-MgGroupSetting* cmdlets retrieve and update group settings. The process to update the settings for an individual group is very like the one used to manipulate a policy setting in the organization policy. The first step is to retrieve the object identifier for a group and store it in a variable. We can do this by running the *Get-MgGroup* cmdlet to retrieve the object identifier for the group. The object identifier is a GUID used to find and update the group object. For example:

```
$GroupId = (Get-MgGroup -Filter "displayName eq 'Office 365 Questions'").Id
```

Now, check that a settings object exists for the group. A group will have a settings object if it has a sensitivity label or if someone created the object using PowerShell:

```
$GroupSettings = Get-MgGroupSetting -GroupId $GroupId
```

If running the cmdlet does not return a value in the `$GroupSettings`, the group does not have a settings object. Groups with assigned sensitivity labels always have a settings object to control guest access. Not having a settings object means that the group follows the organization-level settings. If necessary, we first create a settings object for the group as follows:

- Create a new directory setting template object using the values of the `"Group.Unified.Guest"` template object.
- Create a new group setting and populate the setting with a hash table containing the name `AllowToAddGuests` and the value `false`. The identifier pointing to the group comes from the `Get-MgGroup` command above.

Here's the code:

```
$GroupTemplateId = (Get-MgBetaDirectorySettingTemplate | Where-Object {$_._.DisplayName -eq "Group.Unified.Guest"} | Select-Object -ExpandProperty Id)
New-MgGroupSetting -GroupId $GroupId -TemplateId $GroupTemplateId -Values
(@{'name'='AllowToAddGuests';'value'='false'}) | ConvertTo-Json
```

If the group is assigned a container management sensitivity label that controls external access, the setting applied by the label cannot be overridden by running the PowerShell commands explained here. Settings applied through container management sensitivity labels always take precedence, and if you attempt to override the setting, the cmdlet fails with the `"Assigned label does not allow the group guest setting operation"` error.

To update group settings to allow guests, you reverse the process and either set the value for the `AllowToAddGuests` setting to `true` before update the settings object or remove the policy from the group. This code uses the `Get-MgGroupSetting` cmdlet to read the values from the group and the `Update-MgGroupSetting` cmdlet to update the settings.

```
$GroupId = (Get-MgGroup -Filter "displayName eq 'Office 365 Questions'").Id
$GroupSettings = Get-MgGroupSetting -GroupId $GroupId
Update-MgGroupSetting -GroupId $GroupId -TemplateId $GroupTemplateId -GroupSettingId
$GroupSettings.Id -Values (@{'name'='AllowToAddGuests';'value'='True'}) | ConvertTo-Json
```

If necessary, administrators can add a guest to a group even when its settings prohibit guest membership. This command adds a guest account that already exists in the tenant directory to a group by passing the account alias to the `Add-UnifiedGroupLinks` cmdlet.

```
Add-UnifiedGroupLinks -Identity "Confidential Group" -LinkType Member -Links
SomeUser_outlook.com#EXT#
```

The exception is for dynamic groups, where Entra ID calculates the group membership by running a query against the directory. Administrators can't add individual guest accounts to the membership of a dynamic group except by adjusting the membership rule for the group to include the guest.

See the PowerShell book for information about how to use a script to find groups matching certain criteria and block guest access to those groups.

Restricting Guest Accounts to Certain Domains

Tenants can deploy an Entra ID policy called the *B2BManagementPolicy* to manage the domains that guest users can come from. To access the policy, go to the **External Identities** section in the Entra admin center, select **External collaboration settings**, and scroll down to **Collaboration restrictions**. Three values are available:

- Allow invitations to be sent to any domain (most inclusive): This is the default setting, and it means that invitations to join Groups and Teams can go to users in any other domain.
- Deny invitations to the specified domains: You can create a policy to block invitations going to specific domains. Microsoft believes that using a deny list is the most common scenario as most organizations know the domains with whom they do not wish to share information. For example, you might decide to block guest users with consumer email addresses, and block domains like Gmail.com, Yandex.com, Outlook.com, Yahoo.com, and so on. Including the domains of competitors in a deny list is also sensible. When a deny list is in place, Entra ID blocks any attempt to invite someone to join a group or team if the invitee has an email address in one of the blocked domains.
- Allow invitations only to the specified domains (most restrictive): You can create a policy with an allow list, meaning that invitations can only go to domains in the list. Entra ID blocks any attempt to generate invitations to any other domain that is not on the list.

Applications do not implement blocks. This is done by Entra ID when an application tries to create a new guest account from a prohibited domain.

To create a policy with a deny list, click the deny list button and enter the domains to include and then Save (Figure 10-8). Entra ID supports a policy of up to 25 KB (25,000 characters), meaning that all the settings including the allow or deny list must fit within this limit. In practical terms, this means that it should be possible for the policy to block or allow between 1,500 and 1,600 domains. The allow or deny list specified in the collaboration policy applies to all applications that use B2B collaboration for external sharing, including Groups and Teams.

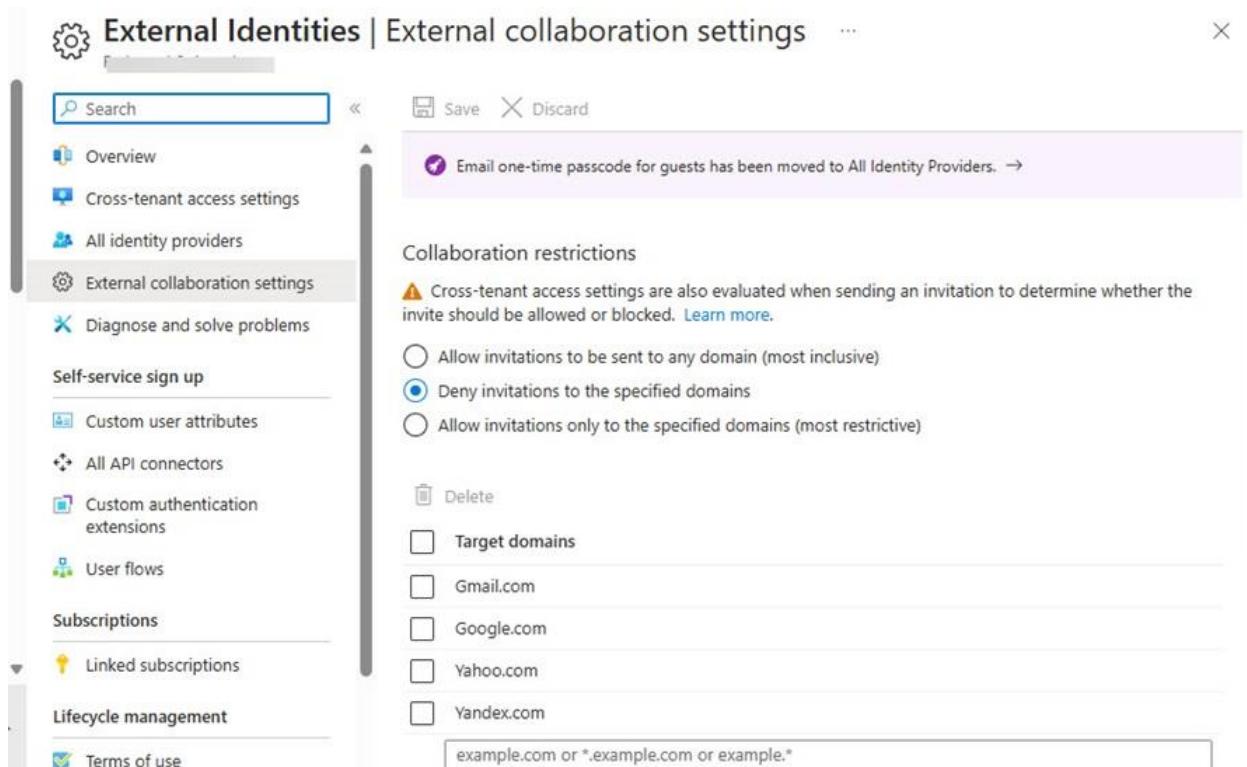


Figure 10-8: Adding domains to the deny list in the B2B collaboration policy

Remember that the policy stops only the creation of new guest accounts. If you want to remove guest accounts from certain domains, you need to take separate action. We'll consider how best to do this shortly.

A tenant can only have a single deny or allow list. If you think that an allow list will work better than a deny list that is already in place, you must remove the current deny list and then create the allow list. The external collaboration list is separate from [a similar list to restrict sharing](#) for OneDrive for Business and SharePoint Online. One list blocks the ability to issue invitations to join groups or teams, and the other blocks sharing invitations for documents or folders. You should synchronize any limitations imposed by the Azure B2B Collaboration policy with SharePoint Online. Inconsistencies in the two lists can cause user problems. For example, a guest user might discover that they can view conversations in a team but cannot access the SharePoint document library.

Finding the Source Domains for Guest Accounts

Before you create your collaboration policy, it's a good idea to check the domains where guests currently in the directory come from. This is easily done with a few lines of PowerShell. This code:

- Finds guests in the tenant.
- Extracts the domain from the user principal name for each guest and stores it in a list.
- Sorts the list and creates a hash table to count the occurrences for each domain, and then sorts the hash table in descending order.
- Outputs the result.

```
$Domains = [System.Collections.Generic.List[Object]]::new()
[array]$Guests = (Get-MgUser -Filter "UserType eq 'Guest'" -All | Select DisplayName,
UserPrincipalName, Mail, Id | Sort DisplayName)
ForEach ($Guest in $Guests) {
    $Domain = ($Guest.Mail.Split("@"))[1]
    $Domains.Add($Domain)
}
$DomainsCount = @{}
$Domains = $Domains | Sort
$Domains | ForEach {$DomainsCount[$_]++}
$DomainsCount = $DomainsCount.GetEnumerator() | Sort -Property Value -Descending
$DomainsCount

Name                                Value
----                                ---
microsoft.com                         59
outlook.com                            11
quest.com                             6
hotmail.com                           5
gmail.com                            4
emea.teams.ms                         4
```

Using PowerShell to Manage Domain Deny or Allow Lists

We can manage the Entra ID policy for external collaboration with PowerShell. For example, to see details of the current B2B Collaboration policy, use this code to run a Graph request against the policy endpoint:

```
$Uri = "https://graph.microsoft.com/beta/legacy/policies"
$Policy = Invoke-MgGraphRequest -Uri $Uri -Method Get
$B2BPolicy = $Policy.Value | Where-Object {$_._displayname -eq 'B2BManagementPolicy'}
```

Name	Value
definition	{"B2BManagementPolicy": {"InvitationsAllowedAndBlockedDomainsPolicy": {"BlockedDomains": []}}
keyCredentials	[{}]
id	14c3fc40-25fd-4f32-a0f0-c3fdd22f7de8
displayName	B2BManagementPolicy
type	B2BManagementPolicy

isOrganizationDefault	True
createdDateTime	08/12/2021 13:59:32

You can update the definition part of the policy with PowerShell, but it's easier and likely to be more accurate to update the policy through the Entra admin center.

Finding Guests from Blocked Domains

Even with an Azure B2B Collaboration policy in place, some unwanted guests might already exist in group memberships. These unwanted guests might have joined groups before you implemented the policy or slipped in because a domain is not in the policy's blocked list. To fix the problem, you can scan the memberships of groups with guests to identify guests from blocked domains. The script starts by:

- Finding the set of Entra ID policies.
- Extracting the B2B Collaboration policy.
- Reading the set of blocked domains from the definition property in the B2B Collaboration policy. The GUID for the policy differs from tenant to tenant.

```
$Uri = "https://graph.microsoft.com/beta/legacy/policies/"
[array]$Policies = Invoke-MgGraphRequest -Uri $Uri -Method Get
$B2BPolicy = $Policies.Value | Where-Object {$_._displayName -eq "B2BManagementPolicy"}
$Uri = ("https://graph.microsoft.com/beta/legacy/policies/{0}/definition" -f $B2BPolicy.id)
$data = Invoke-MgGraphRequest -Uri $Uri -Method Get
$Policy = $data.Value | ConvertFrom-Json
[array]$BlockedDomains =
$Policy.B2BManagementPolicy.InvitationsAllowedAndBlockedDomainsPolicy.BlockedDomains
```

After finding if a set of blocked domains exists, the script proceeds by finding the set of Microsoft 365 groups with guest accounts and checking each group for guests from blocked domains. You can [download the full script from our GitHub repository](#).

A blunter way to solve the problem is to look for guest accounts from a specific domain and remove them from Entra ID. This action removes the account from the membership of any group they belong to and stops access to any document shared through a sharing link.

```
$BadAccounts = [System.Collections.Generic.List[Object]]::new()
[array]$Guests = (Get-MgUser -Filter "UserType eq 'Guest'" -All | Select DisplayName,
UserPrincipalName, Mail, Id | Sort DisplayName)
ForEach ($Guest in $Guests) {
    If (($Guest.Mail.Split("@")[1]) -eq "Gmail.com") {
        $BadAccounts.Add($Guest.UserPrincipalName)
    }
}
If ($BadAccounts) { Write-Host ("Removing {0} bad accounts" -f $BadAccounts.count) }
ForEach ($BadAccount in $BadAccounts) { Remove-MgUser -UserId $BadAccount }
```

Removing and Recovering Groups

The nature of all IT systems is that some groups become unwanted soon after creation or that the use of a group declines over time to a point where it falls into disuse. You might then decide to remove the group from the tenant. As noted previously, you can remove a group from the Microsoft 365 admin center, EAC, OWA, Outlook, a mobile app, or from a group-enabled application like Teams. When you remove a group, the action removes all the connected resources belonging to the group. In addition, group owners or tenant administrators can remove a group by running the *Remove-UnifiedGroup* or *Remove-Team* cmdlets. In this example, we remove a group and suppress the prompt to continue that the cmdlet usually needs before it proceeds:

```
Remove-UnifiedGroup -Identity "Offshore Traders" -Confirm:$False
```

In addition to explicit removals by owners or administrators, if you operate an expiration policy, Entra ID removes groups automatically when they expire after a set period (explained later). In all cases, a removed group and any associated resources first enter a soft-deleted state and stay there for 30 days. During this time, an administrator or group owner can restore the group to make it accessible again to users.

Alternatively, they can force the permanent removal of the group, which means that the resources of the group become irrecoverable. Table 10-5 lists the data recovered for a soft-deleted group.

Group Resource	Data restored
Entra ID	Group object, properties, and membership.
Exchange Online mailbox	Group mailbox holding conversations and group calendar. Also, the SMTP email address. Note – if the SMTP address has been assigned to another group, you cannot restore the original group until you update the SMTP address for that group.
SharePoint Online Team site	Group document library, including the shared OneNote notebook and the folders used by channels within Teams. The site is retained by SharePoint Online for up to 93 days. During this time, the site URL cannot be reused.
Planner	Group shared plan, including the plans created for channels within Teams.
Teams	Team channels and associated messages and metadata such as team and channel properties.
Viva Engage	Conversations in Yammer data store (for Viva Engage communities).

Table 10-5: Data restored when recovering a soft-deleted group

Auditing Group Deletions

When you (soft) delete a group, Entra ID records the details in a “Delete Group” audit record in the audit log. Later, when it removes a group permanently, Entra ID captures a “Hard Delete Group” audit record.

Permanent deletion happens when the *Microsoft Online Service Garbage Collector* process runs, so the exact period when a group is in a soft-deleted state will vary from 30 days to perhaps a few days afterward.

The Report and Auditing chapter contains many examples of how to interrogate the audit log to understand when events occur. For instance, to look back and see when the garbage collector permanently removes groups, we look for “Delete Group” operations (audit records for both soft-delete and hard-delete actions are returned). We can then parse the audit data from the events found using the *Search-UnifiedAuditLog* cmdlet to generate a report using code like:

```
$StartDate = (Get-Date).AddDays(-90); $EndDate = (Get-Date)
[array]$Records = (Search-UnifiedAuditLog -StartDate $StartDate -EndDate $EndDate -Operations
"Delete Group") -ResultSize 5000 -SessionControl ReturnLargeSet
$Records = $Records | Sort-Object Identity -Unique

$Report = [System.Collections.Generic.List[Object]]::new()
ForEach ($Rec in $Records) {
    $AuditData = ConvertFrom-Json $Rec.Auditdata
    If ($AuditData.ResultStatus -eq "Success") {
        $ReportLine = [PSCustomObject]@{
            TimeStamp = Get-Date $AuditData.CreationTime -Format g
            User = $AuditData.UserId
            Action = $AuditData.Operation
            Status = $AuditData.ResultStatus
            GroupId = $AuditData.Target.id[1]
            Group = $AuditData.Target.id[3]
        }
        $Report.Add($ReportLine)
    }
}
$Report = $Report | Sort-Object GroupId -Unique
$Report = $Report | Sort-Object {$_.TimeStamp -as [DateTime]} -Descending
$Report | Format-Table Timestamp, User, Group -AutoSize
```

The script sorts the report data twice. The first sorts by the group identifier to remove duplicate audit records which sometimes turn up in the audit log. The second sorts by date. The output is something like:

TimeStamp	User	Group
18/05/2022 16:37	Tony.Redmond@office365itpros.com	2021 Edition Book
15/04/2022 10:01	ServicePrincipal_1342cefb-7a89-4ee2-af90-c8443053e1e8	Plastic Production (Team)
30/03/2022 17:46	Administrator@office365itpros.com	March 2023 Sales Operations
25/03/2022 17:49	Administrator@office365itpros.com	Sun Seekers
15/03/2022 11:10	James.Ryan@office365itpros.com	Analytics Anonymous

These actions are all soft deletes. The hard deletes to remove the groups permanently happened a month later. The system removals are listed with "Certificate" as the User.

Recovering a Deleted Group

As explained earlier, during the 30-day soft-deleted period, group owners can restore groups with OWA. Administrators can recover groups through the Microsoft 365 admin center, Entra admin center, EAC, or with PowerShell. To recover a group with the Microsoft 365 admin center, select **Deleted groups** under the **Teams & Groups** section.

To restore a group, select it from the list shown in the admin center either:

- Use the **Restore group** option in the group header.
- Click the group name to bring up the details pane, which has some basic information about the (display name, description, and email addresses), and click the **Restore group** button.

Both options do the same to restore the deleted group. After a short delay, Entra ID restores the group object and begins the process of notifying the associated workloads to reconnect. As discussed later, it takes a little while for resources like the SharePoint site, a plan, or a team to be reconnected.

Recovering a Deleted Group with PowerShell

The PowerShell command to list the set of deleted Microsoft 365 Groups is:

```
Get-UnifiedGroup -ResultSize Unlimited -IncludeSoftDeletedGroups:$True | Where-Object
{$_._WhenSoftDeleted -ne $Null} | Sort-Object WhenSoftDeleted | Format-Table DisplayName,
PrimarySmtpAddress, WhenSoftDeleted
```

You can mimic the steps taken by the Microsoft 365 admin center to recover a deleted group as follows. First, retrieve the object identifier for the group you want to recover:

```
$Object = (Get-UnifiedGroup -Identity "Group to Recover"
-IncludeSoftDeletedGroups).ExternalDirectoryObjectId
```

Now, use the identifier to recover the group.

```
Undo-SoftDeletedUnifiedGroup -SoftDeletedObject $Object
```

Reconnecting Group Resources

Because many different applications use Groups, the recovery of a deleted group involves several complex operations. Recovery of a simple group (one that uses Exchange and SharePoint resources only) usually happens within a few minutes and should be complete within an hour. Depending on the current load within the service, recovery of a group that is enabled for Teams or Planner might take up to 24 hours before all the data is reconnected. The added delay is due to the need to synchronize multiple directories and often to ensure that data for Teams and Planner stored in Azure data services are restored correctly. It is also the case that when you restore a dynamic group, it can take up to 24 hours before Entra ID runs the query to calculate the group membership.

The first stage in recovery is to restore the group using the option available in the Microsoft 365 admin center or the Entra admin center. Once the group object is restored, Entra ID notifies each of the attached workloads to tell them to reconnect. As the workloads respond to the instruction, the full set of group resources come online to construct a fully-functional group.

Restoring the directory objects is only the first stage in the recovery process and does not mean that users can use the membership represented in the directory to access group contents. To perform further validation and before telling users that they can work with the group, you should check each of the workloads used by the group using clients to confirm that the expected conversations, files, plans, and chats are present. If you use a browser, make sure that you clear the browser cache or create a private session to avoid any problems caused by stale data. Teams is usually the last application to have its data restored and available to users.

If a workload is not ready an hour or so after the restore, wait for another hour, and check again. Because the restoration process involves many different connections, it could be that one of the steps in the process is waiting for another step to complete.

Time Limit for Recovery

You have 30 days to recover a group following its deletion. After this period elapses, you might still be able to recover some information for a deleted group. For example, administrators might be able to recover files from the SharePoint recycle bin. If a hold is active for the group, you can run a content search to find information in the group mailbox and document library and export those items. However, the search results in a set of unconnected objects. You cannot reassemble them into a functioning group because the group object no longer exists in Entra ID.

Recovering Individual Documents and Items

The possibility always exists that someone will remove a document in error, which then brings the question of how best to restore the now-deleted document. The first place to look is in SharePoint's recycle bin where items stay for up to 93 days after deletion (across the first and second stages). If the item isn't in the recycle bin and you have a backup, you might be able to recover the document from the backup. To prevent SharePoint from deleting items after 93 days, you can assign a retention label to important documents or apply a retention policy to entire sites. Users can delete documents with retention labels or those that come within the scope of a retention policy, but SharePoint keeps the retained items in the preservation hold library, and administrators can restore documents from there.

When someone removes an email conversation from a group, the item goes into the Deletions folder in the group mailbox and stays there for 14 days, after which the Managed Folder Assistant permanently removes the item from the mailbox database. You cannot use the standard Recover Deleted Items feature in Outlook or OWA because it is not available for group mailboxes. During the 14-day retention period, an administrator can recover deleted items by running the *Get-RecoverableItems* and *Restore-RecoverableItems* cmdlets to view and restore deleted items as these cmdlets work with group mailboxes.

Backup solutions from ISVs offer the ability to backup and restore documents selectively, which is a better outcome than having to restore a complete site. AvePoint has a backup solution for Groups that can restore conversations.

Group Expiration Policy

Although it is possible to restrict the ability to create new groups to a select set of users, even in the most tightly managed tenant, some groups eventually reach their best-by date and become disused. If this happens, it is good to track down those groups, recover anything valuable stored in the group resources, and then remove the groups to reduce GAL debris. Groups are not unusual in this respect. Experience shows that

the same falloff in usage over time happens for shared mailboxes, distribution lists, public folders, and other objects shared by teams of people.

To help administrators manage potentially obsolete groups, Entra ID supports the group expiration policy to control how long groups can exist within a tenant before requiring renewal. If groups expire, Entra ID can automatically remove them from the tenant. The expiration policy can apply to some or all groups, no matter which application creates a group, or how people use the group and its resources.

Microsoft automatically creates a disabled group expiration policy for every tenant. An enabled expiration policy requires Entra ID P1 licenses for every member of the groups coming within the scope of the policy. To work with the expiration policy, go to the Entra admin center and navigate to the Groups section. The **Expiration** policy is managed under Group Settings. You can enable the policy, define settings and the groups that come under the scope of the policy.

Name	Object Id	Membership Type	Email
Cricket Lovers (Ar...)	12d57049-89ce-424a-bc...	Assigned	CricketLovers_archived@...
Operations Depar...	0b9313ca-5b39-43a9-bd...	Assigned	OperationsDepartment...
Windows File Ser...	06fc846d-141d-4e38-8b...	Assigned	WindowsFileServerRepla...
Ask HR!	129bfa64-3d11-4d6f-b9...	Assigned	askhr@Office365itpros.c...

Figure 10-9: Updating the group expiration policy settings

The settings in the group expiration policy are:

- The **group lifetime**: The default is 365 days, but you can select a higher or lower value. For example, you could use 730 days to make groups expire after two years. Consider setting a high number of days in the policy initially so that older groups do not expire when you enable the policy and to allow group owners to become used to the idea of expiring groups. For example, Microsoft started with a group lifetime of 360 days and subsequently reduced the period to 180 days.
- The **default notification address**: This handles the situation where a group has no owner. You can specify a single address (usually an administrator) to receive these notifications, the address of a distribution list or group, or the SMTP addresses for multiple recipients (separated by semi-colons).
- The **groups that come under the scope of the policy**: Initially, the value is **None**, meaning that the policy is in the default disabled state and groups do not expire. Selecting **All** means that every group in the tenant comes within its scope. The **Selected** button allows you to apply the policy to one or more groups, up to a maximum of 500 groups. You pick the target groups for the policy from a list of all groups in the tenant (for example, you might decide to exclude all the groups used by Teams from the policy and only include the groups that Teams doesn't use). This is easy to do in a small tenant but can become very tiresome for larger tenants which might span thousands of groups. In this case, you can use PowerShell to script to include the right groups within the scope of the policy. We

explore how to manage the expiration policy through PowerShell in the PowerShell book. Figure 10-9 shows the settings of a group expiration policy that applies to selected groups.

If you change the scope of the policy from **All** to **Selected**, the policy ceases to apply to the groups outside the selected set.

Automatic Renewal

Originally, Groups used an age-based renewal mechanism with the sole criterion for renewal being the time since the original creation date of the group and then, following a renewal, the date of the group's last renewal. Group owners had to renew groups manually, even if the groups are very active. An example of where this might cause a problem is when you use a policy covering all groups in the tenant, including a group used to limit the users who can create new groups. Eventually, that group will expire like every other group. If you ignore the notification, Entra ID removes the group when its expiration period elapses, which means that no one except an administrator will then be able to create a group.

The expiry policy uses a check for group activity. When the time comes to renew a group, Groups looks for evidence that the group is active. A background process called the Activity Tracking Service monitors group activities logged in the Microsoft Graph when users perform activities such as:

- SharePoint Online (group document library): View, edit, download, share, or upload files.
- OWA: Join a group, read, or send messages to group conversations, or like a message. Note: sending emails to contribute to a group conversation is not considered a renewal activity. The interaction must happen through OWA.
- Teams: Interact with a channel in the team.
- Viva Engage (network configured in Microsoft 365 mode): View a post in a Viva Engage community or use Outlook to respond to an interactive message.

It's obvious from this list that group renewal never considers some common activities when calculating group activity. For example, the process ignores adding tasks to Planner plans. Even in the workloads which are covered, many activities go unremarked, like participation in Teams meetings, using apps in channels, or assigning retention or sensitivity labels to SharePoint documents.

Many signals for the selected set usually exist for an active group, and when the time comes for renewal, Entra ID renews the group for a further period without the need for owner intervention. If the renewal process finds no activity signals for a group, the group owners receive group expiry notification messages and must go through the normal renewal process. At the Ignite 2020 conference, Microsoft said that 79% of all groups coming within the scope of an expiration policy automatically renewed because of their activity. That's an impressive number, but the fact that 21% of groups didn't auto-renew because of a lack of activity gives pause for thought as it means that over a fifth of all groups created did not have enough activity (as measured by the limited set of signals) to allow Microsoft 365 to auto-renew them.

Logging the Renewed Date

The *renewedDateTime* property of a group holds the last renewal time for a group (or the time of creation). Entra ID maintains the property to know when a group expires. After you renew or restore a group, Microsoft 365 updates its *renewedDateTime* property with the current date and time to give a new starting point for the group's expiry countdown. Records for the update to group properties are logged in the Audit logs section of the Entra admin center.

Expiry Notifications

No one wants a system to remove data without warning. When an expiration policy is active, Entra ID checks the last renewed date for every group covered by the policy. The auto-renewal process takes care of groups

that are active (see the discussion above). For groups that have no activity signals in the Graph, warning notifications are sent to group owners to tell them when their groups need renewal.

Exchange Online sends expiry notifications using email irrespective of how groups are created or used. Group owners must check their mailbox regularly for expiry notifications. If not, they might overlook a notification to inform them about the impending expiration of a group and Entra ID ends up removing the group unexpectedly. Teams exposes the expiration date for a team in its settings (*Manage team > Settings > Team expiry*) and allows team owners to renew the underlying group for the lifetime defined in the policy. As explained earlier, group owners can also renew a group through the **Manage groups** section of OWA.

Three warning notifications are sent before Entra ID removes a group:

- 30 days before the group expires.
- 15 days before the group expires.
- One day before the group expires.

For example, if the expiry interval is 365 days (one year), the timeline in Table 10-6 applies. (You cannot change these intervals as they are hardcoded).

Days	Action
1	Group created (or renewed).
335	First expiry notification sent to group owners.
350	Second expiry notification sent to group owners.
364	Final warning sent to group owners.
365	Expiry period reached. Entra ID soft-deletes the group.
395	The 30-day soft-delete retention period expires. Entra ID removes the group permanently.

Table 10-6: Timeline for Group Expiry

When they receive notifications, group owners decide whether to renew the group or let it expire. To help owners decide whether they wish to renew the group, notifications include links to:

- **Outlook:** Open the group and view the conversations that are taking place to see the last time that anyone was active. If the group is used for Teams, none of these events are captured.
- **SharePoint:** Open the document library in a browser to reveal the documents stored there. Because Teams uses the SharePoint library to hold its files, including a folder for each channel in a team, this is a valuable indicator of activity in a team.
- **Teams:** If the group is team-enabled, open the team, and expose the channels, conversations, and apps inside the team.
- **Group details:** Open the Entra admin center in a browser to reveal information about group members and owners.

Group Renewal

To renew a group, an owner clicks the **Renew group** button in the notification message. This brings them to the Entra admin center to renew the group. Three things can happen:

1. If the group still exists and has not expired, Entra ID renews the group and signals success. An “Updated Group” audit record is captured because the renewal updates the group’s *RenewedDateTime* property. The same action occurs when a group is renewed from Teams.
2. If the group is soft-deleted, Entra ID restores it and sets a new expiration date.
3. If the group is hard deleted (permanently removed from the tenant), the owner sees an error message. The group is no longer recoverable.

If you decide not to renew a group and let it proceed to deletion, consider preserving any valuable information that exists in these resources before the deletion happens. This is not an automatic process, and it will take time and effort to retrieve information.

After the expiration period expires, Exchange Online soft-deletes the group and sends a final email to the group owners to inform them about the group deletion. All group resources are removed at this point – the group mailbox, team, plan, and SharePoint site, but kept in a restorable state. A group owner can restore the group for up to 30 days following the deletion. The notification message shows the drop-dead date, and once this period passes, the group becomes irrecoverable.

Normally, Entra ID soft deletes expired groups. Special processing occurs if groups expire at the point when a tenant enables the policy. In this case, owners receive a specific notification that's treated as a second reminder. In effect, even though their groups are already technically expired, the owners have 15 days to renew these expired groups.

Restoring Expired Groups

When a group expires, the expiration process moves the group into a soft-deleted state and its owners get a confirmation that Entra ID removed the group. The notification includes a **Restore group** button that the owner can click to restore the group and bring it back from the dead. Group owners can also restore a group through OWA.

Like any other soft-deleted group, Entra ID permanently removes the group after 30 days, so you have limited time to restore a group. Alternatively, you can use the steps described earlier to recover a group.

Dynamic Microsoft 365 Groups

Microsoft 365 Groups support both static (fixed) and dynamic membership. Static membership is where you add and remove people from group membership via a client or programmatically. Entra ID computes the membership of dynamic groups by using membership rules to query the properties of Entra ID user accounts (dynamic groups also support devices; this discussion focuses on user accounts). The properties available for dynamic group membership rules are [documented online](#). The properties most commonly used to build membership rules for dynamic groups include department, job title, office location, country, and the tenant-specific values stored in the fifteen custom ("extension") attributes.

Dynamic membership is useful when you have groups that change often and whose membership can be determined by reference to one or more attributes of user accounts. For example, the people who work in the Madrid office, or everyone in the Engineering department. Teams, Outlook, and Viva Engage support dynamic groups.

Because of the processing load required to maintain dynamic group membership, Entra ID restricts the number of dynamic groups and dynamic administrative units combined per tenant to 5,000. Dynamic administrative units use the same kind of membership rules as found in dynamic groups.

The methods available to create a dynamic group are:

- **Entra admin center:** Set the type for the group to "Microsoft 365" and its membership type to "Dynamic User." You'll also need to add a membership rule.
- **PowerShell:** Run the *New-MgGroup* cmdlet. Due to the difficulties of making sure to build complex membership rules to find members in Entra ID, we recommend using this method only for dynamic groups that use simple queries. An example of creating a dynamic group with PowerShell is described in the PowerShell book.

Although you can create a dynamic group with PowerShell, the need to configure and test membership rules to find the correct group membership means that it's often easier to create and manage dynamic groups through the Entra admin center. In the Groups section, select the option to create a new group. Choose *Microsoft 365* for the group type and *Dynamic User* for the membership type and enter a name and description for the new group. The final step is to configure rules for the dynamic query used to find group members.

You can also create a static group through the Microsoft 365 admin center and change it to dynamic membership in the Entra admin center. You can also switch a dynamic group to static membership by editing its properties. When this happens, Entra ID removes the membership query from the group and creates a static membership based on the current members. You can switch the group back to dynamic membership afterward, but you must then re-enter the membership query.

Group owners and administrators cannot update the membership of dynamic groups through OWA, Outlook, or the PowerShell **-UnifiedGroupLinks* cmdlet. The only methods available to change membership are:

- Alter the group's membership query to find another set of users.
- Update the properties of individual user accounts so that they come within the scope of the group's membership query.

Dynamic Group Owners

Like any other group, a dynamic group must have at least one owner. The ownership of a dynamic group is static in that the membership rule used to compute group membership has no effect on owners. Instead, administrators manage group owners using the Entra admin center or with PowerShell. To find the current group owners, run the *Get-MgGroupOwner* cmdlet:

```
[array]$Owners = Get-MgGroupOwner -GroupId (Get-MgGroup -Filter "displayname eq 'Marketing Department'").Id  
Write-Host "Group Owners are" $Owners.AdditionalProperties.displayName
```

Membership Rules

You can choose between a simple rule or an advanced rule for the query. A simple rule checks against the value of user account attributes such as Department, JobTitle, City, or Country. An advanced rule combines checks against multiple properties to find the accounts to include in the group and includes some of the more complex checks using operators like *-in*, *-notin*, and *-any*. The *-in* and *-notin* operators are especially valuable in comparing the value of user attributes against a list of values (such as countries or department codes). The maximum size of an advanced rule is about 3,000 characters. Before creating membership rules (or before debugging existing rules), it's a good idea to read the [Microsoft documentation about how to create efficient rules](#).

In Figure 10-10, we see an advanced rule based on a modified version of one of the examples in the [documentation for membership rules](#). The examples are useful basics to start building membership rules and include:

- How to find user accounts with specific email addresses.
- How to build a rule for the direct reports of a manager.
- How to use custom (extension) and security attributes in membership rules.
- How to create membership rules for different types of devices.

In this instance, the intention is to find accounts that have licenses enabled for the Teams service plan, and it's done with this query:

```
user.assignedPlans -any (assignedPlan.servicePlanId -eq "57ff2da0-773e-42df-b2af-ffb7a2317929" -and
assignedPlan.capabilityStatus -eq "Enabled")
```

The membership rule checks the service plans assigned to accounts and looks for an enabled license for the plan identified by the GUID. It will find any user assigned a product that contains the Teams service plan. This page [lists GUIDs for service plans and product SKUs](#).

Figure 10-10: Creating rules for dynamic membership of a Microsoft 365 group

Membership rules don't allow you to mix properties of different types. For instance, the rule to check for Teams licenses uses the *assignedPlans* multi-value property. You can't combine filtering against that property with a check against the department or country properties because both of those properties are single-value strings. If you try, Entra ID signals a "*mixed use of properties from different types of object*" error.

The **Validate Rules** option allows you to input accounts to see if they match the criteria set for the group, which is a useful way of checking the effectiveness of the query. To test the example shown in Figure 10-10, you can select a mix of accounts with and without the license to check that the query generates the correct results.

A variation of the query is one that finds any licensed account. It's easy to find all member accounts, but many accounts are not used by humans, and there's not a good filter to find just those accounts. A quick and dirty solution is to find accounts that have any enabled license with a query like this:

```
user.assignedPlans -any (assignedPlan.capabilityStatus -eq "Enabled")
```

When the query is complete, save it, and create the group. After creation, it can take a little time before the new group shows up everywhere within Microsoft 365. This is because of the need to synchronize information between Entra ID and other workloads. It will also take Entra ID some time to calculate the membership of the group. The two biggest factors are the overall size of the tenant directory and the number of matching entries. Entra ID can easily support dynamic groups of more than 10,000 members and Microsoft has reported (Ignite 2020) that they created and used a dynamic group containing more than 100,000 members. When Entra ID completes its scan for matching objects, you will see "update complete" as the membership process status in the overview properties for the group together with a timestamp when Entra ID last calculated the group membership. A list of members is available through the **Members** link in group properties. Entra ID does not include disabled accounts when calculating dynamic group membership.

Following the update of a dynamic group's membership rule, Entra ID recalculates the group membership. Microsoft has a 24-hour SLA to resolve the membership query and update the membership of dynamic groups. Experience proves that Entra ID usually processes changes much faster and you can expect that a change to the membership rules should be active within a few hours.

Restriction in Rule Builder: The dynamic group rule builder in the Entra ID and Intune admin centers don't support the use of the *contains* or *Notcontains* operators in membership rules. Microsoft blocked these operators from the rule builder to encourage administrators to create more performant membership rules. However, you can still use the operators by editing a membership rule without using the rule builder. See [this article](#) for more details.

Checking Dynamic Membership

If you are uncertain about the query or want to confirm that it will generate the expected results, you can use the *Get-MgUser* cmdlet to execute a similar query against Entra ID and check the results that it reports. If the results from both queries match, you know that everything is working as expected. Here is an example of how to look for accounts using an advanced query:

```
Get-MgUser -All -Filter "Department eq 'IT' and Country eq 'Ireland'" | Format-Table DisplayName, Department, Country
```

DisplayName	Department	Country
Andy Ruth (Director)	IT	Ireland
David Pelton (Sales)	IT	Ireland
Luka Abrus (Sales)	IT	Ireland

You can then compare the membership calculated with the filter with the data reported by running the *Get-UnifiedGroupLinks* cmdlet against the group.

```
Get-UnifiedGroupLinks -Identity "IT Ireland" -LinkType Member
```

After Entra ID resolves the membership rule to compute the group membership, you can read member information from the group:

```
$GroupId = (Get-UnifiedGroup -Identity "Marketing Department").ExternalDirectoryObjectId
$Members = (Get-MgGroupMember -Group $GroupId)
Write-Host "Group Members are" $Members.AdditionalProperties.displayName
```

Alternatively, if the Exchange Online management module is not loaded, use the *Get-MgGroupMember* cmdlet without first calling the *Get-UnifiedGroup* cmdlet. This command works for both security groups and Microsoft 365 groups. For example:

```
[array]$Members = Get-MgGroupMember -GroupId (Get-MgGroup -Filter "displayname eq 'Marketing Department").Id
Write-Host "Group Members are" $Members.AdditionalProperties.displayName
```

The technique used to display a list of member names is slightly odd. It's because the Microsoft Graph PowerShell SDK cmdlets return a set of object identifiers for group members with their other details in the *AdditionalProperties* property. The same technique works to return the names of members of a dynamic administrative unit, albeit with a different cmdlet:

```
$AUData = Get-MgAdministrativeUnitMember -AdministrativeUnitId (Get-MgAdministrativeUnit -Filter "displayName eq 'Guests AU").Id
Write-Host "Members of the administrative unit are: " $AUData.AdditionalProperties.displayName
```

Pause Membership Processing

An administrator can pause processing of group membership if required. When a pause is in effect, Entra ID won't attempt to evaluate the membership query, so the group membership remains the same. The option to control membership processing for a dynamic group is available when viewing group properties in the Entra admin center. Additionally, you can pause and reset membership processing for a group using the *Update-MgGroup* cmdlet. For example, these commands pause and then resume update processing for a group:

```
Update-MgGroup -GroupId e9bbac2f-3bfe-4751-9f25-9ebe38dff569 -MembershipRuleProcessingState Paused  
Update-MgGroup -GroupId e9bbac2f-3bfe-4751-9f25-9ebe38dff569 -MembershipRuleProcessingState On
```

The properties of a dynamic group tell you the current state of processing and when the last membership change happened. Common processing states are:

- *Succeeded*: Entra ID has evaluated the membership query and the membership is up to date.
- *Evaluating*: Entra ID is currently resolving the membership query to identify group members.
- *Processing*: Entra ID is currently processing the membership.
- *Processing error*: Entra ID was unable to evaluate the membership query.
- *Updates paused*: An administrator has paused updates. The membership remains static until updates resume.
- *Not started*: Entra ID has not started to evaluate the membership query.

User Access to Dynamic Groups

User access to dynamic Groups works identically to groups that have static membership. Every time someone tries to access a group resource, Entra ID checks whether they have the necessary permission and if so, the user gains access. Like regular Groups, messages sent to a dynamic group exist as conversations in the group mailbox. Groups automatically adds members as subscribers so that they receive copies of all contributions to group conversations via email. One difference between a static and dynamic group is that Groups does not add the user who creates the group to the member list. This is because the query for the group defines the membership. Unless the account that creates the group comes within the scope of the query, the group owner is not a member and therefore cannot access group resources. Likewise, the group owner is not part of the subscriber list.

Users do not receive notifications when they lose membership of dynamic groups due to a change in the query that populates the group membership or because their account details have changed. The first time someone is likely to discover that they no longer are a member is when they try to access some group resources.

Licensing Dynamic Microsoft 365 Groups

The use of dynamic Microsoft 365 groups means that administrators who create and update dynamic groups plus any user whose account falls under the scope of a filter used by a dynamic group need Entra ID P1 licenses. In other words, if you create a dynamic group that has a filter that resolves to every person in the organization, you need to buy an Entra ID P1 license for all those users. In most cases, it is better to use a standard dynamic distribution list to communicate with large sets of employees because you avoid any licensing issues and will not exceed the supported limit for group membership. If you want to use something like an "All Employees" group to foster a sense of collaboration rather than simply a means of sending out information, a Viva Engage community might be a better choice.

Microsoft does not enforce the licensing requirement for dynamic groups. Those who create or update the queries for dynamic groups need a license before the Entra admin center allows them to change queries, but the query used in groups returns all matching accounts found in the directory even if some do not have the

necessary license. Microsoft might enforce the licensing restriction in the future. When that happens, queries will return licensed accounts only.

Because dynamic groups come at a cost, you should be careful to decide which groups should be dynamic, and which can stay with static membership. Before creating a new dynamic group, ask whether the membership is likely to change over time. If you expect a low turnover in group membership, then static membership is a better choice as it will not incur an extra cost and the membership is not dependent on the directory. On the other hand, organizations that manage many groups whose membership is volatile (such as the students who sign up for a class) and can calculate group membership by querying one or more of the supported directory attributes for dynamic membership might be able to justify the cost.

Using Dynamic Groups with Teams and Planner: You can use a dynamic group with Teams but not with Planner, which depends on fixed team membership. Dynamic groups are intended for groups whose membership is highly volatile and whose communication is email centric.

Comparing Email Dynamic Distribution Lists and Dynamic Microsoft 365 Groups

Experience in using Exchange dynamic distribution lists suggests that dynamic membership is a popular feature. Some obvious differences exist in the implementations of the two types of dynamic groups. Table 10-7 compares the two ways to create objects with dynamic membership inside Office 365.

Attribute	Dynamic distribution list	Microsoft 365 dynamic list
Resolved against	Exchange Online Directory (EXODS)	Microsoft Entra ID
Used for	Email	Teams, Outlook Groups, Viva Engage (Yammer)
Purpose	Send email to list members	Send email and calendar events to group members and manage access to Microsoft 365 resources like SharePoint sites and plans
Supported objects	Any mail-enabled recipient type (including hybrid objects)	User and guest accounts
Licensing	Included in Exchange Online	Entra ID P1
Syntax for query rules	OPATH	ODATA
Filters based on	Exchange object attributes	Entra ID object attributes

Table 10-7: Comparing Exchange Online dynamic distribution lists and dynamic Microsoft 365 groups

Groups and Compliance

As explored elsewhere in this book, compliance technology exists to help companies follow the regulatory and legal frameworks that apply to their business activities. Groups use Microsoft 365 compliance features rather than workload-specific features. For example, you can include group mailboxes and the group document libraries in simple content searches, or the searches associated with standard or premium eDiscovery cases. Retention policies can apply to content held in group mailboxes and document libraries and group owners can apply retention labels to conversations to keep those items for compliance purposes.

Viva Engage communities store messages in the Yammer data store. Compliance records for eDiscovery are generated if the Yammer network is configured in Microsoft 365 native mode.

Controlling Group Creation and Compliance: One aspect of compliance sometimes overlooked is the desirability of controlling group creation. If you allow everyone to create groups, you might end up with an unmanageable mess. Not only will obsolete and unwanted groups clutter up the tenant, but their presence does make it harder to figure out what groups hold information needed for compliance purposes. If compliance is of concern, consider applying a policy to control group creation so that you know what groups exist, their purpose, and whether they should come under the control of compliance policies.

Viva Engage and Groups

Microsoft bought Yammer for \$1.2 billion in June 2012 to gain a presence in the enterprise social networking market. Facebook defines the concept of a social network to many people, a feeling emphasized by the film of the same name that charts the development of Facebook from an application used to connect college students in an electronic yearbook to a platform that supports billions of users today. Facebook is a public social network that is open to anyone who cares to join. An enterprise social network offers much the same communication and collaboration facilities offered by applications like Facebook, but inside the confines of a single enterprise. Of course, you can stretch the concept of a single enterprise to a public space, as in the case of Microsoft's original Office 365 Network where Yammer hosted over 88,000 members discussing technical issues and ideas in the many groups that reflect the different interests of customers. Microsoft transitioned the Office 365 Network to the Microsoft Technical Community platform in September 2016. In February 2023, Microsoft decided to rename Yammer as Viva Engage.

Microsoft enables Viva Engage for all enterprise tenants, and the app supports browser, Apple iOS, Android, and Mac clients. Once activated, you can use Viva Engage in diverse ways. Some find that it is an excellent way to introduce users to cloud applications because its communities work very much like other social networking networks. Anyone who is familiar with those applications can quickly become productive with Viva Engage. Given a well-curated set of groups for people to go to find and share information, Viva Engage can quickly become an important success factor in a Microsoft 365 deployment, especially when the number of potential users who might contribute to conversations is more than can be accommodated by Groups or Teams.

Viva Engage supports sharing across communities (in other words, you can cross-post a conversation to have it appear in multiple communities). Users can post [video, text, and graphic stories](#) to their "storyline" to share information more broadly within the organization. And of course, Viva Engage is well-equipped with reactions and emoticons. Integrations are available with other applications such as Dynamics 365 and SalesForce.com.

Viva Engage is collaboration writ large, created with the enterprise in mind. It is best when used by hundreds or thousands of contributors meeting in groups dedicated to different topics, especially when contributors are geographically remote from each other. Some examples of Viva Engage communities are cross-company knowledge sharing or distributing information on behalf of specific parts of the business, such as an HR discussion group or an IT suggestions group.

Any consideration of collaboration for a Microsoft 365 organization should take Viva Engage into account. You should lay out the needs of the organizations and map those needs against the different applications available. You can then decide which type of group is best suited to specific scenarios. Although the question seems a tough one to answer, the reality is that most organizations will find the choice relatively straightforward. Most tenants will standardize on a certain type of collaboration and use it wherever possible. Those who have used email in the past will continue to do so with Outlook-based groups while organizations that deploy Viva Engage will continue to use Viva Engage communities. Teams has replaced the use of email in many internal communication scenarios and is often easier to deploy, so it's another factor to consider.

Collaboration Overlap

Anyone looking at the collaboration options available will probably conclude that some overlap exists. Why use Groups instead of Viva Engage or vice versa? How do these applications compare to Teams? These applications allow users to contribute to discussions and preserve contributions so that they are accessible to other users who join the debate after it starts. The applications support the sharing of files and are accessible through a browser interface – and that is pretty much where the similarities end.

Because Outlook groups can act as distribution lists, they are easy to deploy. Users who interact with Outlook Groups through email and never access the shared resources will probably think of them as another form of distribution list. You send messages to groups and copies arrive in the mailboxes of any member who subscribes to the group. Given the large population of Exchange Online mailboxes, Outlook groups have a lot of room to grow.

Viva Engage is different. You can certainly interact with communities through email, but the experience is less seamless. The decision to deploy any collaboration technology needs more thought and preparation than simply turning it on. Such an approach will invariably result in a couple of active communities (for some period) and a lot of stagnation. Any project to introduce a new form of collaboration to an enterprise, even though people are aware of the power of social networking through their exposure to consumer versions, needs planning, evangelism, leadership, endorsement from executive level, and a whole lot of energy applied to get the network going, including the identification of suitable ways to use the network to solve real-life business problems. An electronic chat room is nice to have but worthless in the long term; an active social network that brings people together on an ongoing basis to debate, refine, and drive solutions to identifiable and quantifiable business issues is invaluable.

Today, the role for Viva Engage within Microsoft 365 is two-fold:

- **Enterprise social networking:** This is the core role and one that Viva Engage succeeds in delivering for some (usually large) enterprise accounts, many of which heavily invested in Viva Engage as their corporate employee communication strategy. In other organizations Teams takes this role.
- **Employee engagement:** Just like SharePoint Online delivers document management to other Microsoft 365 apps and Exchange Online delivers messaging services, Viva Engage delivers services to help drive better employee engagement. An example is the Q&A capability available for Teams meetings.

Viva Engage introduced “stories” and the “storyline” in late 2022. Stories are brief photos or videos (3 minute maximum) shared to inform the organization about some news. It could be a product announcement, information about an event, or personal reflection. Stories appear on user storylines, which can also feature regular posts. Users can follow others to make sure that they see their stories, which also appear in the Viva Engage app.

Network Modes

Viva Engage organizes communities into a network. Older deployments could support multiple networks within a single tenant, but now it’s more common to find a single network per tenant. The network mode can be:

- [Native mode for Microsoft 365](#). As of January 2020, all new enterprise networks start in native mode (and can’t change to any other mode).
- Non-native mode. All external networks are in this mode. External networks are those which support people outside the organization. In May 2023, Microsoft began the process of retiring support for 1:many mode (prohibited for new networks since October 2018), meaning that [an organization is limited to one external network](#).

- Hybrid mode. Another older mode that is replaced by native mode.

Running a network in native mode is best for Microsoft 365 because:

- Microsoft 365 administrative tools manage Viva Engage users and communities. Groups manage the membership of communities. A special group is created for the "All Company" community with no membership. All tenant administrators are added as owners of this group. In the case of other communities, network admins must have the appropriate Microsoft 365 permissions to manage the membership of communities where they are not group owners. The Groups used by Viva Engage are inaccessible to clients of other group-enabled applications (like Outlook).
- Each community can access resources like a SharePoint Online team site. The files uploaded to a community are in a document library on its team site.
- Viva Engage generates compliance records for conversations. The compliance records for a discussion are in the group mailbox belonging to the community and are discoverable by content searches.

See [this page](#) for more information about migration to native mode.

Communities

The original Yammer nomenclature referred to collection of users as "groups." In late 2019, Microsoft announced that "communities" more accurately reflects the kind of knowledge sharing and community building that Viva Engage excels at. Communities still use Groups to manage their identities and membership and connect to group-provisioned resources like SharePoint sites.

When a community uses a Microsoft 365 group, you can work with the group using the Groups cmdlets in the Microsoft Graph PowerShell SDK and Exchange Online modules, or by using Graph API queries. For example, you can set the classification or access type for a community by running the *Set-UnifiedGroup* cmdlet. You can also recover a deleted community using the process to recover a deleted Outlook group. Although you can add members to a community using the *Add-UnifiedGroupLinks* cmdlet, it is best to manage membership through and this minimizes any directory synchronization lag.

Communities in networks configured in Microsoft 365 native mode support Azure B2B collaboration guest user accounts. The functionality only works for external accounts in other Office 365 tenants. Microsoft hopes to support external access for Microsoft Service Accounts soon.

Discussions

Leaving Microsoft Teams aside, tenants have a choice of technology to host group discussions: Viva Engage or Exchange (Outlook Groups). The major difference between communities and Outlook Groups is that Viva Engage keeps its conversations in the Yammer data store while an Outlook group stores its conversations as items in the Inbox folder in a group mailbox. A community that uses the Groups service is easily identifiable because it lists links to the group-connected resources provisioned for the group (Figure 10-11).

Viva Engage supports marking communities as "official," as a way of increasing the status of a community and the discussions contained there. For instance, an organization might mark an HR Community as official to encourage people to ask questions relating to HR policies and regulations there. Among the other features are:

- Mark conversations as announcements to give them extra importance. Community members receive email notifications for announcements even if they disable email notifications.
- Threaded conversations.
- Delegate access (users can allow others to post on their behalf in communities both people belong to).
- Feature a conversation (pin it to the top of the feed).

- Ask and answer questions. You can also change a regular conversation to become a question. Viva Engage uses different formatting to highlight questions in user feeds.
- View insights (statistics) about a conversation.
- Restrict posting of new topics in communities to administrators.

Instead of posting to a community, users can post to their storyline. These posts are available to everyone in the network. User storylines can also feature photo and video stories, short snippets to inform others about something that's happening.

Figure 10-11: A discussion in a Viva Engage community

Although you cannot transform a community to become an Outlook group or vice versa, it is possible to run the two types of groups alongside each other. After all, both use a common group framework, and the only major differences are the storage of conversations and the clients that people can use to access a group. Outlook and OWA cannot access conversations in a community. Access to community conversations is only possible through the Viva Engage browser and mobile clients. Although they do not use Exchange Online for messaging, members of communities can still send messages and users can also send messages to communities.

Actionable Notifications

As conversations happen in communities, members can choose to receive notifications via email. Traditionally, the notifications were simple messages with a clickable link to open a browser and go to the conversation. Notifications include a *"fully-interactive thread"* with the ability to:

- See the complete conversation.
- Like a comment in the conversation.
- Share the conversation with another community.
- Know how many people have already seen the conversation.
- Add people to a conversation.

- Post a comment to the conversation from OWA, including attaching files and images or @mentioning people in a comment.
- Vote in polls.

Actionable notifications only work in OWA. Other clients see the older-style notifications.

Viva Engage Compliance Records

When a network is configured in native mode, it stores compliance records in the *MessageIngestion\Yammer* folder in the non-IPM part of user and group mailboxes. The records are created by the Microsoft 365 substrate when people post new messages to communities or private conversations. Records are available for different forms of posts, including polls, questions, discussions, and so on. Graphics and GIFs included in posts are captured. Reactions to posts are the only element that the substrate does not capture.

The example below uses the *Get-ExoMailboxFolderStatistics* cmdlet to examine and report what it finds in the folder:

```
Get-ExoMailboxFolderStatistics -Identity "Company-Wide Debate" -Folderscope NonIPMRoot -  
IncludeOldestAndNewestItems | Where-Object {$_.FolderType -eq "Yammer"} | Format-Table Name,  
ItemsInFolder, NewestItemReceivedDate  
  
Name      ItemsInFolder NewestItemReceivedDate  
-----  
Yammer        6213 1 Jun 2023 12:12:17
```

When run against a user mailbox, the code reports the number of compliance records created for posts to communities and private messages sent by that user. Using compliance records is often used to track activity in groups. This script in the [Office 365 for IT Pros GitHub](#) repository generates an activity report for communities using the compliance records, including calculating how long it has been since anyone posted to a community.

Evaluating Viva Engage, Groups, and Teams

Occasionally, Microsoft 365 offers many ways to get work done. Selecting the right tool for team collaboration is one of those areas where overlap exists. Groups offer a solid choice for teams to work together based on email while Teams delivers a chat-based workspace that works well for small to medium teams. Groups, Teams, and Viva Engage support guest user access (the network must run in Microsoft 365 mode).

Because many factors drive the choice of the best collaboration tools for an organization, it is hard to make a choice and say that any one tool will handle all circumstances and contexts. No collaboration tool ever invented in the history of technology has been able to make that claim in any credible sense.

Some guidelines can help administrators and users select the best form of collaboration technology for a specific task. The following might serve as a basis for discussion:

- An **Outlook group** is an excellent choice when a team requires a collective repository where they can share documents, a OneNote notebook, and a calendar, and discuss topics through email. It is likely that the group has a well-defined purpose and might be part of the organizational structure, like a department or location. Because these groups often serve as a direct replacement for traditional distribution lists, the email traffic can be relatively high compared to the number of files generated in the document library. Together, the files and conversations held in the group represent its collective history and are valuable in terms of bringing new members up to speed with the group's activities.
- **Teams** is a good choice for small to medium projects where sets of people come together to execute specific tasks. Deadlines are likely to be in place for the team to achieve and this encourages a certain kind of focused and rapid conversation between team members that Microsoft refers to as "high-velocity chats". The chats tend to be short and informal. The intention behind a team is to get work

done rather than to accumulate knowledge. When the project or work item is complete, the team members might disband and come together in other teams.

- **Viva Engage Communities** are an effective way to share knowledge broadly within large communities. They work well as public forums within companies, where Viva Engage can be the basis for communities who share a common interest. Unlike Teams and Groups, which configure their groups to be private or public, communities often host unstructured audiences that flex over time. The information held in communities is often not as specific as found in Groups or Teams but is no less valuable. Indeed, the knowledge developed through the contributions of the higher number of users supported by Viva Engage often has long-lasting value for the entire company.

Considerable overlap exists between the various methods. An Outlook group might be as good a choice as a team in some circumstances. Some companies use nothing but Viva Engage and are quite happy with their choice. Some consider that Teams revolutionize the way that small groups work. All of which proves that collaboration is uniquely individual to a company or organization. No one size fits all, which is why choice exists within Microsoft 365.

Distribution Lists

Distribution lists or distribution groups have existed in email systems since the early days of the technology. A distribution list is a collection of known email recipients which gives users the ability to send emails to everyone on the list through a single recipient. The membership of a distribution list is composed of mail-enabled recipients registered in the Exchange Online directory and accessible through the GAL:

- User and shared mailboxes.
- Mail-enabled public folders.
- Other distribution lists, including dynamic distribution lists.
- Mail contacts. You can include a Teams channel in a distribution list by creating a mail contact using the channel's email address.
- Mail users (including those created for guest accounts).
- Microsoft 365 Groups (these objects can only be added using PowerShell).

A single distribution list can span up to 100,000 members. The Exchange Online transport system calculates the total recipient count after expanding the distribution list, including any nested distribution lists and dynamic distribution lists in the membership. If you use Azure AD Connect to synchronize with an on-premises directory, a lower maximum of 250,000 members applies. After it expands the set of individual recipients, Exchange figures out how best to route a copy of the message to each recipient. It is at this point that Exchange imposes other limits, such as the 25 MB maximum message size that can be sent to distribution lists of up to 99,999 members.

If your tenant uses large distribution lists (more than 5,000 members), Exchange forces you to configure delivery management restrictions for those lists to lessen the possibility of people sending messages to the lists in error. Sending a 5 MB message to a distribution list containing 100,000 recipients imposes a huge load on the service. Limitations include specifying a set of mailboxes allowed to send messages to large lists or imposing moderation on those lists so that messages must be approved before Exchange distributes copies to all members.

Normally, the sole purpose of the distribution list is to act as a convenient way to send messages to multiple people. Alternatively, a distribution list can be a mail-enabled security group (MESG), which means that you can use it to send mail and control access to resources, such as access to a shared mailbox. You cannot change a distribution list to make it a mail-enabled security group or vice versa.

The perceived wisdom expressed by Microsoft and many others is that Microsoft 365 Groups are more functional and productive than distribution lists and that users will benefit if organizations upgrade distribution lists to become Groups. For this reason, Microsoft offers multiple methods to convert distribution lists. Notwithstanding the features available to Groups, valid reasons still exist to continue using distribution lists, including:

- The ability to include different mail-enabled recipient types in group membership. For instance, mail contacts, mailboxes, and other groups.
- No licensing requirement to use dynamic distribution lists.
- Easier interoperability with other third-party email systems.
- Ability to nest distribution lists.

Microsoft is aware of where the functionality of Groups lags the capabilities of distribution lists and is working to close the gap, so this is an area to monitor over time.

Creating a New Distribution List

The Groups section of the EAC offers the opportunity to create a new Microsoft 365 group, a distribution list, mail-enabled security group, or a dynamic distribution list. The group type tells EAC which UI to display to gather information about the properties of the new group. When you choose a distribution list, the GUI displays some text to convince you to create a new Microsoft 365 group instead, which is fine if you need the extra features like a SharePoint Online site.

To simplify the creation of distribution lists, just a few settings are needed, divided into Basics and Settings. The two basic settings are:

- **Name:** The *Name* property of the distribution list must be unique. If you don't supply a value for the *DisplayName* property, it takes the value assigned to the *Name* property. The *DisplayName* is the one listed in the GA and it's important to give some thought to its composition. Ideally, the name should convey the reason why the group exists, how to use it, and what its membership might be. Groups created by administrators are not subject to the organizational group naming policy as this only applies to user-created groups. We will discuss how to create a group naming policy and how to restrict users from being able to create groups later.
- **Description:** An optional free-text description to explain the purpose of the distribution list. In some cases, administrators note who requested the creation of the list and capture some background for its expected use.

The settings dictating the basic operation of the distribution list are:

- **Owners:** Groups of any type, including a distribution list, should have at least one owner.
- **Members:** Owners can be members, but there are likely a few other people who are members of a new distribution list.
- **Group mail address** (Primary SMTP address): To ensure uniqueness, I typically create the username part of the mail address from the name of the distribution list (separating words with full stops). The domain can be chosen from any of the tenant's registered domains. The list also receives an alias from the tenant's service domain.
- **Communication:** A checkbox to note if people outside the tenant can send emails to the list.
- **Joining the group:** This can be open (anyone can join), closed (members must be added by a list owner), or owner approval (people can apply to join but must be approved or join or leave the group).

Once the EAC creates the distribution list, you can go ahead and amend its membership and other details of the list (Figure 10-12). The person who creates the distribution list is automatically an owner but is not a member. The ideal situation is to have two or more owners. This is more important with a security group

because, apart from administrators, only owners can add or remove members from a security group. You can choose to add owners to the membership so that they receive messages sent to the group, but this is not necessary. The ownership of a group can include other groups as well as individual users.

Tenant Working Group
Distribution list group • 1 owner • 0 members

General Members Settings

General settings
 Hide this group from the global address list

Delivery management
Sender options: Only allow messages from people inside my organization
Specified senders:
[Edit delivery management](#)

Manage delegates
Delegates:
[Edit manage delegates](#)

Message approval
Require moderator approval for messages sent to this group: No
Group moderators:
Add senders who don't require message approval:
Notify a sender if their message is not approved: Any sender
[Edit message approval](#)

Membership approvals
Joining the group: Open
Leaving the group: Open
[Edit membership approvals](#)

Save

Figure 10-12: Amending the settings for a distribution list

Users can browse available groups that they belong to or which they own through the **Distribution groups** section of OWA options. Options are also available to join a group and leave a group. Joining a group involves a user first searching the directory to find the group and then creating a request to join it. Exchange automatically approves requests to join open groups and rejects them for closed groups. Otherwise, Exchange sends requests to join these groups to the group owner(s) for approval.

The *MemberJoinRestriction* and *MemberDepartRestriction* properties control how users can join or leave distribution lists. You can update a distribution list with the *Set-DistributionGroup* cmdlet. This example sets the group properties so that an owner must approve requests to join but a user can leave without approval.

```
Set-DistributionGroup -Identity "All Company" -MemberJoinRestriction ApprovalRequired
-MemberDepartRestriction Open
```

The options to control user-initiated joining and leaving of a group do not exist for either mail-enabled security groups or dynamic distribution lists. Mail-enabled security groups are security principals that can grant access to other resources. It makes sense that only the group owners should be able to control who

enjoys that access. Exchange Online calculates the membership of a dynamic distribution list by running a query against the Exchange directory service. An administrator can decide whether the results of a query will find a specific object by adjusting the object's properties (for instance, they change the value of an attribute used by the query), but unless the owner is also an administrator, they cannot influence the query results.

Other properties of distribution lists often updated with PowerShell include:

- **RequireSenderAuthenticationEnabled**: The default is `$True`, meaning that Exchange Online will deliver messages to the group only when the sender can authenticate (the sender belongs to the tenant). Exchange rejects messages generated by external senders unless this property is `$False`. Normally, you do not want external people sending emails to internal distribution lists, but some good exceptions exist. For example, when a distribution list route messages from external parties (like customers or partners) to a public folder or Teams channel.
- **RejectMessagesFrom**, **RejectMessagesFromDLMembers**, **RejectMessagesFromSendersOrMembers** and **AcceptMessagesOnlyFrom**, **AcceptMessagesOnlyFromDLMembers**, **AcceptMessagesOnlyFromSendersOrMembers**: Exchange Online allows for reasonably granular control over who can send to a distribution list. You can block specific users or members of other distribution lists with the `Reject*` properties or block everyone except those specified in the `Accept*` properties. The EAC populates the `Accept*` properties when you edit a distribution list to update its delivery management parameters. All the objects specified in these lists must be known to Exchange Online and can include mail contacts and mail users. If you try to add a user via their SMTP address, Exchange Online checks the address against the Exchange directory service and rejects it if the address does not match a mail-enabled object.

When updating a reject or accept list for a group, you must update the relevant `*SendersOrMembers` property and Exchange Online will sort out the individual object types and update the properties accordingly. For instance, here is how to update a group so that it will only accept messages from two mailboxes and the members of another group:

```
Set-DistributionGroup -Identity "Executive Committee"
-AcceptMessagesOnlyFromSendersOrMembers "Ben Owens", "CEO Mailbox", "Vice Presidents"
```

- **GrantSendOnBehalfTo**: Controls who has the right to send messages on behalf of the distribution list.
- You can also assign the **SendAs** right to a user for a distribution list. For example, here is how to assign the `SendAs` permission for the Executive Committee distribution list to the CEO Mailbox user.

```
Add-RecipientPermission -Identity ExecCommittee -Trustee "CEO Mailbox" -AccessRights SendAs
```

Note: To protect resources, Exchange Online [enforces limits](#) on the number of recipients that can exist for an individual message (500) and the total number of recipients that a mailbox can send messages to in a single day (10,000). As explained in the Mail Flow chapter, Exchange Online is scheduled to introduce an additional daily limit called the external recipient rate (2,000). These limits exist to prevent tenants using Exchange Online as a bulk email service. When Exchange Online checks messages against these limits, distribution lists, and dynamic distribution lists count as a single recipient, even if the use of these groups means that a message addresses many more recipients than allowed by the limit after the transport service expands groups into individual addressees.

Blocking BCC Delivery to Distribution Lists

Distribution lists can often become very chatty, which leads members to create inbox rules to filter messages sent to the list to stop emails from cluttering up their inbox. People can get around inbox rules by addressing

the distribution list as a BCC recipient. Inbox rules can process TO and CC recipients, but not BCC recipients because these recipients are not present in the message header.

To solve the problem, you can set the *BccBlocked* property of a distribution list to \$True. By default, the value is \$False. When set to \$True, the transport service blocks any message sent to the distribution list as a BCC recipient and the sender receives a non-delivery notification with code 5.7.138. To block BCC deliveries to a distribution list, run the *Set-DistributionGroup* cmdlet:

```
Set-DistributionGroup -Identity "Message Board Posting" -BccBlocked $True
```

Reporting Distribution List Membership

You can use the EAC, the People app, or Outlook to view the membership of a distribution list, but neither interface does a good job with distribution lists of more than 20 or so recipients. The best experience is through the People interface in OWA, which makes it easy to scroll through large memberships. None of the interfaces provided by Microsoft allow you to print off the membership of a distribution list, so unless you invest in a third-party reporting product (see the discussion about standard usage reports in the Auditing and Reporting chapter), it's necessary to create custom reports using PowerShell. For example, this one-liner extracts all the members of the Executive Committee distribution list and outputs some of their details into a CSV file.

```
Get-DistributionGroupMember -Identity "Executive Committee" | Select-Object Name, DisplayName, PrimarySmtpAddress | Export-Csv "c:\temp\ExecutiveCommittee.csv" -NoTypeInformation
```

A script to create a report of distribution list membership [is available on GitHub](#).

Updating Distribution List Membership with PowerShell

The membership of a distribution list is composed of backward links to the EXODS objects for the mail-enabled recipients that make up the membership of groups. EXODS is used instead of Entra ID because some mail-enabled objects which can be members of distribution lists, like mail-enabled public folders, do not exist as Entra ID objects. To view the membership of a distribution list, use the EAC or the Microsoft 365 admin center. If you view it through the Entra admin center, objects that don't exist in Entra ID are missing.

So much for reporting. Updating group membership is more interesting. We can use the *Update-DistributionGroupMember* cmdlet to update the complete group membership at one time, overwriting anything that might already exist. As shown below, the input to the cmdlet is a comma-separated list of identities (aliases, display names, or email addresses) for the group members. Make sure that Exchange can resolve all the identities. If even one is erroneous, the update will fail.

```
Update-DistributionGroupMember -Identity "Blog Writers" -Members @("TRedmond", "Bowens")
```

Alternatively, you can use the *Add-DistributionGroupMember* cmdlet to add a single object to a group or *Remove-DistributionGroupMember* to remove a member. For example:

```
Add-DistributionGroupMember -Identity "Blog Writers" -Member VanHybrid  
Remove-DistributionGroupMember -Identity "Blog Writers" -Member VanHybrid -Confirm:$False
```

Here's another example of a script to add a mailbox to a set of distribution lists. A single-column CSV file holds the aliases of the target distribution lists. After checking that the input mailbox is valid, the *Import-Csv* cmdlet imports the set of distribution lists from the file and stores it in an array. A loop then moves through the array to add the mailbox to each of the target lists.

```
$CheckName = Read-Host "Enter Name of mailbox to add"  
Try {  
    $Mbx = Get-ExoMailbox -Identity $CheckName -ErrorAction Stop | Select -ExpandProperty PrimarySmtpAddress}
```

```
Catch {
    Write-Host "No mailbox can be found called" $CheckName; break }

$DLs = Import-Csv "C:\Temp\InputDLs.csv"

ForEach ($DL in $DLs) {
    Try {
        Add-DistributionGroupMember -Identity $DL."DL Alias" -Member $Mbx -ErrorAction Continue }
    Catch {
        Write-Host "Couldn't add" $Mbx "to DL" (Get-DistributionGroup -Identity $DL."DL Alias").DisplayName }
}
```

Sometimes people change jobs and need to transfer membership of several distribution lists to another person. This is easily scripted with PowerShell, as evident [in this example](#).

User Updates of Distribution Lists

Users with cloud mailboxes can edit the membership of the distribution lists that they own using Outlook or OWA. Distribution list owners should select the object from the online Global Address List rather than the Offline Address Book (OAB) as this will ensure that up-to-date group membership is available and that updates occur quickly. You can still update group membership through the OAB, but everything seems to happen much slower.

Things are much trickier in a hybrid environment where those with Exchange Online mailboxes cannot manage on-premises distribution lists, even if they are a registered owner. The same is true for those who have on-premises mailboxes as they cannot edit distribution lists created in the cloud. Permissions and the ability of Outlook to support cross-platform editing of the membership of distribution lists are the main reasons. In hybrid environments, you are better off using OWA to edit distribution list membership unless you are positively sure that the mailbox and group are on the same platform.

Including a Microsoft 365 Group in a Distribution List

You can include a Microsoft 365 group in the membership of a distribution list, but only through PowerShell. The Microsoft 365 group is treated like a nested distribution list composed of mailboxes and guest accounts (mail contacts). To add a group, run the *Add-DistributionGroupMember* cmdlet. For example:

```
Add-DistributionGroupMember -Identity P365.Authors -Member ExchangeMVPs
```

Including a Teams Channel in a Distribution List

As discussed in the Teams chapter, the email integration for Teams creates email addresses used to send emails to a channel in a team. Messages sent to a channel appear as new conversations in the channel. Teams also captures a copy of messages delivered to the channel in the SharePoint site belonging to the team. To add a team channel email address to a distribution list, create a new mail contact with the address and add the mail contact to the distribution list.

Including a Guest Account in a Distribution List

Groups, Teams, Planner, and SharePoint are among the apps which use Azure B2B Collaboration to share resources with external people using guest accounts. Exchange Online represents guest accounts as mail users, but the mail user objects for guest accounts don't show up in address lists, so you can't add them to a distribution list through EAC or a client UI. Instead, you can add them to a distribution list via PowerShell. This code adds the mail user object for the guest account JohnSmith@outlook.com to a distribution list:

```
Add-DistributionGroupMember -Identity MyDL -Member JohnSmith_outlook.com#EXT#
```

Discovering Distribution Lists and Groups Someone Belongs to

You can discover the distribution lists to which a user belongs by examining their mailbox properties through EAC or the Microsoft 365 admin center. Here's how to do it with PowerShell:

```
$Dn = (Get-ExoMailbox -Identity Kim.Akers).DistinguishedName  
Get-DistributionGroup -Filter "Members -eq '$Dn'"
```

You can replace *Get-DistributionGroup* with the *Get-ExoRecipient* cmdlet to report the different types of groups to which someone belongs. We sort the output to report membership of the different types of groups based on the *RecipientTypeDetails* (group type) information.

```
Get-ExoRecipient -Filter "Members -eq '$Dn'" -Properties RecipientTypeDetails | Sort  
RecipientTypeDetails | Format-Table DisplayName, RecipientTypeDetails
```

You can use a variation of this command to focus on membership of a specific group type. For instance, this command creates a list of Microsoft 365 Groups to which the user belongs because we specify that we only want to see data with *RecipientTypeDetails* set to *GroupMailbox*.

```
Get-Recipient -Filter "Members -eq '$Dn'" -RecipientTypeDetails GroupMailbox | Format-Table  
DisplayName
```

Removing a Distribution List

The *Remove-DistributionGroup* cmdlet removes a distribution list. Once you remove a list, it's irrecoverable and will need to be recreated if removed in error. This command is an example of removing a distribution list without using a confirmation prompt:

```
Remove-DistributionGroup -Identity P365.Authors -Confirm:$False
```

Finding Inactive Distribution Lists

Another common request is to know if any distribution lists are inactive and are therefore candidates for removal. Exchange Online does not include a way to find and report inactive distribution lists, so we must create one with PowerShell. The key points to remember are:

- A distribution list is active when people use it to address messages.
- Evidence of distribution list activity can be found in the message tracking logs by running a message trace to find events noting the expansion of distribution list memberships.
- Exchange Online keeps message tracking logs online for up to 10 days, after which the information is moved into data repositories and kept there for an extra 80 days. Thus, online searches can only look back 10 days to find expansion events. See the Mail Flow chapter for more information about running message traces from the Exchange admin center.

With these points in mind, it's possible to write a PowerShell script to collect expansion events from the message tracking logs for the last 10 days and store the results in a table. We can then check the distribution lists in the tenant against the table to discover if a match exists. If a match is present, we know that the distribution list was used in the last ten days. If not, it was inactive at that time. Apart from reporting each list as it is checked, the script also outputs the results to a CSV file. The method is explored in [this article](#).

Given that message traces give a limited ten-day window to detect inactive distribution lists, this is not a practical technique for a production-quality solution. Nevertheless, it's possible to develop the technique further. For instance, you could run a script every ten days and merge the results over a few months to give a more precise view of inactive and active lists.

Controlling User-Created Distribution Lists

The set of OWA options controllable on a per-mailbox basis includes a “distribution groups” link to allow users to manage distribution lists they belong to and those that they own. To see the set of distribution lists owned by a user, select **OWA Options**, then **General**, and then **Distribution groups**. OWA decides what options are available for a user to work with distribution lists by evaluating if the “*MyDistributionGroups*” and “*MyDistributionGroupMembership*” roles are in the user role assignment policy assigned to their mailbox.

Figure 10-13 shows that both distribution list roles are present in the default role assignment policy used by Exchange Online. Note that users can only create standard distribution lists – they cannot create security groups or dynamic distribution lists. As explained earlier, the Entra ID Groups policy controls if a user can create a new Microsoft 365 Group.

The screenshot shows the 'User roles' section of the 'Default Role Assignment Policy'. On the left, a list of policies is shown, with 'Default Role Assignment Policy' selected. On the right, under 'Contact information', 'MyContactInformation' is checked. Under 'Profile information', 'MyProfileInformation' is checked. Under 'Distribution groups', 'MyDistributionGroups' is checked. Under 'Distribution group memberships', 'MyDistributionGroupMembership' is checked. Under 'Other roles', 'My Custom Apps', 'My Marketplace Apps', 'My ReadWriteMailbox Apps', and 'MyBaseOptions' are all checked. At the bottom is a 'Save changes' button.

Figure 10-13: Distribution list entries in the default user role assignment policy

Even if your tenant has a distribution list naming policy, to prevent “directory anarchy”, many organizations also like to control who can create new distribution lists, and do not want users to create new distribution lists without oversight. You can remove the ability of users to create new distribution lists by unchecking the *MyDistributionGroups* option in the default role assignment policy as OWA will not then display the UI. A subtler approach is also possible that allows users to see the distribution lists to which they belong and to edit the membership of distribution lists that they own. Given that some organizations are migrating distribution lists to Microsoft 365 Groups, it makes sense to leave users with the ability to work with existing distribution lists that they own while blocking their ability to create new distribution lists.

To achieve the goal, you must create a new user role assignment policy and amend it to remove the setting which allows users to create new distribution lists. Here are the steps:

- Open the Roles section of the Exchange admin center and select **User roles**. Select the option to create a new user role assignment policy. Give the policy a suitable name and description and check all the boxes to allow users access to the various items of functionality. In effect, you start by cloning the default user role assignment policy. This example uses a policy called "Restricted Group Management."
- Using PowerShell, define a new management role that is based on the existing *MyDistributionGroups* role. We will call the new management role *MyGroupsNoCreate*.

```
New-ManagementRole -Name "MyGroupsNoCreate" -Parent MyDistributionGroups
```

- The new management role still allows users to create new distribution lists. To remove that ability, we must remove the reference (or role entry) to the *New-DistributionGroup* cmdlet from the *MyGroupsNoCreate* management role. This command breaks the link.

```
Remove-ManagementRoleEntry -Identity MyGroupsNoCreate\New-DistributionGroup -Confirm:$False
```

- A user role assignment policy consists of a set of connections between management roles and the policy. The new user role assignment policy that we created in the first step still contains a reference to the standard *MyDistributionGroups* role. We need to remove it before we can add the altered management role that we have just created.

```
Remove-ManagementRoleAssignment -Identity "MyDistributionGroups-Restricted Group Management" -Confirm:$False
```

- Now add a management role assignment to link the *MyGroupsNoCreate* role to the "Restricted Group Management" policy.

```
New-ManagementRoleAssignment -Name "MyGroupsNoCreate-Restricted Group Management" -Role MyGroupsNoCreate -Policy "Restricted Group Management"
```

- We can then check that the correct roles exist in the "Restricted Group Management" policy. You should find a link to the *MyGroupsNoCreate* in the list and no reference to *MyDistributionGroups*. Remember that *MyGroupsNoCreate* has all the functionality of *MyDistributionGroups* except the link to the *New-DistributionGroup* cmdlet. Because they cannot run the cmdlet, a user to whom we assign this policy can do everything except create a new distribution list.

```
Get-ManagementRoleAssignment -RoleAssignee "Restricted Group Management" | Format-Table Name, Role -AutoSize
```

To prove that everything works, apply the Restricted Group Management policy to a mailbox:

```
Set-Mailbox -Identity Lotte.Vetler -RoleAssignmentPolicy "Restricted Group Management"
```

After waiting ten minutes or so to ensure that any cached permissions are clear, sign into the mailbox and follow the same path through settings to expose the set of distribution lists available to the user. The option uses a special page under <admin.exchange.microsoft.com> with tabs for groups the user belongs to and those they own. On the tab for owned groups (Figure 10-14), the policy works if the option to create a new group is missing.

Groups

Instead of a distribution group, consider using a new Microsoft 365 Group to collaborate by sharing conversations, documents, and a calendar. [Learn more](#)

Name	Email address	Members
All Company Employees	All.Company@Of...	123 members
Engineering Department	HABEngineering@...	123 members
Executive Committee	ExecutiveCommit...	123 members
VIP Users	VIPUsers@Office...	123 members
Yammer Development	HABYammer@off...	123 members

Figure 10-14: The effect of the restricted user role assignment policy is that users can't create new groups

Distribution List Naming Policy

If you allow users to create new distribution lists, you can expect that some interesting names will turn up for distribution lists. No one likes to see entries such as "Billy-Bob's Fishing Aficionados" in the GAL. The name does not convey a sense of the true business purpose. To guide users, organizations can create a distribution list naming policy. The policy can include:

- A prefix to apply to the user-supplied name for a new distribution list. The prefix can be multi-part and consist of text strings and the values of user account attributes. The policy forces the insertion of a blank character if the user account does not store a value for the chosen attribute.
- A suffix to add to the user-supplied name for a new distribution list. Again, you can use both text and attribute values.
- Barred or forbidden words that users cannot include in the name for a new distribution list. For instance, you can prohibit potentially offensive terms by including them in the policy.

To configure the distribution list naming policy, go to the Groups section of the EAC, select the distribution list tab and then Add naming policy. You can then add the various elements of the policy.

One reason why organizations use a naming policy is to ensure that distribution lists appear in a single section within the GAL. Adding the department name ensures that the distribution lists belonging to a department are found together. Behind the scenes, Exchange Online stores details of the distribution list naming policy as settings in the tenant organization configuration. You can view the settings with the *Get-OrganizationConfig* cmdlet:

```
Get-OrganizationConfig | Format-Table Distr* -AutoSize
DistributionGroupDefaultOU DistributionGroupNameBlockedWordsList DistributionGroupNamingPolicy
-----
```

{XXX, Cheese}	DL-<Department> <GroupName>
---------------	-----------------------------

These properties have the following meanings:

- The *DistributionGroupBlockedWordsList* property holds words that cannot be used in a group name.
- The *DistributionGroupNamingPolicy* property defines the pattern for names. In the example shown below, the policy consists of four elements:
 - A text string "DL-."
 - <Department> means that the Department value stored in the user account is inserted.
 - Another space is then inserted.
 - <GroupName> means the name of the distribution list as supplied by the user.
- The *DistributionGroupDefaultOU* property is only used in on-premises deployments but still features in the Exchange Online organization configuration.

It is possible to create or amend the naming policy through PowerShell. For instance:

```
Set-OrganizationConfig -DistributionGroupNamingPolicy "DL-<Department> <GroupName>"
```

To remove the distribution list naming policy, set the value of *DistributionGroupNamingPolicy* to *\$Null*:

```
Set-OrganizationConfig -DistributionGroupNamingPolicy $Null
```

The distribution list naming policy applies to user-created distribution lists and has no retrospective effect. You must update the names of existing distribution lists if you want them to follow a new policy. To do this, use PowerShell to find distribution lists with non-compliant names and then update their names according to the naming policy. The EAC does not allow administrators to create distribution lists without applying the policy.

If an administrator creates a distribution list with PowerShell, they can pass the *IgnoreNamingPolicy* parameter to instruct Exchange Online to not apply the policy. For example:

```
New-DistributionGroup -Name "Tiger Team" -Members Jill.Smith@Office365itpros.com, Ben.Owens@Office365itpros.com, Kim.Akers@Office365itpros.com -IgnoreNamingPolicy
```

The distribution list naming policy does not apply to dynamic distribution lists or mail-enabled security groups because users cannot create these types of groups. The policy does not apply to Microsoft 365 Groups, which use a separate naming policy.

Defining a distribution list naming policy for Exchange Online can also affect the way that on-premises distribution lists synchronize in hybrid deployments. To make everything consistent, Exchange applies the naming policy to distribution lists belonging to the on-premises organization when they synchronize with Entra ID objects with AAD Connect. Thus, an on-premises distribution list might have a different name in the on-premises directory than that shown in Entra ID unless you make sure to apply the same naming policy in both environments.

Migrating On-Premises Distribution Lists to Exchange Online

Exchange Online doesn't include any out-of-the-box method to migrate a distribution list from an on-premises Exchange organization to Exchange Online. When an on-premises organization is synchronized with Exchange Online in a hybrid deployment, the suggested method is to remove the distribution list from on-premises and recreate it as a brand-new object in the cloud. For anything but simple lists with just a few members, this is a tiresome process, but it reflects the fact that transferring a distribution list to the cloud can be quite complex because:

- The owner(s) of the distribution list might not have their account(s) in the cloud. An on-premises user cannot manage a cloud-based distribution list.
- Objects for mail-enabled members of the distribution list might not exist in the cloud. For example, a mail contact in the on-premises environment might not be synchronized to the cloud.
- The distribution list might hold other distribution lists.

- The proxy addresses for the on-premises distribution list must be transferred to the new list.
- Some properties of distribution lists refer to other directory objects that must exist in the target environment before they can be used. For example, the property that controls the ability of users to send emails on behalf of the list.

It is possible to write a PowerShell script to concurrently connect to Exchange on-premises and Exchange Online and perform the processing to transfer a distribution list. The script must:

- Check that all the prerequisites are satisfied for the transfer to go ahead. For example, are all the members of the list known in the cloud.
- Create the target distribution list in Exchange Online.
- Read information about the source distribution list from Exchange on-premises and update the properties of the target distribution list.
- Assign a new proxy address to the source distribution list and transfer it to the target distribution list.
- Update the membership of the target distribution list with the membership of the source list.
- Hide the source distribution list from address lists so that the only list that is visible to users is the target. Eventually, if the transfer worked and no problems are found, the old list is removed.

An example of a migration script for distribution lists is [available on GitHub](#) (the documentation [is here](#)). As with any script, you should test it carefully and adapt the code where necessary to meet the needs of your deployment.

Dynamic Distribution Lists

Traditional email distribution lists work well to deliver email to large sets of recipients. Maintenance of group membership to ensure accurate delivery of messages can be an issue, especially for groups with frequent membership changes. Dynamic distribution lists do not have fixed membership. Instead, the Exchange transport service calculates the membership by resolving a query (recipient filter) against the EXODS directory to return the current set of members. The recipients can be any type of mail-enabled object supported by Exchange, including user and shared mailboxes, public folders, mail contacts, and other distribution lists.

Dynamic distribution lists are EXODS objects and do not exist in Entra ID. If you use dynamic distribution lists with Exchange Server, you should remember that synchronization utilities do not process dynamic distribution lists. If you want to use the same dynamic distribution lists on both sides of a hybrid organization, you must:

- Create the dynamic distribution list objects in Exchange Server and Exchange Online.
- Update the queries for the dynamic distribution lists so that they find the right recipients. If a recipient does not exist in a directory, it cannot be found. For instance, the query for an Exchange Online dynamic distribution list cannot find on-premises recipients if they don't exist (as a mail user object or mail contact) in Exchange Online.
- As users migrate between the two environments, adjust the queries to ensure that the dynamic distribution lists find the correct set of recipients.

In addition, because dynamic distribution lists don't exist in Entra ID, they cannot be used to specify sets of users for processing by Microsoft 365 solutions such as information protection (sensitivity labels) or data lifecycle management (retention).

Dynamic Distribution Lists are simple, robust, and work well when you need to communicate with a changeable set of mail-enabled recipients. The key to success is to make sure that EXODS contains accurate data to allow recipient filters to find the correct recipients. With that thought in mind, let's discuss how recipient filters work.

Recipient Filters

Recipient filters are OPATH queries executed against the directory to return a set of objects. A query can vary from very simple lookups such as “all the users in the London office” or “everyone who works for the Accounting department” or “all full-time employees” to more complex queries involving lookups against multiple recipient attributes stored in EXODS. The weak point for a recipient filter is the accuracy of the data in the queried repository. If recipient properties do not store accurate data, then incomplete or erroneous sets of recipients will be found when the transport service uses the queries to find the set of recipients to route messages. On the other hand, if EXODS is well maintained (or Entra ID, as many attributes synchronize from Entra ID to EXODS) with the information required to support effective queries, dynamic distribution lists work very well.

Once you know the query to find the desired recipient set, creating a new dynamic distribution list is not difficult. The EAC interface helps administrators to compose the query used to determine distribution list membership. Each condition that you add to the query is a rule that checks an attribute of the objects that fall under the scope of the query (all recipient types, user mailboxes, and so on) against one or more text values. In Figure 10-15, we check the Company attribute for user mailboxes to look for a specific value. If multiple acceptable values exist for an attribute, input each value separated by a comma.

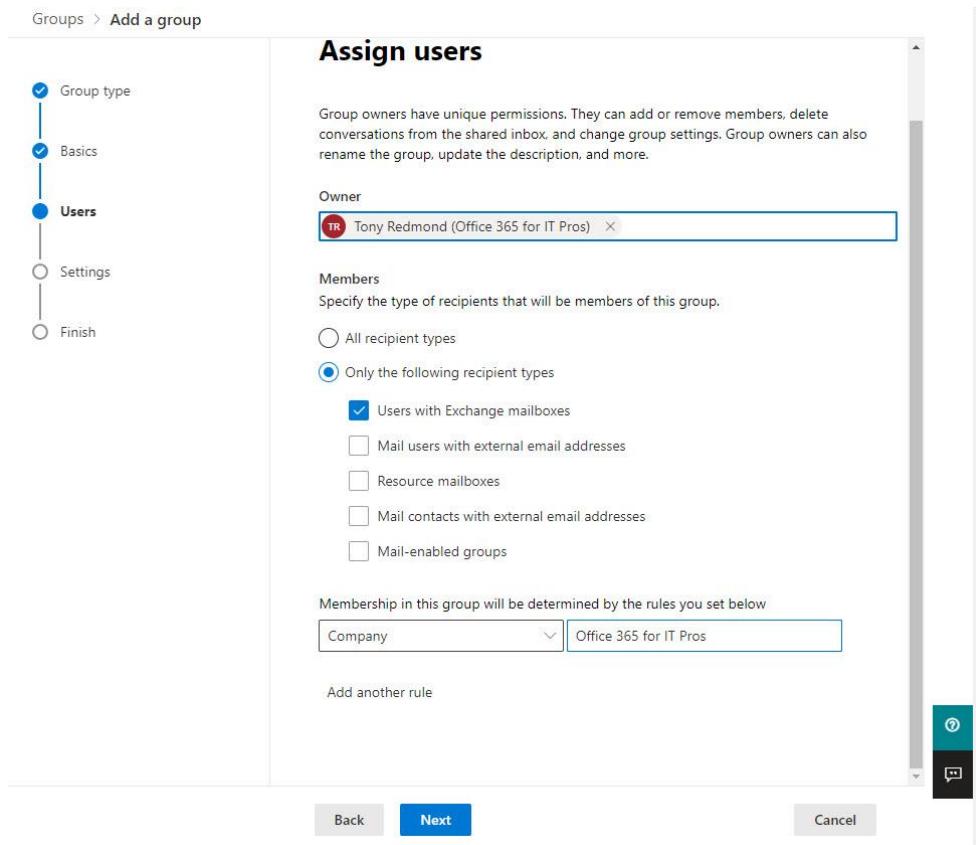


Figure 10-15: Defining settings for a dynamic distribution list

Dynamic distribution lists use one of two types of recipient filters:

- **Precanned filters** are used when a DDL is created through the EAC. Precanned filters are restricted to queries against a small number of object properties such as the department, city, and 15 customizable attributes.
- **Custom filters** are created when you use PowerShell to define a recipient filter. Custom filters are more powerful and flexible than precanned filters because a wider set of properties can be included in a query. Once you apply a custom filter to a DDL, you won’t be able to edit the filter through the EAC.

The EAC UI restricts queries to a limited set of mailbox properties selected because they are the most popular:

- StateOrProvince.
- Company.
- Department.
- Any of the 15 single-value custom attributes (CustomAttribute1 through CustomAttribute15).

When you save a dynamic distribution list with either EAC or PowerShell, Exchange writes its recipient filter into the list properties after applying some extra processing to the filter to ensure that it finds the right objects. This means that a relatively simple recipient filter as viewed in the EAC GUI looks very different when viewed through PowerShell using the Get-DynamicDistributionGroup cmdlet. For example:

```
Get-DynamicDistributionGroup -Identity "Microsoft 365 Gurus" | Select-Object RecipientFilter, RecipientFilterType

RecipientFilter      : (((RecipientType -eq 'UserMailbox') -and (CustomAttribute1 -like 'Exchange'))) --and (Alias -ne $null)) -and (-not(Name -like 'SystemMailbox{*'})) -and (-not(Name -like 'CAS_{*'})) -and (-not(RecipientTypeDetailsValue -eq 'MailboxPlan'))) -and (-not(RecipientTypeDetailsValue -eq 'DiscoveryMailbox'))) -and (-not(RecipientTypeDetailsValue -eq 'PublicFolderMailbox'))) -and (-not(RecipientTypeDetailsValue -eq 'ArbitrationMailbox'))) -and (-not(RecipientTypeDetailsValue -eq 'AuditLogMailbox'))) -and (-not(RecipientTypeDetailsValue -eq 'AuxAuditLogMailbox'))) -and (-not(RecipientTypeDetailsValue -eq 'SupervisoryReviewPolicyMailbox'))) -and (-not(RecipientTypeDetailsValue -eq 'GuestMailUser'))) -and (-not(Name -like 'SystemMailbox{*'})) -and (-not(Name -like 'CAS_{*'})) -and (-not(RecipientTypeDetailsValue -eq 'MailboxPlan')) -and (-not(RecipientTypeDetailsValue -eq 'DiscoveryMailbox')) -and (-not(RecipientTypeDetailsValue -eq 'PublicFolderMailbox')) -and (-not(RecipientTypeDetailsValue -eq 'ArbitrationMailbox')) -and (-not(RecipientTypeDetailsValue -eq 'AuditLogMailbox')) -and (-not(RecipientTypeDetailsValue -eq 'AuxAuditLogMailbox')) -and (-not(RecipientTypeDetailsValue -eq 'SupervisoryReviewPolicyMailbox')))

RecipientFilterType: Custom
```

The recipient filter shown above looks for user mailboxes that have “Exchange” in *CustomAttribute1* and excludes all the various types of system mailboxes. The filter seems very complex and difficult to construct, but you don’t have to insert these exclusions as Exchange creates them automatically.

When you see *Custom* as the *RecipientFilterType*, you know that PowerShell was used to create a custom recipient filter (see example below). If you see *Precanned*, you know that the recipient filter is based on the pre-prepared queries (like “all mail-enabled recipients”) available through EAC. Only dynamic distribution lists with precanned filters can have their recipient filters updated through the EAC. Although the other properties of dynamic distribution lists which have custom filters can be maintained through EAC, PowerShell must be used to edit their custom recipient filters.

Complex Recipient Filters

Recipient filters support [a much wider set of filterable properties](#) than the set exposed by the EAC when composing query rules, but you can only use these properties by creating a custom recipient filter and writing the filter into the dynamic distribution list using PowerShell. The custom recipient filter for a dynamic distribution group cannot be edited through EAC.

For instance, let’s assume that we want to create a dynamic distribution list to communicate with users whose mailboxes have been placed on litigation hold. To accomplish the goal, we follow these steps:

- Build the filter and test its effectiveness by using it with the *Get-Recipient* cmdlet.
- Update an existing dynamic distribution list or create a new dynamic distribution list with the tested filter.

For example, here’s how to define and test a filter to find mailboxes on litigation hold based in Dublin:

```
$Filter = "((LitigationHoldEnabled -eq '$True') -and (StateOrProvince -eq 'Dublin') -and (RecipientType -eq 'UserMailbox'))"
```

```
Get-Recipient -RecipientPreviewFilter $Filter

Name      RecipientType
-----
TRedmond   UserMailbox
James.Ryan  UserMailbox
```

Another example is a filter that looks for accounts with a certain job title that the organization has not disabled (the *ExchangeUserAccountControl* setting for a mailbox is set to *AccountDisabled* when the owning user account is blocked). This requires a filter that's slightly more complex to cover the range of job titles that might be in use. The need to specify multiple variants of the property is explained by the lack of wildcard support preceding a value in recipient filters (like “*architect”). You can use wildcards after the value (like “architect*”). The net result is that a filter for multiple variants of a value can end up with many *-or* clauses:

```
$Filter = "((Title -eq 'Architect') -or (Title -eq 'Senior Architect') -or (Title -eq 'Principal Architect') -and (ExchangeUserAccountControl -ne 'AccountDisabled'))"
```

System values like *\$True* and *\$null* must be enclosed in single quotes. If you don't do this, OPATH will signal an error. Here's an example of using *\$null* in a filter:

```
$Filter = 'department -eq $null -and Company -eq "Contoso'"
```

The [Microsoft documentation](#) includes additional information about how to form OPATH queries in different situations.

After testing the filter and verifying its accuracy, we can use it when creating a dynamic distribution list. In this case, the filter finds mailboxes on litigation hold in Dublin. Enclosing the filter in curly braces is the equivalent of enclosing it in single quotation marks:

```
$Filter = {city -eq "Dublin" -and LitigationHoldEnabled -eq $true}
New-DynamicDistributionGroup -Name "Dublin Mailboxes on Litigation Hold" -DisplayName "Dublin User Mailboxes on Litigation Hold" -Alias Dublin.Litigation -PrimarySmtpAddress
Dublin.Litigation@Office365itpros.com -RecipientFilter $Filter

Set-DynamicDistributionGroup -Identity Dublin.Litigation -ManagedBy
Legal.Assistant@Office365itpros.com -MailTip "People under litigation hold in Dublin"
```

Dynamic distribution lists to address sets of people like those under litigation hold might be deemed confidential. In this situation, you can hide them from address lists by setting their *HiddenFromAddressLists* property to *\$True*:

```
Set-DynamicDistributionGroup-Identity Dublin.Litigation -HiddenFromAddressListsEnabled $True
```

Anyone who needs to send messages to a hidden dynamic distribution list can do so by using its SMTP address. Messages sent to dynamic distribution lists with queries that don't find any recipients go into a void. Exchange doesn't generate a non-delivery notification for the sender because the address for the dynamic distribution list is valid: the problem is that the list query doesn't return any recipients, which is a valid condition. This is a good reason for testing the recipient filter for a dynamic distribution list to make sure that it finds the correct set of recipients.

As mentioned above, if you create a custom recipient filter for a dynamic distribution group, the filter for the group can no longer be edited through EAC. If you want to remove the custom recipient filter and put the group into a state where its filter can be edited through EAC, use *Set-DynamicDistributionGroup* to add a precanned filter. This action overwrites the custom recipient filter and makes the group editable through EAC. For instance, this command updates a dynamic distribution group with the precanned “all Exchange Online mailboxes” filter:

Set-DynamicDistributionGroup -Identity Dublin.Litigation -IncludedRecipients MailboxUsers

Custom recipient filters based on email addresses: A common requirement is to create a dynamic distribution list based on the primary SMTP address assigned to mailboxes and other mail-enabled objects. Although the [list of filterable properties](#) includes the primary SMTP address and says that wildcards are supported, you can't build a recipient filter like "`*office365itpros.com`" to find mail-enabled objects with primary SMTP addresses ending in a certain domain. As [explained in this article](#), it's possible to create a workaround. It's not difficult, but it is a pain that the workaround is required.

Membership Calculation

In Exchange Server and earlier implementations of Exchange Online, the transport service resolves the directory queries for dynamic distribution lists on an on-demand basis. Because a query fetches the latest recipient information from the directory, this approach guarantees that the recipient set used to address messages is always up to date. Resolving on-demand queries can create a heavy demand on system resources, especially when the recipient filter is complex.

Taken together with the fact that most list memberships do not change very often, in late 2021, Microsoft moved Exchange Online to a timed calculation model like that used for dynamic groups. This means that the transport service calculates the memberships of dynamic distribution lists:

- At least once daily.
- After the recipient filter changes.
- Following the creation of a new dynamic distribution group.

In the case of the last two scenarios, it can take up to two hours before group membership is available for use. You can see when the transport service last updated the membership for dynamic distribution lists by running the `Get-DynamicDistributionGroup` cmdlet and examining the `CalculatedMembershipUpdateTime` property. For example:

```
Get-DynamicDistributionGroup | Format-Table DisplayName, CalculatedMembershipUpdateTime
```

DisplayName	CalculatedMembershipUpdateTime
-----	-----
Company-DDG	22/11/2023 20:00:36
Dublin users	22/11/2023 20:00:36
Office 365 Gurus	22/11/2023 20:00:36
AuthorizedGroupCreators	22/11/2023 20:00:36

Checking the Effectiveness of a Recipient Filter

The EAC doesn't include a way to check the effectiveness of a recipient filter. In other words, how to be sure that the filter will find the right set of recipients when the Exchange transport service resolves it against the directory to compute the list membership. You can check with PowerShell by inputting the filter to the `Get-Recipient` cmdlet. For example, here's how to check the recipient filter for the Microsoft 365 Gurus dynamic distribution list:

```
Get-Recipient -RecipientPreviewFilter (Get-DynamicDistributionGroup -Identity "Microsoft 365 Gurus").RecipientFilter
```

Name	RecipientType
-----	-----
Jeff.GUILLET	UserMailbox
Tony.REDMOND	UserMailbox
Paul.ROBICHAUX	UserMailbox

In this instance, if you expect the query to return three mailboxes, it works. If not, the fault is either in the query (it searches for the wrong data) or the underlying data (does not contain the right values). Testing the

results of a query is important not only because the results will reveal any flaw in your logic and identify whether the filter returns the correct recipient set when the query executes against the directory. It will also tell you how many recipients are in the selected set. Equipped with that knowledge, we can construct some guidelines to help administrators maintain dynamic distribution lists. For example, your organization might use the following guidelines for both standard and dynamic distribution lists:

- Any distribution list with more than 200 recipients should have a MailTip to highlight the fact to users. Exchange Online automatically displays a MailTip to tell the sender how many people will receive their email, but you can add another MailTip to urge additional caution when sending to very large distribution lists.
- Any distribution list with more than 500 recipients should be moderated to ensure that people do not inadvertently broadcast to distribution lists such as "The Entire Company". Moderated distribution lists are also a good way to stop email storms that result when users reply-all to very large distributions.

After you create a new dynamic distribution list or update the recipient filter for an existing list, the Exchange transport service resolves the recipient filter against the directory to compute the set of members. This process can take up to two hours. When it is complete, you can run the *Get-DynamicDistributionGroupMember* cmdlet to check the set of recipients Exchange will use when someone addresses a message to the list.

```
Get-DynamicDistributionGroupMember -Identity "Microsoft 365 Gurus"
```

Name	RecipientType
-----	-----
Tony.Redmond	UserMailbox
Jeff.GUILLET	UserMailbox
Paul.Robichaux	UserMailbox

Even if the members do not appear in the same order, the memberships reported by *Get-Recipient* and *Get-DynamicDistributionGroupMember* for the same list should be the same.

Finding the set of dynamic distribution lists a user belongs to is a two-step process. After fetching the distinguished name of their mailbox, we use the distinguished name to check the membership of each dynamic distribution list as it passes through the pipeline:

```
$Dn = (Get-ExoMailbox -Identity Chris.Bishop).DistinguishedName
Get-DynamicDistributionGroup | Where-Object { (Get-DynamicDistributionGroupMember -Identity
$_._PrimarySMTPAddress | Where-Object {$_._DistinguishedName -eq $Dn}) }
```

Migration from Email Distribution Lists

Microsoft is keen that tenants should replace distribution lists with Groups. To make the move easy for tenants, five methods are available:

- Administrators can migrate individual distribution lists using the function available in the EAC.
- Group owners can migrate individual distribution lists using the function available in OWA.
- Administrators can run the PowerShell scripts created by Microsoft to migrate batches of distribution lists at one time.
- Administrators can run the *New-UnifiedGroup* cmdlet to convert an individual distribution list to a group.
- Tenants can create their versions of PowerShell scripts to perform custom migrations.

None of these methods work with distribution lists belonging to on-premises organizations. To convert these groups, you must first move them to Exchange Online, and then, when the groups are "cloud-owned", you can

go ahead and convert them. Of course, it might be simpler to recreate the on-premises distribution lists as Groups and then remove them from the on-premises organization.

Email distribution lists have been around for a long time. Different forms of distribution lists exist, some of which are easy to convert while others are very difficult to move to Groups today. It is safe to say that it is relatively easy to code the steps to migrate a simple distribution list managed by Exchange Online that only has cloud mailboxes in its membership. Things become more challenging when the need arises to process distribution lists with the following characteristics:

- **Dynamic distribution lists:** Groups supports dynamic membership, but no conversion facilities are available to migrate dynamic email distribution lists to become dynamic Groups. This could be due to some of the difficulties created by the fact that the two types of groups support different sets of member objects. For example, you can create a dynamic distribution list that includes several types of mail-enabled objects that are not all supported by Groups.
- **Nested distribution list:** It is common to meet distribution lists where the membership contains other (nested) distribution lists. For example, an "All Company" list might include several other groups, each of which might include people who work in a business unit or other division of the company. In turn, each divisional list might include other distribution lists for its operating units that hold the actual mail-enabled recipients. Nested distribution lists are not supported by Microsoft's migration toolset.
- **Distribution lists that include more than mailboxes:** Groups only support user and guest accounts as members. They do not support some of the other kinds of mail-enabled recipients often found in email distribution lists, such as public folders.
- **Distribution lists with advanced settings:** Lists with send on behalf of settings or are hidden from address lists, or that have restrictions on who can join a group.

Email distribution lists with the characteristics listed above must stay in place until they are either not needed and you can remove them safely or Groups evolve to a point where they can serve as a replacement. In some cases, as in the example of nested or dynamic distribution lists used by organizations to send messages to a very large number of users, that point might never come. Remember too that some clients still in use do not support Groups, so do not plan to move away from distribution lists until all clients are prepared.

In this context, migrating an email distribution list to a group is only a question of moving members from one group to another. Any other assets used with an email distribution list, such as an associated public folder, are unaffected by the migration.

Microsoft's PowerShell Scripts

PowerShell is a terrific way to automate the process of converting distribution lists. Microsoft has [scripts available in the download center](#) to migrate all eligible distribution lists found in a tenant:

- **Get-DIEligibilityList.ps1:** Scans the tenant to find distribution lists to create a report detailing the distribution lists that can be migrated to Groups along with those that cannot (for one of the reasons given above). The output of the script is a text file (DIEligibility.txt) that you can review.
- **Convert-DistributionGroupToUnifiedGroup.ps1:** Converts all eligible distribution lists in a tenant to Groups.

The scripts are effective but can only deal with distribution lists that have the same characteristics discussed above.

The DIY Approach to Converting Distribution Lists

Another example of how to approach the task of converting an email distribution list to a Microsoft 365 group is posted on [GitHub](#). Like all PowerShell scripts, the code is easily altered to meet the needs of a certain scenario. The basic set of tasks that a conversion script needs to perform include:

- Check whether a group with the same alias exists. The script could exit if this is the case or continue by migrating the distribution list to a new group with a different alias.
- Check whether the distribution list being migrated is a simple distribution list (type equals *MailUniversalDistributionGroup*). You could migrate the membership of a universal mail-enabled security group to a group but not the security principal. There is probably some good reason why the security principal exists, so it is probably best not to migrate these groups unless you are sure that the security element is resolved.
- Gather information about the owners (managers) and members of the input distribution list.
- Update the alias of the input distribution list with a new value to allow the reuse of the existing alias for the new group.
- Check whether the new group should be public or private. One way to do this is to look at the *MemberJoinRestriction* property of the input list. If this is "Closed" or "ApprovalRequired", then it is reasonable to assume that a private group should be the result.
- Create the new group by running the *New-UnifiedGroup* cmdlet.
- Migrate the properties of the input distribution list to the new group. A direct match of all properties does not exist, but a reasonable number of properties are common to both distribution lists and Microsoft 365 groups.
- Add the members of the new group by reading the membership information from the input distribution list and using the *Add-UnifiedGroupLinks* cmdlet to update the membership of the group. Some checking is necessary to ensure that only mailboxes are added to the group. Mail-enabled public folders and shared mailboxes are supported for distribution lists but not for Groups. In addition, you must expand the membership of nested distribution lists to figure out the set of valid members and then add them to the group.
- Because distribution lists act as a single address to distribute emails to members, it is reasonable to expect that the substitute group would behave comparably. Accordingly, you can also add the members of the group as subscribers so that they receive new copies of conversations via email.
- Add the owners of the new group by running the *Add-UnifiedGroupLinks* cmdlet. Users must be members of the group before they can be added as owners.
- Hide the old distribution list from the GAL so that users pick up and start using the replacement group.

Simple scripts with the PowerShell commands to migrate a distribution list (like this example [available on GitHub](#)) are readily available. A more comprehensive solution is available in Tim McMichael's DLConversionV2 module ([available from GitHub](#)) and the [PowerShell gallery](#). If you have a question about using DLConversionV2, you'll probably find an answer on [Tim's blog](#).

It's important not to migrate distribution lists without putting some thought into the matter. In some cases, migrating a distribution list is absolutely the right thing to do. In others, creating a Microsoft 365 group might be a better option. Don't rush to migrate until you're prepared and ready to do the job.

Comparing Groups, Distribution Lists, and Shared Mailboxes

Although Microsoft dedicates an impressive amount of development effort to support and enhance the capabilities of Groups, situations do exist when you should use a distribution list, a dynamic distribution list, or a shared mailbox rather than a Microsoft 365 group. You can use the following questions to help guide your choice:

- Is the intended use of the group to distribute email to a set of people? If so, then a standard distribution list is probably the best choice. Remember, if you need to, you can convert a standard distribution list to a group.
- Does the group span more than Exchange Online mailboxes? Groups support a limited set of recipient types (Exchange Online user mailboxes and guest users) while standard distribution lists support all mail-enabled recipient types – mailboxes, mail users, mail contacts, public folders, resource mailboxes, and other groups.
- Do you want to have access to more than the Inbox and Calendar folders and allow group members to move items between mailbox folders? If so, a shared mailbox might be a better solution. The same is true if you want to use other mailbox features, such as assigning categories to messages. Although OWA can expose some of the folders in group mailboxes and allow users to move, copy, and delete items in those folders, its support for folder access does not include some of the default folders such as Sent Items.
- Do you want to preserve earlier contributions and conversations shared between members of the group? You can do this with the old-fashioned combination of a public folder (to hold the content) and distribution list or with a shared mailbox, but the added functionality available to a group means that it is a better long-term solution.
- Do you want dynamic membership of groups based on Entra ID attributes? Microsoft 365 groups support dynamic membership, but only if you have Entra ID P1 licenses. In addition, if you want to have groups whose membership has more than Microsoft 365 user and guest accounts, then dynamic distribution lists are the right choice.
- Is the communication flow within the workgroup purely internal and the ability to send outbound emails is unnecessary? If so, Teams might be a better choice.

The arguments for Groups are often based on the use of a common identity to access resources drawn across from the service. They are much less email-centric than standard distribution lists are, so the question often comes down to the fundamental choice of whether you just need email or to exploit that common identity across Exchange Online, SharePoint Online, Teams, Planner, Power BI, and so on.

Chapter 11: Teams Basics

Tony Redmond

Workgroup Collaboration

Teams is Microsoft 365's workgroup application for consumer, enterprise, government, and education customers. The central concept behind Teams is that it delivers workspaces that bring people together to collaborate through chats, files, meetings, and associated applications. The original implementation of Teams focused on chat, or "high velocity" communication, to allow Microsoft to compete with Slack and other messaging products, including Facebook. Today, Teams is both a platform for delivery apps and an ecosystem to serve many different client bases including commercial, education, and government customers.

Calling and meeting capabilities are a particular strength of the platform. People connect with audio or video streams to share information in a very natural fashion. The Covid-19 pandemic accelerated the movement from in-person to virtual meetings, as evident in the billions of "collaboration minutes" created monthly along with associated recordings, transcripts, captions, and files. Teams meetings include screen and application sharing, chat, transcription, caption translation, and recordings. More on this topic in the chapter about Teams Devices and Calling.

Microsoft's [Teams Adoption Guide](#) sets out their vision and intent for Teams. We'll explore the concepts and ideas described in the guide throughout this chapter. We also describe the Teams architecture and how Teams integrates different Microsoft 365 components to deliver its functionality along with lots of practical information about how to use Teams. We develop the information presented here to explore how to manage Teams in a Microsoft 365 tenant in the next chapter.

Teams User Base

At the Ignite 2018 conference, Microsoft announced that Teams was the fastest-growing business application in the company's history. Teams achieved that status just two years after its launch. Today, [Accenture is the largest Teams deployment](#) and has a user community of more than 569,000. In December 2020, Accenture said that their use of Teams included [900 million minutes of audio conferencing and 90 million minutes of video conferencing](#) monthly. Microsoft put the number of audio minutes consumed by Accenture monthly at over one billion just a month later when reporting their [FY21 Q2 results](#). Microsoft said that the U.S. Department of Veterans Affairs also had more than 500,000 users.

In October 2021, Microsoft said that 138 organizations have more than 100,000 Teams users and more than 3,000 organizations have more than 10,000 Teams users (in January 2021, the numbers were 117 and 2,700 organizations respectively). 93 of the Fortune 100 use Teams. In terms of the overall user base, Microsoft changed their method of reporting [Teams usage in July 2021](#) from daily active users to monthly active users. At the time, Microsoft claimed that Teams has "nearly 250 million" monthly active users, but did not specify the breakdown across commercial users, education users, and personal users. The latest figure is 320 million monthly active users.

An active user is someone who does something with an application. For Teams, it means that they send a message, participate in a meeting, and so on. A big difference exists between active users and licensed users. Organizations often acquire licenses well before they deploy a product, and because Teams is bundled into many Microsoft 365 SKUs, the number of people who can use Teams is potentially much higher.

Teams and U.S. Government Cloud: Due to the need to achieve compliance with several government security standards, the introduction of Teams features in the GCC, GCC High, and DoD clouds often lags several months after commercial availability. It's not clear if the numbers for Teams users cited by Microsoft include the massive [U.S. Department of Defense contracts](#).

Teams Versions

Teams is available in paid-for and free versions:

- **Teams Enterprise (aka for Work or School):** This is the version bundled in (and equivalent academic and government) Office 365 and Microsoft 365 enterprise plans and is the focus of the discussion here. The Microsoft 365 Business plans also include Teams. The enterprise version of Teams is the only one that supports the Microsoft Phone system. From October 1, 2023, [new users in the European Economic Area \(EEA\)](#) must purchase separate Teams EEA licenses to use with Office 365 or Microsoft 365. Existing licenses are unaffected.
- **Teams Exploratory/Trial:** If you have a Microsoft 365 plan that doesn't include Teams, Microsoft offers the [Teams Exploratory license](#). Users with a valid tenant account can sign up for the exploratory experience and receive a license for the software components needed for Teams, some of which, like Exchange Online, Forms, Planner, and Stream, their account might already hold. Tenant administrators can stop users from signing up for the Teams Exploratory license by disabling the option to let users install trial apps and services in the **User owned Apps and Services** section under Settings in the Microsoft 365 admin center.
- **Teams Essentials:** Introduced in December 2021 for \$48/user per year to replace Teams Free (Classic) (now retired), Teams Essentials is based on the original implementation of Teams Free (Classic) re-engineered for SMBs and other small organizations. The major differences between the Essentials and Free versions are higher participant numbers for meetings and group chats (300 versus 100), longer meetings, more storage, and Microsoft support. For an extra \$12/user per year, the Microsoft 365 Business Basics product includes Teams along with Microsoft 365 functionality (Exchange Online, SharePoint Online, Stream, Planner, etc.).
- **Teams Free (Teams for Home):** Originally [launched in preview in June 2020](#), the version of Teams aimed at helping people to organize aspects of their personal lives is available for the Teams mobile clients and Windows desktop and browser clients. The clients support different features tailored to the operating system, but all clients support personal chat (up to 250 participants), video and audio calls, and calendar scheduling of meetings. The application uses a Microsoft personal account for access to the calendar and OneDrive shared file storage. Users can switch between work and personal accounts like switching between different tenants. Teams for Home uses Microsoft Service accounts (MSAs) for authentication. Windows 11 includes a version of Teams Free with chat and calling capabilities.

Organizations typically choose the Enterprise version of Teams when they want:

- *Scalability:* The membership limit for teams in the enterprise version is 25,000 (tenant and guest accounts).
- *Storage:* Enterprise users receive large quotas in OneDrive for Business to store documents and other files like Loop components, whiteboards, and Stream videos.
- *Access to Phone System features* such as PSTN calling.
- *Compliance:* Support for the capture of compliance records for audit purposes. Support for retention and data loss prevention policies.
- *Office Collaboration:* The desktop versions of the Office applications include added collaboration and security features (like support for protected documents).

- **IT Controls:** Tools for the administration of Teams, including automation through PowerShell and Microsoft Graph.
- **Extensions:** The enterprise version of Teams supports extra first- and third-party apps, like Stream, Planner, Viva, and Dynamics 365.

Microsoft generates the different versions of Teams from a common code base. Some but not all of the new features for the common areas of functionality (like messaging and meetings) that show up in the enterprise version might appear in the other versions, but there's no guarantee.

Teams Premium

Teams Premium is an add-on product costing \$10/user/month that enables a set of security/compliance and artificial intelligence-based features designed to make meetings (in particular) safer and more productive.

Microsoft made [Teams Premium generally available](#) on February 1, 2023.

Here are some of the Teams Premium features:

- **Intelligent recap.** This is likely to be the most-hyped feature. Teams applies artificial intelligence on a per-user basis to extract information like action items from meetings. AI processes elements like the meeting agenda, chat, and notes to generate insights for individual users. Intelligent recap is the only Teams Premium feature shared with Microsoft 365 Copilot.
- **Live translations for captions.** Teams can generate real-time captions from spoken contributions in meetings. This capability allows users to choose to have Teams translate the captions generated in a meeting into their preferred language. Teams can translate 40 spoken languages into captions in 34 languages.
- **Meeting guides.** Organizations can create [meeting templates](#) that users can choose from when they create new meetings. A template contains preconfigured meeting settings (for instance, is the meeting recorded automatically) that administrators can assign for use to specific employees. New meeting settings, like who can record a meeting, are available. Templates can lock settings to stop meeting organizers changing options and organizations can apply sensitivity labels to force a template to have specific settings.
- **Custom branding.** Organizations can apply their branding to the graphics displayed in the Teams lobby and during the meeting pre-join process.
- **Meeting watermarking.** To prevent participants taking screenshots of confidential information presented during a meeting, each participant's video feed includes their user principal name (the watermark). Although this cannot stop someone from taking a photo of the screen and it's easy to edit out the watermark from a screenshot, its purpose is to dissuade and make people think twice before they attempt to share confidential information through screenshots.
- **Auto-application of sensitivity labels to meetings.** Sensitivity labels already support container management, meaning that when applied to a team, group, or site, the container inherits settings from the label. The same approach is used for meetings. When an organizer applies a sensitivity label to a meeting, the meeting inherits settings from the label.
- **Advanced webinars.** Several new settings will be available for webinars, including setting a registration start and end date, manual approvals for webinar participants, and operating a registration waitlist.
- **Advanced virtual appointments.** This feature allows users to set up customized virtual appointments with customers. According to Microsoft, the feature includes queue management and SMS reminders to avoid no-shows. This should be an attractive capability in industries like healthcare and financial services.

Microsoft targets Teams Premium at its high-end enterprise customers. Over time, it's likely that Microsoft will further differentiate its premium offering from the base product, if only to convince more customers to

upgrade. [Microsoft makes a 30-day test license](#) (for up to 25 users) available to organizations to test Teams Premium features. Tenants can claim the trial license through the Billing section of the Microsoft 365 admin center.

Microsoft also makes individual trial licenses available for Teams Premium through its self-service purchase program. These licenses last sixty days. See the User management chapter for details about how to manage the set of products available for self-purchase. Given the highly collaborative nature of Teams, it seems logical that organizations will get better information about the value of Teams Premium within their environment by running a structured test involving multiple users rather than encouraging individual self-service purchases.

Industry-Specific Versions

Microsoft has several packaged versions of Teams developed for different verticals. These include:

- [Teams for Healthcare](#).
- [Teams for Education](#).
- [Teams for Frontline Workers](#).
- [Teams for Government](#).
- [Teams for Nonprofit](#).
- [Teams for Retail](#).

Each package includes apps and customizations tailored for the vertical. For example, Teams for Healthcare includes the Virtual Visits app, while Teams for Retail includes apps like Shifts, Approvals, and Walkie-Talkie.

Teams Architecture

The Teams architecture integrates many facets of Microsoft 365 and exploits functionality from different Microsoft 365 applications and components. Figure 11-1 shows the major components in the Teams desktop client architecture. The current generation of Teams (2.1) clients are React-based and make use of the [Edge WebView2 control](#). Apps like Outlook already use Edge WebView2 for components like the calendar room finder and the Teams meeting add-in. You can [read more about the architecture here](#).

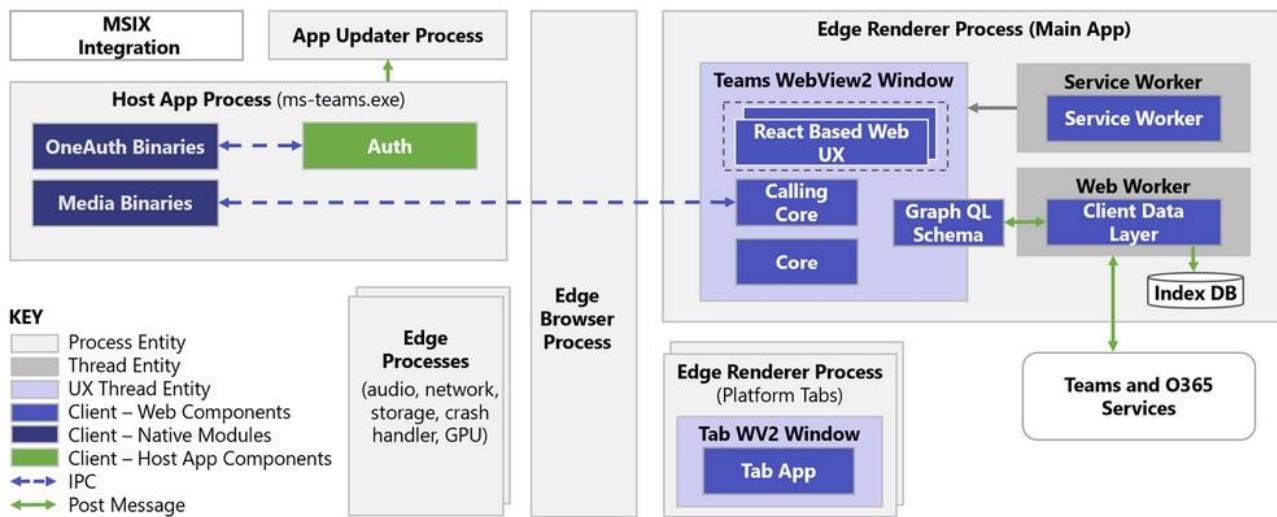


Figure 11-1: Teams desktop architecture (source: Microsoft)

Teams includes an experimentation layer to support the deployment of different features to targeted tenants. The layer allows Teams to deploy new features to targeted sets of users for testing at different stages of the development process. Users within Microsoft see a very early version of the feature, customers who sign up for testing through the Technology Adoption Program (TAP), or people who enable Teams preview run software that's still under development. Normal tenants only see the feature when Microsoft makes the software generally available.

At the server level, Teams consumes many services drawn from across Microsoft 365, including:

- A media stack shared with Skype consumer for video and audio conferencing.
- The MRU, or “Most Recently Used” service used to keep track of files accessed by users through Teams.
- Teams inbound email service to accept and process messages sent to Teams channels. Teams does not support outbound messages.
- Entra ID to authenticate tenant and guest accounts and to process cross-tenant access policies. Teams also consumes Entra ID services such as group expiration and B2B collaboration.
- Exchange Online for mailbox support. Each team has a group mailbox, and users access their calendar in an Exchange mailbox. In addition, Exchange Online provides special cloud-only mailboxes to store compliance records for guest accounts.
- Telemetry services to generate anonymized information about user activities.
- SharePoint Online and OneDrive for Business for document management.

Because the Teams architecture spans many interconnected pieces, triggers and notifications are used extensively to inform components when they need to do something. For instance, when a user posts a message into a conversation, Teams generates a new thread (for a new conversation) or adds the message to a reply chain (for an existing conversation). The members of the team or private channel hosting the conversation (known as the “roster”) need to know that a new message is available. This happens through direct notifications to desktop and browser clients connected to the Teams service and via platform-specific push notifications to mobile clients. At the same time, the new message synchronizes with clients.

In the background, components receive notifications about new messages to initiate further processing. For example, Teams might need to check a message against one or more data loss prevention policies. For compliance purposes, the Microsoft 365 substrate also captures one or more copies of the message and stores these items in Exchange Online. An update goes to the Activity Feed for each recipient, @mentions in the message might generate notifications in Teams or the operating system, and so on. Other actions, such as adding a new member to a team, lead to the capture of audit records in the audit log. In other words, actions within Teams can generate a cascade of further actions across a range of Microsoft 365 services.

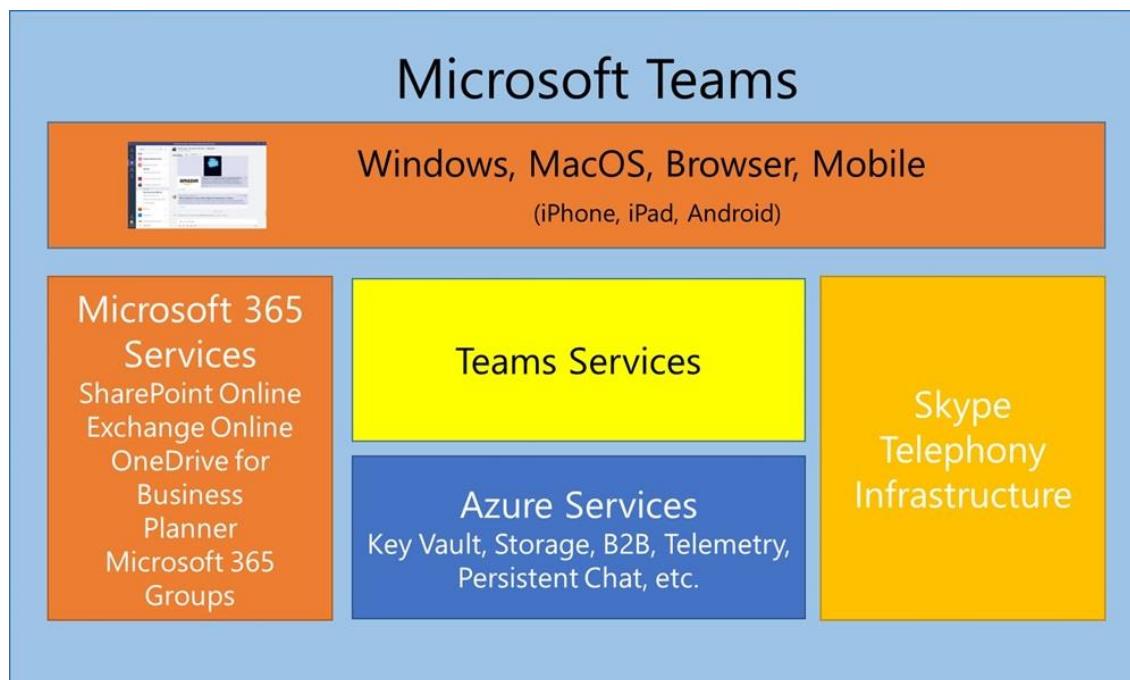


Figure 11-2: Building blocks for Teams

Figure 11-2 views Teams from the server perspective and divides its services into five major building blocks:

- Clients are available in desktop, browser, and mobile versions.
- Teams consumes a range of services drawn from other applications like Exchange Online and SharePoint Online to avoid recreating any wheels. See the later section covering dependencies on other services.
- Teams has its own set of microservices to manage different elements within its infrastructure. We discuss these microservices below.
- The voice, audio, and telephony components share a common infrastructure with the Skype consumer service.
- Teams consumes many Azure services. For performance reasons, the chat service stores recent chats in memory and commits its data to [Azure Cosmos DB](#). Teams stores images inserted in conversations in an Azure media store. Another example is the use of Azure B2B collaboration to support guest user access to Teams.

Microsoft publishes [architectural diagrams for Teams online](#) in PDF and Visio formats.

Teams Microservices

In addition to major service components, Teams uses many microservices. For example, the compliance microservice generates audit records about activities that occur in Teams, such as the creation or deletion of a channel. It also captures copies of personal and channel conversations for compliance purposes. Like all applications, Teams has some settings that are individual to it, like the settings that control whether users can remove or edit messages. The configuration microservice manages these settings and works with the synchronization microservice to manage other settings that affect Teams, like whether users can create new teams.

Synchronization with Entra ID also makes sure that changes to the groups that underpin Teams flow from Groups to Teams and Teams to Groups. It is important to ensure that membership and ownership changes are effective, user properties (like photos, job titles, and reporting relationships) become known to Teams, and that Teams executes its side of management actions like the deletion of a group (and its associated team). The expected synchronization interval is less than 15 minutes, but the defined SLA (internal to Microsoft) is 24 hours, so it might take some time before changes made to user or group objects in Entra ID appear in Teams or vice versa. The synchronization microservice is also responsible for the recovery of Teams components when an administrator recovers a soft-deleted group (see the Groups chapter for details).

Teams is a Collection of Apps

Apps form the basic framework of Teams. Some apps are fundamental to Teams, others are optional. Some come from Microsoft, others from third parties, and others are line of business applications unique to an organization. Administrators can control the apps made available to users through app setup and permissions policies (explained in the next chapter).

- **Fundamental Apps.**
 - **Teams:** Access to teams and channels, including the applications installed in the channels.
 - **Activity:** The activity feed.
 - **Chat:** Personal and group chats. This also includes federated chat with users in other tenants and Skype consumer users.
 - **OneDrive** (previously Files): Replicates the browser experience of the OneDrive for Business app within Teams.
 - **Calendar:** Access to the user's Exchange Online calendar.
 - **Calls:** Access to the Teams calling subsystem to make VOIP calls to other Teams subscribers and external parties (external calls and PSTN connections are available only after buying a calling plan).

- **Microsoft First-Party Apps for Teams:**
 - **Planner:** Access to group (Planner) tasks and personal (To Do) tasks.
 - **Viva Engage:** Access to communities and other employee engagement functionality.
 - **Insights:** Viva Insights for Teams combines insights from Viva Insights, Workplace Analytics, Wellbeing, and third-party data sources.
 - **Copilot:** For users with Microsoft 365 Copilot licenses, supports chats with Copilot about meetings, chats, and other information.
 - **Stream:** Access to videos managed by the Stream service.
 - **Forms:** Conduct polls (including during meetings) and questionnaires.
 - **Channel Calendar:** Access to meetings scheduled within a channel.
 - **Lists:** Access to Microsoft Lists stored in SharePoint Online.
 - **Meet:** Displays details of recent and upcoming meetings for a user.
 - **Approvals:** Basic approval workflow based on Power Automate.
 - **OneNote:** Access to OneNote notebooks.
 - **Praise:** Recognize the achievements of co-workers. The ability to praise co-workers is also available through the Viva Insights app and the Viva Connections dashboard. The app also allows users to track praise they have sent and received over the previous six months.
 - **Shifts:** Front-line worker shift setup and management.

Microsoft continues to develop new first-party apps for Teams to add functionality and demonstrate the power of the platform.

Dependencies on Other Microsoft 365 Components

Along with its microservices, Teams consumes a range of services drawn from other parts of Microsoft 365. These dependencies are:

- **Groups.** An Entra ID group object exists for each team. The members of the group are the members of the team.
- **Exchange Online.** The Teams Calendar app displays information synchronized from the calendar folder in the signed-in user's mailbox (the channel calendar app reads information about channel meetings from the group mailbox belonging to the team). The contacts used in the Calls application are in the user's mailbox, as is their profile picture. The Microsoft 365 substrate captures compliance records for channel conversations in the group mailbox belonging to the team while the compliance records for personal and group chats are in the mailboxes of chat participants. With [some limitations](#), users with on-premises mailboxes can use Teams. The most important requirement is that mailboxes must be hosted on Exchange 2016 CU3 or later (always use the latest available version of Exchange Server) to create and view meetings. This requirement exists because the Teams middle layer uses Autodiscover V2 to find how to retrieve mailbox and calendar data. Read more about [how Teams retrieves calendar information from Exchange on-premises servers](#) and how to [troubleshoot common issues](#).
- **SharePoint Online:** The Files channel tab gives users access to the SharePoint team site provisioned during the creation of a new team. Users do not need a SharePoint license to use it in Teams (in many cases, users have a SharePoint Online license through one or more of the product licenses assigned to their account) to use the Files tab, but SharePoint Online must be available within the tenant. Teams does not support SharePoint on-premises. SharePoint eSignature can be selected as the signature provider for the Approvals app.
- **OneDrive for Business:** Users require a OneDrive for Business license to be able to share files in personal and group chats (including loop components) and to store recordings of the meetings they organize.
- **Microsoft Forms:** Teams meetings use Forms for meeting polls and quizzes.

- **Planner/To Do:** The Tasks by Planner app integrates tasks created in Planner and To-Do. Team members can access Planner plans through channel tabs.
- **Power Automate:** The Teams Approvals app uses Power Automate as its workflow engine.
- **Microsoft Bookings:** The Teams [Virtual Visits app](#) depends on Bookings.
- **Whiteboard:** Teams meetings can share whiteboards to allow collaboration around a shared canvas.

In addition to these base services, Teams takes advantage of other Microsoft 365 components to extend its functionality as required by channel tabs and apps. Examples of other Microsoft 365 components used by Teams include Stream, Microsoft Information Protection, OneNote, the Office Online apps, workflows, Power BI, and actionable messages.

Teams and Service Plan Licensing: Products like Office 365 E3 and Office 365 E5 include access to the service plans for all the Microsoft 365 components listed above, meaning that users can use the individual services as needed. However, administrators can disable selected service plans. For instance, they could decide to disable Forms and Power Automate because the organization considers these services unnecessary. If this happens, users cannot access the standalone services, and they won't be able to use Teams features that depend on those services.

Teams Limits

Microsoft's service limits for Teams are [documented online](#). Because of its dependencies on other Microsoft 365 components, some of the limits applying to Teams come from those components. For example, while Teams can support hundreds of thousands of teams in a tenant, only 5,000 of those teams can have dynamic membership due to an Entra ID restriction.

Each team has a fully provisioned SharePoint Online team site to hold files, the shared notebook, lists, and videos. The storage used by team sites comes from the overall quota available to SharePoint Online in the tenant. Usually, SharePoint manages storage automatically and assigns storage to individual sites as necessary. You can also configure SharePoint for manual storage and [set specific limits on sites](#). If necessary, organizations can buy extra storage to increase the overall amount available to the tenant.

Microsoft has not documented any restrictions on the number of conversations, messages, or graphics that Teams can hold for a tenant in its Azure-based services. Teams does not apply any numeric or storage quotas for messages in a single team or channel.

Teams mega-tenants: Some tenants need to support more Entra ID objects than allowed by [the service limits](#). For instance, some education tenants need to go past the limit for groups (500,000). Microsoft has a process to allow customers who need to exceed the documented limits. If you're in this situation, contact Microsoft support and ask how to increase the limits applying to your tenant.

Teams Storage

We've already mentioned how Teams uses different cloud locations to store its data, such as how SharePoint Online stores the files created through the Files interface. Table 11-1 describes how Teams stores the different types of data used by its components. The dependencies that exist with other parts of the Microsoft cloud are obvious.

Data	Primary Storage	Other Storage
Messages	The Chat service stores its messages in Azure Cosmos DB.	Compliance records (copies of messages) are in group and personal Exchange Online mailboxes.
Images	Media service (Azure) using blob storage.	Any images referenced in messages are copied into compliance records and stored in Exchange Online.
OneDrive and Files	Personal files are in users' OneDrive for Business accounts. Files shared in channels are in the team's SharePoint document library.	
Voicemail	Personal Exchange mailboxes.	
Recordings	Meeting recordings are in OneDrive for Business (personal meetings) or SharePoint Online (channel meetings).	Links to recordings posted in the meeting chat.
Calendars	Group and personal Exchange mailboxes.	
Contacts	Personal Exchange mailboxes.	
Telemetry	Microsoft data warehouse (inaccessible to customers).	
Meeting resources	Transcripts, attendance, and registration reports are in the Exchange mailbox of the meeting organizer.	
Loop components	SharePoint Online stores Loop components used in channel conversations. OneDrive for Business stores Loop components used in chats.	

Table 11-1: Where Teams stores its data

The messages making up Teams channel conversations and personal chats form "reply chains" (the original topic and all subsequent replies). Messages for channel conversations remain in the Teams store unless removed by retention policies or the deletion of the team. Unlike channel messages, which the hosting team owns, participants in a personal or group chat collectively "own" the messages in a conversation. Messages remain in the Teams store unless removed by retention policies or following the removal of the accounts of all participants.

Geographic Location of Teams Data

Like other non-core workloads, Microsoft does not store the Teams-specific data in every data center region. This data includes personal chats and channel conversations, teams and channel metadata for a tenant, and media inserted into chats (data inserted by Teams into SharePoint and Exchange exists in the data center region to which a tenant belongs). The Microsoft 365 substrate captures copies of chats in group and user mailboxes to make them available for searches and eDiscovery. The storage for images and media used in chats (except for Giphy GIFs, which Teams stores as a URL to the original file) runs in an Azure-based Media service deployed alongside the chat service.

Although Teams is not yet available in every data center region, Microsoft plans to deploy the necessary Azure services to support Teams more broadly to satisfy customer data sovereignty concerns. Microsoft documents the [current set of data center locations for Teams data online](#).

Some data accessed through Teams might be in other data center regions. For instance, in a multi-geo situation, a team's SharePoint site (holding documents, the shared notebook, and videos) runs in the same region as the person who created the Microsoft 365 group for the team. The user's personal Teams data such as the compliance records captured for personal and group chats and any OneDrive for Business documents

shared in chats are in the satellite region. Remember that Microsoft's commitment to data sovereignty only extends to the data that they manage and does not include third-party data accessible through Teams. For instance, if you create a tab for Trello, the data manipulated through that tab are in Trello's cloud and might be outside the region.

The Structure of Teams

A team can have up to 25,000 members. The basic structure for a team is a set of channels that give members a framework to organize conversations (discussions composed of "persistent" chats) and other relevant information, activities, and applications. A channel is a dedicated section within a team used by members to communicate about a topic, like a space to organize a project that the team must manage. All team members can see everything in a channel, so if you want to keep something private, you must do so in a personal chat. Only the people involved in a personal chat can see what goes on there.

Private teams limit access to any team resources to people added as team members, including guest members. Public teams are open to anyone who wishes to join. When someone joins a team, they can work with the resources available to the team. When they leave a team, they lose access to those resources. Although some restrictions do exist for guest members, the principle that all members share equal access to team resources holds true.

Owners and Members

Teams use Groups to manage team membership, which means that the roles available within a team are owners (who manage the team) and members. An owner is also a member and there should be at least two owners for each team to make sure that someone is always available to handle basic administration such as adding new members. If all the owners leave a team (perhaps because they leave the organization), a tenant administrator can promote a member to become an owner or add a new owner to the team. Unlike Groups, Teams does not support the concept of subscribers who receive copies of any new posts for a conversation via email. If a member wants to see what is happening inside a team, they must open it to join in the conversation.

A team owner can promote any other team member except a guest to become an owner. To do this, use **Manage team** to display the current membership and then click the down arrow in the role column beside the member's name to select Owner. When someone is a group owner, they automatically become an owner (or administrator) of the associated team and can perform actions such as adding or removing users, adding new channels and apps, and so on. To remove owner status, reverse the process and change Owner to Member. If you want to remove an owner from a team, you must first demote them to Member status and then remove them by clicking the **X** alongside their name. If an owner removes a user from a team, they also lose their membership in the underlying group. You cannot have a situation where a subset of the members of a group can access the associated team and other members cannot.

Like any other group, a team can have up to a hundred owners. An individual user can create up to 250 teams. However, a global administrator can create as many teams as they need to within a tenant.

Communications Rosters and Disabled Accounts

The membership of each team comes from its Microsoft 365 group. Internally, Teams uses the concept of communication rosters or people who can communicate with each other, to control access to features. For example, in hybrid environments, you can synchronize disabled AD accounts with Entra AD. Because these users cannot communicate with the other team members, Teams excludes these accounts from its rosters even though they are present in the underlying group (you can see this by running the `Get-MgGroupMember` or `Get-TeamUser` cmdlets against the group). Organizations often disable the accounts of ex-employees to

stop them from accessing applications. Disabled accounts can't sign into Microsoft 365, so Teams suppresses their presence because they can't participate in conversations, share files, or otherwise engage with the rest of the members. The membership of private channels is another example of a roster used by Teams.

Teams also removes blocked user accounts from the rosters of regular and org-wide teams. A Teams background process scans for blocked accounts and removes them from the rosters (but not from the underlying Microsoft 365 Groups). This process can take some time to happen. Upon the unblocking of the account, Teams restores the account to team rosters. Some [issues exist in this process](#) that you should be aware of.

The General Channel

Channels divide conversations into logical sections within a team. Every team has a default regular channel called "General" (or the local language equivalent), which is the physical embodiment of the team. Team owners cannot remove the General channel. However, team members can hide the General channel from their channel view. If the General channel is the last channel in a team, this action also hides the team. The member can reveal the channel again by marking it to be shown in the team channels list.

The General channel is often where team owners post information about the team's goals and charter and discuss topics such as what those goals should be or how to reach them. People often recommend that the General channel should be kept for announcements and other information related to the team. To do this, they update the channel settings to restrict the ability to post messages to team owners only.

From August 2024, team owners can rename the General channel to update its display name to match its intended purpose. A channel name can be up to 50 characters long (some [restrictions on characters exist](#)). The General channel can be renamed as many times as you like, but once renamed, it can never be given the "General" name again. This is because Teams treats this name as a reserved word and doesn't allow team owners to use it for a channel.

Managing Channels

To support discussions, team owners create a set of channels in the team and encourage users to post conversations into these channels rather than the General channel. Before moving the focus of conversations away from the General channel, team owners should think about how to use channels to organize the work of the team. A well-thought-out, well-named, and logical channel structure avoids the potential that the team becomes a confusing mess. When the overall structure of the team is known, you can create the channels and encourage users to think about which channel is best for their posts.

In addition to conversations, channels host extensions like tabs, apps, and bots. These components allow owners to equip teams with the necessary functionality needed by members. You can also mail-enable a channel by asking Teams to generate an SMTP email address for the channel (see the Teams management chapter). When a channel is email-enabled, authorized users can send emails to the channel to start conversations. The email capability only extends to inbound communications as Teams does not support the ability to send email as a channel or on behalf of a channel.

Teams supports three types of channels:

- A **regular channel** is available to all team members. This is the default type of channel created by Teams. The General channel is always a regular channel.
- A **private channel** is available to a subset of the team members. A team can support up to 30 private channels, each of which has a dedicated SharePoint site to hold the files for the channel. Like a regular channel, you can add tabs (except Forms, Stream, and Planner) to private channels. A private

- channel supports up to 250 members, all of whom must be members of the team owning the private channel before they can join the channel membership.
- Individual teams can host **shared channels**. The membership (or roster) of a shared channel is composed of individual members and teams from the host tenant or external tenants who want to collaborate on a common topic. People who aren't members of the host team can join a shared channel. Like private channels, each shared channel has its own dedicated SharePoint Online site.

A single team supports a maximum of 1,000 channels, including deleted channels (which expire after 30 days). Any combination of channel types is supported, but you can only include up to 30 private channels in a team.

Table 11-2 compares the capabilities available in the three types of channels. The limited support noted for channel tabs, apps, and bots for shared and private channels reflects the need for app developers to support these channels and the authentication models used to limit access to channel membership.

Capability	Standard channel	Private channel	Shared channel
Guest access (B2B Collaboration)	Yes	Yes	No
Federated access (Direct Connect)	No	No	Yes
Automatic access to all team members	Yes	No	No
Join channel without team membership	No	No	Yes
Share channel with other teams	No	No	Yes
Share channel with the parent team	No	No	Yes
Channel moderation	Yes	No	No
Breakout rooms	Yes	No	No
Email support for channel	Yes	Yes	Yes
Dedicated SharePoint site	No	Yes	Yes
Support for scheduled channel meetings	Yes	No	Yes
Support for channel tabs	Yes	Limited	Limited
Support for bots and apps	Yes	Limited	Limited
Planner support	Yes	No	No
Tag members in channel conversations	Yes	No	No
Channel analytics	Yes	No	No

Table 11-2: Capability comparison for Teams channel types

Guest members enjoy full access to everything in a team except private and shared channels. They can access a private channel, but only after a channel owner adds their account to the membership of that channel. Shared channels don't support guest accounts as members. However, a guest member with a Microsoft 365 account can join a shared channel if the channel owner sends an invitation to their account in their home tenant. In this scenario, the user joins the shared channel using their account from their home tenant rather than their guest account, which belongs to the host tenant.

Inactive Channel Clean-Up

Inactive channels existed well before the introduction of the 1,000 channel limit per team. An inactive channel is one where nothing happens – no new conversations, no replies, and no activity. With so many channels available, the potential for inactive channels is obviously greater. From a user perspective, the problem is that they might have inactive channels in their channel list. They can hide these channels, but serendipity and lack of time usually means that people don't do a good job of hiding inactive channels. The result is that the channel list becomes cluttered with channels that the user never goes near.

To assist with the problem, Teams checks channel lists periodically to look for channels that the user hasn't accessed in the last 45 days and hides these channels. The review happens for both tenant member and guest

accounts. Users have the chance to review the set of inactive channels before they are hidden, and they can opt out of the automatic channel clean-up process through Teams settings. The settings app also includes the option for users to perform a channel clean up on demand.

When a user hides a channel or Teams automatically hides a channel, it affects the notifications from the channel that appears in a user's activity feed. Team and channel mentions, reactions, replies, and apps no longer appear, and the only notifications shown are when the user is tagged or personally mentioned.

Channel Type and Controlling Creation

You cannot convert a channel from one type to another. Once you assign a type when creating a channel, a channel retains that type until its deletion. If you make a mistake and create a channel with the wrong type, you must delete the channel created in error and create a new channel of the correct type. The teams policy assigned to an account controls its ability to create:

- Org-wide teams (*AllowOrgWideTeamCreation*)
- Private channels (*AllowPrivateChannelCreation*)
- Shared channels (*AllowSharedChannelCreation*)

In addition, policy settings are available to control if a user can share channels with external users or participate in shared channels hosted by other tenants. These settings are available through the Teams admin center or PowerShell. For example:

```
Get-CsTeamsChannelsPolicy | Format-List Identity, AllowPrivateChannelCreation,  
AllowSharedChannelCreation, AllowChannelSharingToExternalUser,  
AllowUserToParticipateInExternalSharedChannel
```

Identity	: Global
AllowPrivateChannelCreation	: False
AllowSharedChannelCreation	: True
AllowChannelSharingToExternalUser	: True
AllowUserToParticipateInExternalSharedChannel	: True

Although organizations can control the creation of private and shared channels by policy, there's no policy to control the creation of regular channels. Creation of regular channels is controlled by settings in individual teams where owners can decide if team members (including guests) can create new channels. If an organization wants to stop team members creating new channels, they must update the *AllowCreateUpdateChannels* setting for a team to False. The process is [discussed in this article](#).

Channel Purpose

Each channel should have a clearly defined purpose. For instance, a team might have a channel for their weekly update calls and others for specific topics, like ideas for a marketing campaign or plans for a trade show. Although the ability to split conversations over many channels gives a wide degree of latitude in the topics supported by a team, the trick is to create just the right number of channels. Creating too many channels runs the risk of confusing users (the "where do I start this conversation" syndrome). Take the example shown in Figure 11-3 (taken from a real-life deployment). How do you think the average user will respond when they see that a team has 114 hidden channels to explore? How will the average person decide what channel is the best destination for their topic? The other side of the coin is that too few channels can result in a mixture of wildly different topics in channels and lead to people losing sight of important conversations. It's important to achieve a balance, with the preference to go slowly when creating new channels.



114 hidden channels New

Figure 11-3: Too much choice in too many channels?

When users find channels with content that interests them, they can follow those channels so that notifications for items posted to the channel appear in their activity feed. Unless you like dealing with hundreds of notifications daily, it can be a bad idea to do this for a busy channel. Instead, users should only choose channels where they want to see notifications of new activity.

Naming Channels

A channel should have a name and description to inform members what they should expect to discuss in the channel. When composing the name of a channel, you cannot use the special characters (~#%&*{}+/\>?|"), but you can include the @ sign. You can include a full stop in a channel name if it is not at the end. You can also include emojis in channel names.

Although you don't need to enter a description for a channel, it is good practice to do so. Teams displays the name given to a channel no matter what language someone uses. For this reason, in multinational organizations, it is wise to seek channel names that make sense in as many languages as possible. This isn't needed for the General channel because Teams displays a translated value for "General" based on the language chosen for the client. For instance, the channel is *Général* in French and *Allgemein* in German.

A team owner can edit channel settings to rename a channel if necessary. Until September 2021, Teams didn't synchronize the new name assigned to a channel with SharePoint Online, meaning that the channel name shown in Teams could differ from what appeared in SharePoint Online. Microsoft then deployed an update to make sure that Teams renames the folder created for the channel in SharePoint Online when it renames a channel. Channels renamed before September 2021 did not synchronize their name with SharePoint Online, so if you want the same name to appear in both places, you must rename the channel again.

Showing Channels and Notifications

Some teams have more channels than others and the discussions in some channels are more interesting than others. Users can organize the channels that they find most interesting by making sure that these channels are visible while putting the less interesting channels into the background. For instance, you might want to keep channels where active discussions about your current projects happen in the foreground while pushing channels used to track posts about code updates or similar developments into the background. Use the **Show** option (in the ellipsis menu) to mark a channel to appear in the visible list while the **Hide** option puts it on the hidden list. You can decide to access a channel at any time (with or without putting it back into the visible list). Note that if you create a channel, Teams assumes that you want the channel to be visible and makes it visible.

To help new members get to know the ebb and flow of what happens inside a team when someone joins a team, the application automatically adds the five most popular channels from the team to the visible list, meaning that the channels appear under the team name when you open it. Popular means the busiest channel in terms of conversations. The user can accept the recommended set of channels or organize a custom list by hiding and revealing available channels. If a team has fewer than five channels, Teams automatically adds all existing channels to the shown list for new members. When they create a new channel, owners can mark the channel to show up automatically in the list visible to team members, which is a good way to make members aware of the existence of an important new channel. If an owner forgets to highlight an important channel, they can do this later through the Channels section of team settings by checking the auto-show box. Users can always hide the channel if they decide that they don't consider the content to be important.

Some channels are inevitably more important than others. For these channels, use the **Channel notifications** option in the channel menu to enable notifications for new posts and replies in the channel. You can choose to have notifications for:

- All new posts.

- All new posts and replies.
- Channel mentions.
- Chat message notifications.

Notifications come in two types: banners and the activity feed (you can choose both). A banner is a notification message that pops up to tell the user that someone has posted in the channel. Banner notifications can become quite distracting, especially in busy channels, so it is usually better to have Teams update the activity feed with notifications for these channels. If the notification settings are not set for a channel, Teams uses the settings for channels in the Settings app.

Pinned Channels

Over time, the number of teams and associated channels available to users will inevitably grow. This can create a challenge for users to keep track of the channels where the most important discussions occur as their activity feed becomes cluttered and they receive too many notifications. The solution is to use the **Pin** option (in the channel menu) to mark selected channels as important.

Teams places the set of pinned channels on top of the teams list in the sidebar. Teams lists the set of pinned channels in the order the user pins them to the list and the user can reorder the list by dragging and dropping channels into their preferred order. The name of the team a pinned channel belongs to appears under the channel name, and if the channel has unread messages, Teams highlights this fact by bolding the channel name. The user can remove a channel from the pinned list at any time with the **Unpin** option.

Dealing with Obsolete Channels

Some channels become underused or obsolete over time. Given that a team can support up to 1,000 channels, it's important that team owners manage channels so that members don't have to navigate through an array of obsolete channels to find current information. To clean up channel debris, owners can either delete or archive any channel except General.

Deleted channels enter a holding pattern for 30 days. During this period, team owners can restore the channel through the Channels section of the Manage team dashboard. After 30 days, Teams removes deleted channels and they become irrecoverable. The content in the channel folder in the team's SharePoint Online document library remains unaffected by the channel deletion. There's no way to force the removal of a deleted channel before the 30-day retention period lapses.

Archiving a channel removes it from the active channel list and puts the channel into a read-only state. Users can still access the channel, but they cannot post new items to the channel or edit existing messages. Optionally, the channel folder in SharePoint Online can be made read-only. Team owners and administrators are unaffected by the read-only state of archived channels and can post new material to these channels if necessary. Archiving is unsupported for private and shared channels.

Before deleting a channel, it's a good idea to update its display name to indicate that it is pending deletion. This allows users to look through the messages in the channel to see if any valuable information exists that team members should extract and keep (you can't copy or move channel messages to another channel in the same or another team). It's also a good idea to check the contents of apps reached through channel tabs. Then, when you're ready to mark the channel as obsolete, a team owner can:

- Use the Edit this channel option to change the channel name. For instance, you could insert a Windows emoji (accessed using the Windows logo key and period) as a prefix as a visual marker for the channel's status, and then add a suffix to indicate that it is obsolete. For example:

🔴 Champions (now obsolete)

Also, make sure that the *Automatically show this channel in everyone's channel list* checkbox is not set.

- Post an announcement to the channel to tell team members the deletion date for the channel.

Another approach is to implement a two-step removal process by archiving obsolete channels for a period before proceeding to deletion.

No Way to Reuse Channels: If a channel becomes disused, you can remove it to clean up the team. However, you cannot then reuse the same name for a new channel in that team. Once a channel name exists within a team, Teams does not allow you to reuse it. Microsoft says that the restriction exists "for information protection scenarios."

Private Channels

Private channels have a small lock shown against their name to mark them in a team's channel list. You can't convert a regular channel to become a private channel or vice versa. Administrators can manage the membership of private channels through the Teams admin center. However, administrators or team owners cannot access the content of private channels unless they are a member of the channel.

Private channels handle scenarios such as the need to limit access to information to a subset of a team. For example, if you create a team to work on a project, there might be financial or other sensitive aspects of the project restricted to people directly involved with that data. To address the need, you can create a private channel in the team and add those people, including guest users, to the membership of the channel. Only the channel members can then access the conversations in the private channel and the files in the SharePoint site belonging to the channel.

Channel owners can add members to a private channel using the Teams client. Team owners and administrators can update channel membership with PowerShell. However, team owners can't access the contents of a private channel unless they become a member. Although they can see private channels listed in the Channels tab of the Manage team option in the Teams client, if they're not a member, the only sign of activity in a private channel available to a team owner is through administrative interfaces. For instance, if they use the *Get-SPOSite* cmdlet to examine the properties of a private channel, the *LastContentModifiedDate* property might indicate recent activity in the site belonging to the channel. Audit records for file activities in the channel are available in the audit log.

Because the channel owners manage the membership of a private channel, these channels need at least one owner. If the last channel owner leaves a tenant (for instance, an administrator deletes their account), the Microsoft Teams AadSync background process detects that the channel is now ownerless and selects a channel member at random and promotes that member to be the channel owner. The user receives a notification of their new status and can then decide if they wish to hand over the responsibility to another channel member by promoting them to be an owner.

The SharePoint Online sites used by private channels inherit their properties and membership from the parent team. A synchronization process updates the site properties when necessary. If an administrator updates the site properties using a SharePoint admin interface, the synchronization process will reverse the change within six hours.

Limiting Creation of Private Channels

By default, any tenant user can create a private channel. If you want to limit the creation of private channels, go to the Teams section of the Teams admin center, and edit the Global (org-wide default) Teams policy to change the **Create private channels** settings to **Off**. Then create a new Teams policy with Create private channels set to On and assign this policy to the accounts you want to be able to create private channels. The PowerShell *Get-CsTeamsChannelsPolicy* cmdlet returns details of the Teams policies in a tenant (the *AllowPrivateChannelCreation* property is the one you're interested in), while the *Grant-CsTeamsChannelsPolicy* cmdlet assigns an appropriate policy to accounts.

Shared Channels

Shared channels are part of the Microsoft Teams Connect initiative. Shared channels depend on a new federation mechanism called Azure B2B Direct Connect. External users can present credentials gained by signing into their home organization and have another Microsoft 365 tenant accept their credentials to authenticate access to resources in that tenant. This mechanism eliminates the need for guest accounts as used for team membership. This does not mean that guest accounts are bad or that Microsoft will remove them. Direct Connect is a different way to grant access to tenant resources that comes with its foibles and concerns.

Users do not need to switch tenants to access shared channels hosted by other tenants. Teams clients use the authentication granted through Direct Connect to open and display shared channels alongside standard and private channels from the user's home tenant. Figure 11-4 shows the manage channel screen for a shared channel. In the teams list, the set of channels for the selected team includes standard, shared, and private channels. As a further visual indicator to users, when browsing the teams list, teams from other tenants with shared channels display the name of the home tenant under the team name, as in "@Tenant Name."

Name	Organization	Members
Office 365 Adoption	[REDACTED]	9
Sales Department team	[REDACTED]	4
Collaboration Central	o365maestro	5

Figure 11-4: Three types of channels are visible in the Office 365 Adoption team

Cross-tenant access settings control Direct Connect sharing with other organizations. Cross-tenant access works on a mutual trust basis. In other words, the tenant hosting shared channels must be happy to allow inbound access for external users while their home tenants must allow outbound access (to allow the users to access resources in the host tenant). If you allow inbound access to a tenant and that tenant doesn't allow outbound access to your tenant, mutual trust doesn't exist, and adding external users to shared channels isn't possible. When trust exists with another tenants, the owners of shared channels can add users and groups from those tenants to a shared channel. When a trust is unavailable, the Teams client highlights this issue and, if enabled in Teams settings, displays a link to a web page to allow the channel owner to get more information and (optionally, if the web page supports this functionality) request administrators to create a cross-tenant access policy to establish trust with the target tenant.

The simplest policy allows inbound access and outbound access from any other Microsoft 365 tenants. However, cross-tenant access settings can limit sharing to a granular level. For instance, only members of a specific group can join shared channels in a specific tenant, or only specific external users or groups (identified by the GUIDs pointing to the user objects in the directory of the external organization) can join shared channels in your tenant. Applying granular control to cross-tenant settings is an Entra ID P1 feature. It's usually best to start with a policy that allows flexible sharing and then amend the policy over time as necessary. See the Identities chapter for more information about cross-tenant access settings.

Like private channels, shared channels have owners who manage the channel membership. Channel owners, who can only be accounts from the host tenant but do not have to be a member of the host team, can share a channel with:

- People (individual users from inside or outside the tenant). There's no need to add users from the home tenant to the host team. The first time an external user accesses a shared channel in a host tenant, they must give consent to allow the host tenant to access details of their profile like their picture, display name, and email address. This information is available to other channel members in the channel roster and profile cards. A shared channel supports up to 5,000 direct members. This number includes invited teams. As noted earlier, because a user's home tenant performs authentication, you can't add a guest account as a member of a shared channel. If you want someone to join a shared channel that already has a guest account in your tenant, you ignore that account and invite their account in their host tenant to join.
- A team (invited using the email address of an owner of the team). Only tenant members from the team will join the shared channel. You can share a channel with a team that has dynamic membership, but you can't share a channel with an org-wide team. A shared channel supports up to 50 teams as members.
- A team from the home tenant that's owned by the channel owner. Teams lists the available teams, and the channel owner selects which one to add.

To share, a channel owner selects the appropriate action from the Share dropdown menu. In Figure 11-4, the *Share with people* option is visible, this shares with individual users. We can see that the current membership of the shared channel includes three teams, including a team from an external tenant. The membership of a shared channel can contain individual users and teams from multiple tenants.

In the case of team membership, an individual's access to the shared channel is available only while they remain a member of a team in the shared channel's membership. Channel owners must invite users or teams to share a channel. Users or teams cannot browse for shared channels and decide to join on their initiative. You cannot invite a guest account to share a channel. Invitations are only valid when extended to full member accounts in the home tenant or other Microsoft 365 tenants.

When a channel owner extends a sharing invitation to the owner of a team, that person sees the invitation in their activity feed and must respond within 14 days. During this period, the channel owner can see the status of the invitation and how much time remains before the invitation becomes void. Once extended, the channel owner cannot revoke an invitation. However, they can reject the acceptance when it comes back from the team owner. Part of the response is the selection of the team whose members will gain access to the channel (this cannot be an org-wide team). When the channel owners receive the response, they can review the team selected by the team owner and decide if they wish to share the channel with the nominated team. A channel owner can see the number of members in the chosen team, but they cannot see any details of the individual members. If necessary, the channel owner who processes the response can reject it. If accepted, Teams validates the membership of the chosen team to ensure that none of the members conflict with the cross-tenant access policy. Teams drops these members, as also happens for any guest members of the team. After Teams completes its check, the team shows up in the membership of the shared channel. A member of a shared channel can leave it at any time, and the owner of a team that shares a channel can remove the entire team from the sharing roster when they wish.

Teams limits members of a shared channel to whatever resources are available to the channel, including a SharePoint team site associated with the channel. External members can only see limited directory information for other channel members, but they can chat or call anyone in the channel. Teams adds an External suffix to the display names of external members to indicate their status. In addition, if a shared channel has external members, Teams flags this with a banner saying *This channel is shared with members in other orgs.*

Unlike private channels, which only support Meet Now meetings, shared channels support both Meet Now and scheduled meetings, but only tenant users can schedule meetings. The person who schedules the meeting becomes the meeting organizer, but the meeting is a channel meeting, not a personal meeting. The Teams channel meeting app does not currently support shared channels. Microsoft stores the calendar data for a shared channel in the cloud-only mailbox created to store compliance data for the channel.

Archive Channels

Over time, it's possible that some channels reach a point where they are no longer in active use but still contain useful information. In these cases, team owners can archive the channel. The channel remains online but it's no longer possible to post new items or edit existing items (including reacting to a conversation). Optionally, team owners can set the SharePoint folder for the channel to be read-only to prevent team members uploading new content to the folder or altering whatever's stored in the folder. If the folder subsequently needs to be reactivated, a team owner can restore it from the Channels tab in the Manage Team screen.

Channel Information Pane

The channel information pane displays information about a channel including the sensitivity label (if applied) and:

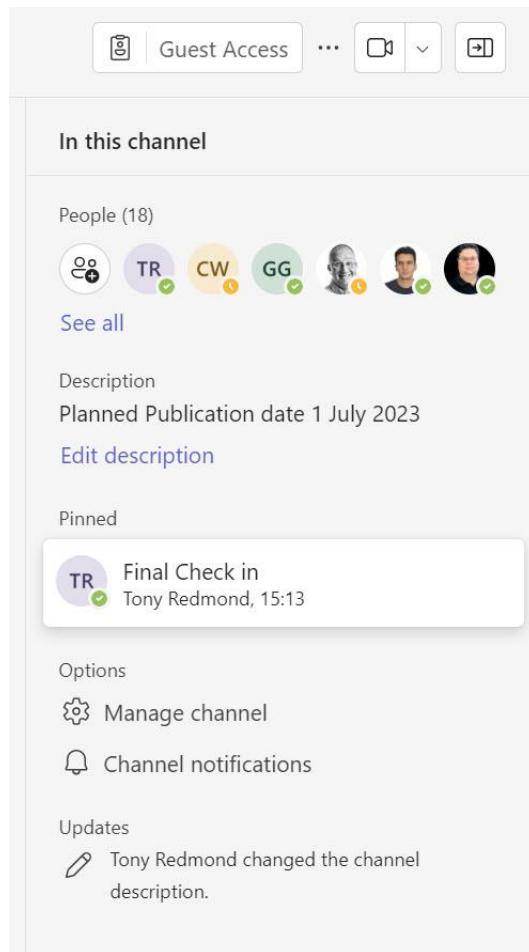


Figure 11-5: Channel information pane

- **People:** Members who have recently participated in the channel by posting or replying to the last twenty topics in the channel. If you select *See all*, you're brought to the Manage team screen to view the full list of owners, members, and guests.

- **Description:** The channel description.
- **Options** to manage the channel or update how channel notifications appear.
- **Pinned messages.**
- **Updates:** This is where Teams posts system messages covering team membership changes and channel updates (Figure 11-5).

When you see *Unknown User* in a system message, it means that Teams can't find a matching Entra ID user account. Usually, this is because of a deleted account. A note that *Microsoft Teams AadSync* has added or removed someone from a team means that the action happened through some other administrative interface, like an update to a Microsoft 365 group using the Exchange Online PowerShell module. Teams learns about changes made to group membership by monitoring a pipeline within Entra ID. When a change is detected, the *Microsoft Teams AadSync* process replicates the change to Teams to update the team roster.

Any team member, including guests, can pin or unpin a channel topic or reply. No limit exists for the number of pinned messages in a channel. However, the channel information pane only shows the three most recently pinned messages.

Channel Tabs

Users access the content owned by a channel through a set of tabs. A tab is analogous to a browser tab and acts as a link to a resource available within the channel. Some channel tabs are available only to regular channels while others are available in shared and private channels too. Conversations and Files are default tabs that appear in all channels. Examples of other tabs that you can add to a channel include:

- **Planner:** Link to a Microsoft Planner plan owned by the underlying group.
- **SharePoint:** Link to a SharePoint site or folder to which team members have the necessary access rights.
- **OneNote:** Link to sections of the shared OneNote notebook for the underlying group.
- **Power BI:** Link to a Power BI report or workspace.
- **Office documents:** Link to specific Excel, Word, or PowerPoint documents in the SharePoint document library for the team. You can also add a link to a **PDF** document in the same manner.
- **Stream:** Link (URL) to a video file or channel stored in Microsoft Stream. Stream videos play inline in chats or channels without needing to display the Stream browser client.
- **Website:** Link to the URL for any website. From April 2024, the Teams client launches websites in a new browser tab instead of rendering the site within the client. This article describes how [to generate a report about website channel tabs](#).
- **Visual Studio:** Link to a Visual Studio Team Services board to allow the team to work on code projects.
- **Third-party apps** such as YouTube, HootSuite, Smartsheet, Polyscribe, Trello, Intercom, Polly, Zendesk, and Asana. You can browse the complete set of available apps through the Teams Store.

Where it makes sense (as in the case of links to individual documents or websites), you can assign your chosen name to the tab. When someone adds a new tab to a channel, Teams highlights the tab with a "New" icon. The icon stays for seven days after the creation of the tab and then disappears. It also disappears after you access the tab for the first time.

Maintaining Team Membership

Teams does not maintain a central directory of teams (like the Exchange Online Global Address List) to allow end-users to browse to find teams to join. People can find teams to join through suggestions or owners can add them to team memberships, but there's no notion of browsing to find interesting teams. In some way, the lack of a directory is understandable because not all teams are public and some host very sensitive

discussions, so no desire exists to make their existence known to all users. To avoid team sprawl when people create new teams unnecessarily because they don't know of the existence of another team dedicated to the topic they want to discuss, some tenants create and publish a Teams directory. [This article](#) explores how to use PowerShell to generate a suitable report for the Teams directory and the ways to publish the directory to users.

The usual ways people join teams include:

- Tenant or Teams administrators add users to team memberships via **admin portals**.
- Administrators can also update team memberships **programmatically** using PowerShell or the Microsoft Graph.
- Team owners can **manage the membership** of their teams, including being able to add guest users if allowed by policy settings.
- **Members of a team** (except guests) can add another tenant user to the membership from the team's [...] menu. If the team is private, an email request to add the new member goes to the team owners for their approval.
- Tenant accounts can **discover and join teams** suggested by Teams based on their membership of other teams and other signals gathered in the Microsoft Graph.
- Tenant accounts can also receive a **code or deeplink** to join a team.

In all cases, when someone joins the membership of a team, they also join the underlying group and can access all the resources available to both the team and the group. A user account can be a member of a maximum of 1,000 teams (including archived teams).

Suggested Teams

To find new and interesting teams to join, tenant users can browse the set of suggestions that Teams creates for them to join by selecting **Teams** in the navigation bar and then **Join team** from the + sign (guests do not see this choice). Teams uses signals collected in the Microsoft Graph to display a list of suggested teams the user might like to join. The list can contain both public and private teams. The display of private teams in the join team gallery depends on the sensitivity labels applied to those teams. See the information protection chapter for more information.

Many suggestions are based on "common interests" shared by the existing membership and the potential new member. In other words, if a public team exists with a membership composed of people who are also members of other teams with the user, a reasonable chance exists that the user will be interested in the topics discussed in that team. Groups perform similar calculations when users browse for groups to join. The computations to suggest teams to users occur behind the scenes and it takes up to a day after its creation or after a team's access changes from private to public before Teams suggests a team to users.

To join one of the suggested teams, move over the icon for the team and a **Join team** button appears. Click the button and the team appears in the navigation bar for the user to access its resources. Once someone is a team member of a public team, they can add new members by selecting **Manage team** from the ellipsis menu for the team, followed by **Add Member**. If the team is private, requests to add members to the team are routed to team owners for approval.

Limited Directory Searches: If a tenant uses Exchange address book policies to set the scope for users to see items in the directory (enabled by the Search by name setting under Teams settings), Teams is no longer able to suggest public teams for people to join. This is because the query against the Microsoft Graph to find teams to suggest doesn't take any notice of directory scoping, so Teams disables the functionality for everyone in a tenant when address book policies are in use. In addition, the /Join command, which also lists the teams available for someone to join, is disabled. If you deploy information barrier policies (see the Compliance chapter), scoped directory searches are used with the same effect.

Joining a Team with a Code

To make things easier for owners to manage teams with hundreds of users, Teams supports the ability of users to join a team with a system-generated code. The idea is that it is easier to supply potential members with a code that they can input to join a team than it is for a team owner to manually add them to the membership. Using a code is also a good way for someone to know that they are joining the right team in a situation where many teams with similar names exist in an organization, such as classes in a school. Team codes work for both public and private teams. The process is as follows:

- A team owner goes to the **Team code** section under team **Settings** and clicks the **Generate** button to have Teams generate a unique seven-character code for the team. The code is a value something like "jny9ota."
- The team owner publishes the code to potential team members. For example, if the team is open to anyone in the organization, you could publish the code on a website for all to see. On the other hand, if the potential membership comes from a more limited population, you could email the code using a distribution list.
- When someone receives a team code, they can join the team using the normal **Join team** process and input the code into the **Join a team with a code** box, or by typing the /Join command in the command box. For example, /Join jny9ota.
- Teams checks the supplied code and flags an error if it is invalid. If valid, Teams adds the user to the membership and opens the team.
- Team codes are only valid for tenant members. Guest users cannot use codes to join teams.
- The team owner also can remove a code at any time or reset the code. You can't use a removed or reset code to join a team.

Apart from the way that they join a team, members who join with codes are like any other member.

Joining a Team with a Deeplink

[A deeplink](#) is a hyperlink (URL) used to navigate to some item within Teams. Examples of deeplinks are the URLs generated by Teams when someone fetches a link to a team, channel, tab, or message. For instance, if you go to the ellipsis menu for a message and select **Copy link**, Teams copies a deeplink to the message to the clipboard. You can paste the link into another message or use it to open Teams at the linked message. The same happens if you use **Get link to team**, **Get link to channel**, or **Copy link to tab** to create a link to these elements.

The format of a deeplink varies depending on its purpose. When you link to something in Teams, the link includes several important elements to allow Teams to find the right data. If we look at the link below, three pieces of information are highlighted:

`https://teams.microsoft.com/l/message/19:45ac50d1afa2425a80362e94f381b1e7@thread.skype/1523005757318?tenantId=c662313f-14fc-43a2-9a7a-d2e27f4f3478&groupId=ce23aef8-c551-40d4-bdb6-2bcc1eb64626&parentMessageId=1523005757318&teamName=The%20New%20Hydra%20Project%20Team&channelName=General&createdTime=1523005757318`

These important parts of the deeplink are:

- The reply chain identifier, which identifies the message thread (**1523005757318**). This identifier appears in several places within the link. The identifier is a Unix timestamp (epoch), based on the number of seconds since 1 January 1970. The timestamp is calculated to the millisecond. You can convert the identifier to human readable time with converters such as [the Epoch Converter](#), which reveals that the identifier shown above is Friday, April 6, 2018, at 9:09:17.318AM.

- The tenant identifier, which tells Teams what tenant to access (**c662313f-14fc-43a2-9a7a-d2e27f4f3478**).
- The group identifier, which tells Teams the team that the message belongs to (**ce23aef8-c551-40d4-bdb6-2bcc1eb64626**). The identifier points to the Microsoft 365 group underpinning the team.

The team and channel name are also included in the link.

If you send a deeplink pointing to an item in a team to another person and they are not a member of that team, they can use it to join the team. The link opens a dialog to ask the person if they want to join the team. If the team is public and the user accepts, they become a member of the team. If the team is private, Teams sends a request to join by email to the team owners, who can then accept or deny the request. In addition to receiving email notifications about requests to join their team, owners can go to the Manage team page to view requests waiting to be processed under the **Pending Requests** tab.

Starting a Chat with a Deeplink

Applications usually generate and consume deeplinks. However, anyone can create and use a deeplink if they know the format of the hyperlink needed by Teams. For example, let's assume that you want to allow other people in the tenant to start a personal chat to follow up with you after receiving some email. To automate the process, you can include a deeplink in your email signature. When someone reads an email from you and clicks the deeplink, Teams navigates to personal chat and starts a new chat (if they have never chatted with you before) or continues an existing chat.

The form of deeplink that you need to include in the email signature is:

`https://teams.microsoft.com/l/chat/0/0?users=Kim.Akers@office365itpros.com&topicname=Chat`

Anyone clicking this link will start a chat with Kim Akers. Deeplinks to personal chats only work for people inside the same tenant. They don't work for guest users or external (federated) access to users in another tenant.

Leaving a Team

A user can leave a team at any time by selecting the **Leave the team** option from the ellipsis menu available for the team and any channel in the team. Alternatively, a team owner can remove a member by selecting **Manage team**, moving to the entry for the member, and then clicking the "X" to the far right of the entry.

Guests can also leave teams. However, this action does not remove their account because the guest account might be in active use for other purposes, such as membership of a group, another team, or access to some SharePoint or OneDrive for Business documents. If you want to remove the account, you must do this through the Azure or Microsoft 365 portals, or by running the *Remove-MgUser* cmdlet.

Maintaining Team Membership

Normally, team owners handle membership. If the team is private, the team owners take care of membership by adding and removing users, promoting members to become owners, or demoting owners to become members, which is a necessary first step before you can remove an owner from a team. If the team is public, users can join the team without owner intervention, so owners only need to add or remove guests and decide who are owners. It is also sensible for team owners to check team membership periodically in case someone joins that should not be there.

Tenant administrators and other users assigned with user management permissions can update team membership even if they are not a team owner. A variety of methods is available to do the job:

- **The Teams admin center.** Update the membership of teams.
- **The Entra admin center.** Update the membership of the Microsoft 365 groups used by Teams.

- **The Microsoft 365 admin center.** Apart from tenant administrators, accounts assigned the User Management Administrator role can update the membership of groups, including those enabled for Teams.
- **The Exchange admin center.** Accounts assigned the Exchange administrator or User Management Administrator role can update the membership of Groups through the EAC.
- **PowerShell.** You can run the *Add-TeamUser* or *Add-UnifiedGroupLinks* cmdlets to update team membership. Given the choice, use the *Add-TeamUser* cmdlet because this mimics what happens when you add a user through a Teams client. See the discussion in the PowerShell book explaining how to use PowerShell to manage Teams. For now, this example shows how to add a user to a team:

```
Add-TeamUser -GroupId (Get-UnifiedGroup -Identity "My Microsoft 365 Group").ExternalDirectoryObjectId -User Donald.Vickers@Office365itpros.com
```

Because of the need to synchronize directories, users might experience a short delay before Teams picks up the new membership data and they can access a team.

Unknown Users: If you see an “unknown user” listed in team membership, it refers to someone whose account has been removed from the tenant directory or whose account cannot be resolved against the directory, or a glitch in the local Teams cache. Because the Teams client cannot resolve the member against the directory, they are deemed to be unknown.

Stale Teams

Over time, people usually accumulate membership in multiple teams. They might end up being a member of so many teams that it’s difficult to find a specific team in their list of teams (or “teams gallery”). Teams divides the teams a user belongs to into a section called *Your teams*, meaning the teams the user has opted to highlight because they are important to them, and *Hidden teams*. Teams in the hidden section might be as important to the user because of the information they contain, but the user might not want to access them as regularly. By hiding teams and placing them in the *Hidden teams* list, the user focuses on the teams they work with most often.

To help users manage the set of teams they belong to, Teams periodically checks the set of teams available to each user (but not for guest users) to detect those that might be “stale” and could be moved out of view to allow the user to focus on the teams most important to the user. Microsoft 365 uses several tests to decide whether a team has become stale. The basic test is that the user has not accessed the team in the last 45 days, but there are some qualifiers. For instance, a team with an unread @mention for the user is never regarded as stale, the team the user last moved from the more list is never regarded as stale, and the same is true for any team marked as a favorite in the last 45 days.

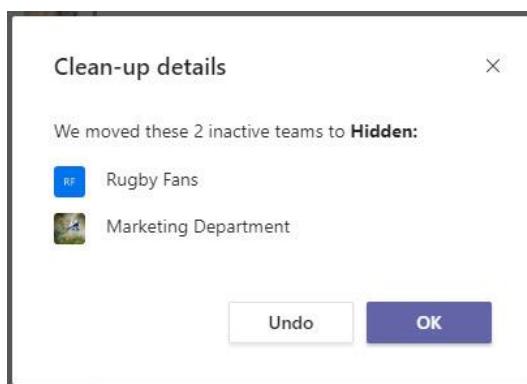


Figure 11-6: Teams lets the user know it has hidden some teams

When Teams decides that some teams are stale, it notifies the user that these teams have been moved to the *Hidden teams* section (Figure 11-6). The user can undo the move if they wish, which moves the team back into their *Your teams* list.

Users always have access to every team they belong to, but they must navigate to the *Hidden teams* section to find hidden teams when they need to access their contents (alternatively, they can go to the Manage teams section and search for the team name). For ease of finding a team in what can be a very large list, Teams organizes the *Hidden teams* section alphabetically, and users cannot move teams up or down within the list. Users can move a team from the hidden list by selecting the team and choosing the Show option from the ellipsis menu. Likewise, they can move a team into the hidden list by selecting the Hide option from the menu.

List All My Teams

To see the set of teams that they belong to, a user invokes the **Your teams** option. The set of teams splits into active and archived teams and lists:

- Team Name. Click on the name to access the General channel for the team.
- Description.
- Membership (Owner or Member).
- People: The number of members of the team.
- Type: Org-wide, Public, or Private.
- Show or hide the team to put it in the *My Teams* (Show) or *Hidden teams* (Hide) lists.
- More options: Manage team, add channel, add members, leave the team, **edit team**, get link to team, **archive team**, or **delete the team**. The bolded options are only available to team owners.

The Analytics option available in this section gives users a view of how active the teams they belong to are. Statistics available for active teams include the number of members, guests, posts, and replies over the last 7, 30, or 90 days.

Arranging the Teams List

After you join a team, you can move the team within the list of teams to which you belong (*Your teams*). Teams does not display the list alphabetically but in the order that you joined the teams. To reorder the list, simply drag and drop a team into the position that you want. In most cases, people place their most important teams at the top. You can also use the **CTRL+Shift+Up** and **CTRL+Shift+Down** key combinations to move a team up or down within the list (on a Mac, use the Command key).

You cannot change the channel order within a team. The General channel is always first, with the other channels following in alphabetical order.

Members and the Manage Team Option

The **Manage team** option displays information about a team and is available to members (including guests) and owners. The ability to take management actions, like changing a team setting or adding a channel, is restricted to team owners, tenant administrators, and teams service administrators. Members can see:

- The **membership** list, including their title, location, and role. Users can add a member here. If the team is private, the membership request must be approved by a team owner.
- The **channels** in the team, including the channel name, description, and date of last activity. The ellipsis menu is available to allow the member to get the email address for the channel (if enabled), get a link to the channel, or follow/unfollow the channel. If team settings allow members to add, remove, or restore channels, they can take those actions here.
- The **apps** that are available to the team. If team settings allow members to add or remove apps, they can do so here.

- **Analytics** for the team are available to give an overview of how active the team is.
- **Tags** defined for use in the team. Some tags are available in all teams, but most are specific to a team.

Teams Messaging

For many organizations, the central focus and purpose of Teams is the ability to connect team members through short, interactive conversations. Or as Microsoft puts it "*communicate in the moment and keep everyone in the know.*" The individual messages that make up conversations are persistent, meaning that they continue to exist unless the author or a team owner decides to remove them. Teams conversations are complete with all the modern ways to brighten discussions (reactions, emoji, and memes). Reactions (like, laugh, angry, and so on) are important signals to chat participants (and recorded in the Microsoft Graph) to show the view someone has about a message in a conversation. If desired, you can disable the ability to add images to conversations through Teams messaging policies managed in the Teams admin center.

Conversations in channels are public because they are available to any member of the team. Those in chats are private to chat participants. You can't change a private conversation to be public or vice versa or move a chat from one channel to another, either within a team or between teams. People control the participants in private chats by adding others to or removing them from chats. The mechanics of contribution are identical for public and private teams, but people indeed tend to be more chatty or informal in personal chats and more formal and perhaps verbose in channel conversations. In either case, participants type their thoughts into the compose box and then post them to the chat or channel. Or just use the thumbs-up reaction to indicate that you've seen and approved of a message without the need to post a more complex response.

Chats are persistent, and people can leave and rejoin the conversation as they wish. Persistent means that conversations are enduring and can be resumed at any time. For performance reasons, Teams caches recent messages in memory. Clients might have to page older messages back from storage before being able to display details of a conversation. Normally, it takes a client just a few seconds to retrieve and show old chats.

If you find that you want to develop a personal chat into a more general discussion, you can either expand the chat up to the participant limit or start a new conversation in an appropriate channel.

Starting Conversations

Channels divide into topics or conversations. Each conversation has a base note to set the context for the conversation followed by a set of replies. In technical terms, a conversation is a set of messages connected by a common thread identifier, which is how Teams knows what messages belong to a conversation. Replies are ordered within a conversation using the message timestamp. To start a new conversation, click **Start a new post** and enter the text for the initial post. It's important to add a subject for the new post to help channel members understand the topic being discussed. Options to pay attention to include:

- **Allow replies:** The default is that all members of the channel can reply, but you can restrict replies to just you and channel moderators. People often do this for announcement posts when organizations want to convey information to team members when the need to debate a matter no longer exists. As explained in the Managing Teams chapter, individual teams can have moderators to restrict who can add topics to channels, but you don't need to enable channel moderation to restrict replies. If specific moderators aren't defined for the channel, team owners serve in their place.
- **Post in multiple channels:** Normally you only want to post a conversation in the channel you're working in, but you can post in up to 49 other channels if you want. Naturally, you can only post in channels that you are a member of. You can't post in channels where posting is restricted to moderators (and you're not a moderator). Teams treats each message separately and, apart from visiting each of the target channels, there's no way to see all the replies for the same message from all the channels where the message is posted. You can include attachments in multi-channel posts. If you

upload a document from your workstation, Teams stores it in the channel folder of the SharePoint document library belonging to the current team and shares it from that folder with the teams for the target channels.

A use case for multi-channel posts: A good example of where it's very useful to post in multiple channels is when a company wants to spread the news of an announcement as widely as possible. Create an announcement post and limit replies to the author and channel moderators to eliminate the need to deal with responses to the individual posts. You still want to encourage communication and responses to the announcement, and a good way to do this is to include a link in the announcement to redirect users to a topic in a channel in an org-wide team where they can post replies.

Editing Posts

If you make a mistake, you can edit a post (message) to correct the error, but only if the Teams messaging policy applied to your account allows you to edit sent messages and the team settings allow members to edit their messages. In most cases, it's reasonable to allow people to edit their messages. All of us make mistakes and there's nothing as annoying as sending a message and then discovering a spelling or grammatical error.

If you post to multiple channels, you can edit the original post and the edited text will appear in all the channels where the original message was posted. However, you won't be able to update the post in channels owned by teams whose settings don't allow members to edit posts. You can also edit a conversation that is only posted in a single channel to add extra channels and make it a multi-channel post. When this happens, the original topic message is posted to the new channels but any existing replies for that topic are not.

The author of a message can recall a multi-channel post from a channel by editing the post to remove that channel. You can even edit a post and remove the channel the message originated from and the message will disappear from that channel. Replies to recalled messages are not removed from channels. If you delete a multi-channel post, Teams removes it from all channels but leaves any replies intact.

Unlike regular posts, Team owners can't edit or delete multi-channel posts.

Finishing Conversations

Starting a conversation is easy (but please make sure you start it with a subject), but finishing is more difficult. Structured conversations about a well-defined topic usually conclude, but how many channel conversations end with a summary? When an important conversation finishes, consider posting an "end of debate" note to let channel members know about the conclusions and what the next steps will be. Another advantage is that people will then be able to see what happened without having to look through all the messages in the thread.

Announcements

Many channel conversations begin with someone asking a question or sharing a piece of information they have learned. Announcements are a more formal kind of post where people highlight something important. Teams supports the announcement post type for this purpose. When you compose a new conversation, you can select the post to be an announcement. To mark announcements in the message stream, they have a large heading with a background composed of a solid color and headline. The title of the announcement can be up to 40 characters long.

Alternatively, you can use Microsoft Designer to create a graphic for an announcement post. Select the Microsoft Designer option when composing the announcement and add some details for Designer to work from. Then either accept or customize one of the ideas generated by Designer. When you customize an image, Teams launches Designer to allow full access to the suite of options available in the app. For instance, you could adjust the typeface or words used in the graphic or select a different background color. Figure 11-7

shows an announcement with a header graphic created by Designer. The feature is available in the U.S. but not yet elsewhere.

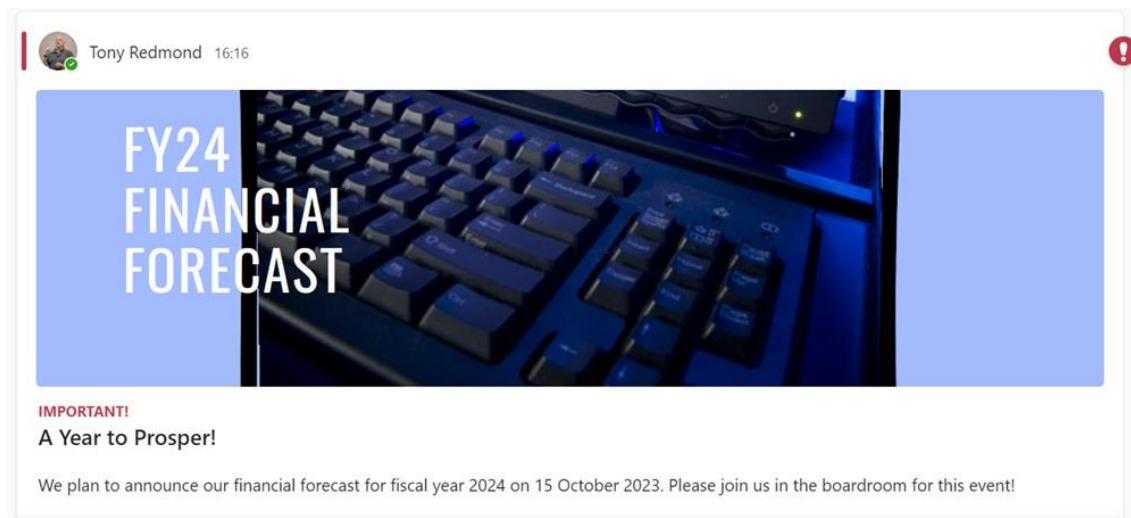


Figure 11-7: An announcement post as seen by readers

The heading attracts the attention of readers, so announcements are a good way to make people aware of important company events or news. Anyone can compose an announcement and if everyone begins to post announcements to a channel, the headings lose their uniqueness. With that in mind, it's a good idea to coach people to post announcements only when they need to highlight something important.

Keeping Conversations Focused

Team conversations tend to be "high velocity," meaning that contributions flow quick and fast. Typical interactions are often brief and use simple formatting, just like text messaging. Like any conversation, people are most productive and achieve the best results when channel members observe some simple guidelines.

A common mistake is to create new conversations instead of replying to an existing conversation. This quickly creates a confusing mass of posts that make it difficult for anyone to understand what happens in a conversation. People sometimes assume that Teams is like email and that it does not matter where they post. This is untrue. Email can preserve the context of a conversation by including the text of earlier replies, meaning that a recipient can see how a conversation unfolds by reading those replies. However, Teams conversations do not include earlier replies, so readers can only see the full context of a discussion if people reply to the conversation and do not split off into new conversations.

Teams Conversation Etiquette

Left to their own devices, it is easy for users to reduce a channel to a confused mass of incoherent conversations. Just like any other communications medium, it is sensible to advise people so that they understand how to extract full advantage from their contribution. Here are some simple rules to help keep Teams conversations civil and focused:

- **Always create a subject for new conversations:** Teams doesn't force users to create a subject for new conversations. However, you should always add a subject to highlight the commencement of a new thread and tell team members what you want to discuss.
- **Leverage existing threads when possible:** The temptation exists for users to start new conversations to express their ideas when existing conversations are better locations for their thoughts. Ask people to check if their contribution should be a reply to an existing thread instead of a new topic as this will help the channel avoid degenerating into many split and duplicated conversations. Using the search feature to check if a team previously discussed something takes only a few seconds. In addition, when

you keep all the posts relating to a topic in a single thread, it maintains the full context of the discussion and makes it easier for people to find the information later.

- **Don't hijack conversations:** Keep conversations to a single topic and resist the temptation to introduce new topics in the middle of a conversation. It doesn't make sense to mix topics in a thread and it makes it harder to search and find information. If a topic is important enough, it deserves a dedicated conversation.
- **Mark important messages.** You can mark a message as being especially important by selecting Important as the Delivery Option. Teams then includes the text "Important!" (highlighted in red bolded and uppercased text) in the message and highlights the message with a red and white exclamation tab as a visual indicator that this is a "must-read" message.
- **Use Announcement posts for important news:** Another way to highlight important messages is to post them as announcements, which allows you to add some attractive graphics and titles to grab the attention of team members. Make sure that the graphic you choose is appropriate to the topic. It's just more professional that way.
- **Don't post private information.** Every channel member has access to all conversations. Never post anything to a channel unless you're happy to share the information with all channel members. If you're unsure, review the membership before posting anything sensitive.
- **Use reactions instead of short replies.** If you receive a question in an email, you might respond with a one-line answer like "OK" or "Go ahead." You can do the same in Teams, but it's usually better to respond with a reaction (for instance, "Like" or "Laugh") to let the author know that you've seen and approved of its contents. Apart from anything else, this also reduces the number of messages in a thread and makes the conversation easier to read. If you don't like the content, the "Sad", "Surprised", or even "Angry" might be a good response. It's sometimes appropriate to react to one of your messages, such as when someone has liked a message to acknowledge what it's saying, and you want to react in turn to show that you've seen their response.
- **Use @mentions and tags intelligently.** Channels can be busy places where it's easy for people to overlook a question to which you want them to respond. Highlight the need for specific individuals to respond by using an @mention or a tag (if a suitable tag is available). And if you expect everyone in a team to respond, use an @Team mention, or even an @channel mention (only those who have the channel visible in their channel lists receive these notifications). Don't use these "reply-all" mentions unless you need to as you don't want to clutter up the activity feed of team members. It's also true that you cannot assume that someone has seen something in a channel conversation unless you @mention them to force the conversation into their activity feed.
- **Be Friendly.** If you @mention someone, Teams automatically inserts their full display name into the text. You can use the backspace key to remove everything but their first name, which seems a little friendlier than something like "Kim Akers (Operations)."
- **Use styles to highlight text.** The in-built styles exist to help users highlight important parts of their conversations. You can add headings, quotations, or code examples.
- **Summarize conversations:** If a conversation comes to a decision, conclude the conversion by writing an end of debate message that summarizes what the decision was and what the next steps will be.
- **Use private chats for personal conversations:** Teams allows people to share their ideas and viewpoints with anyone who can access a team, but sometimes it is best to take a conversation somewhere more private. Personal chats exist for this purpose. Use these chats when small groups need to thrash something out before making a topic public.
- **Don't just say Hello in Chats:** It's polite to let people know why you're contacting them in personal chats. Follow the [guidelines described here](#) and avoid starting a chat with "Hello, Are you there", or something similar. Apart from anything else, starting with a meaningful message gives the recipient some context and allows them to respond with something useful immediately instead of waiting for you to describe what you want in other messages.

Making Your Point

The Teams editor supports highlighting, font size and color, bulleted and numbered lists, bolding, italics, underlining, and a small set of styles. A primitive table formatter is also available to insert and populate tables. You can apply basic formatting to text, such as different headings or marking some text as a quote from a source (you can also use the markdown convention and highlight text as a quote by prefixing it with the ">" character). There is also a code style to include code examples in a code box (click the </> icon) to help programmers share ideas. As shown in Figure 11-8, you can choose the language for a code example (in this case, PowerShell) from a list including C++, CSS, HTML, JSON, Markdown (GitHub), Python, Ruby, and TypeScript.

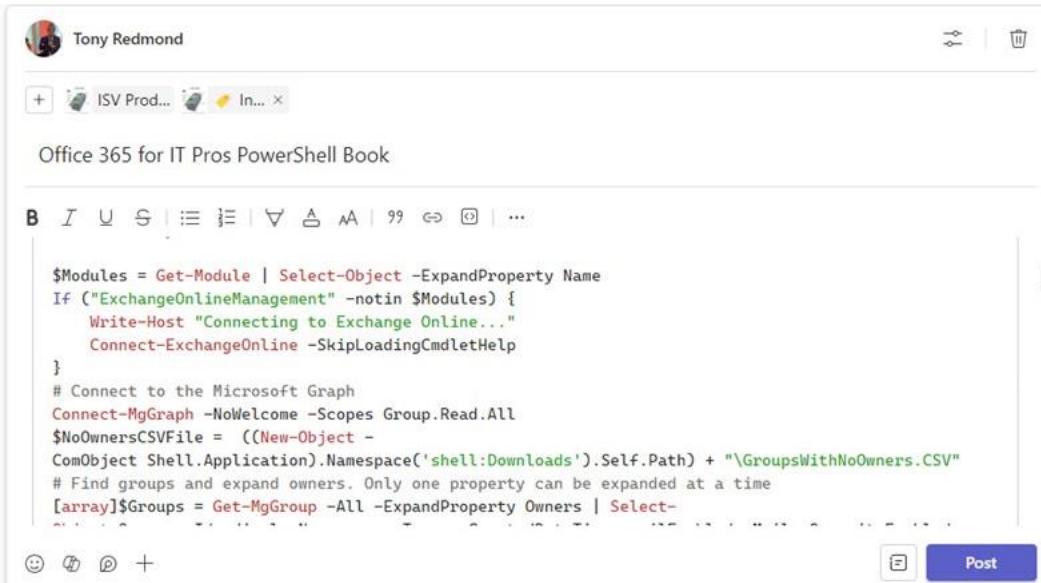


Figure 11-8: Sharing code snippets in a conversation

If you have a Microsoft 365 Copilot license, Copilot can revise or adjust the tone of your message before you post it.

If you make a mistake in a posted message, you can edit the content to fix the error or remove the item if it is no longer valid. Team owners can also exercise editorial control by removing messages from conversations if the need arises, but they cannot edit someone else's message.

The Teams editor does not offer as much control over formatting as a full-featured editor like Word, but if you need to compose something like a complex announcement, you can write it in your preferred editor and copy and paste the text into Teams. If you have a complex document that you want to share and discuss with others, upload it to the channel where you want to discuss the content and link the file in the conversation. Teams stores these documents in SharePoint Online and members can review and discuss the content in the channel.

Quoting Someone

Often you might want to highlight something another person says in a channel conversation. You can use a quoted reply in a chat, but not in channel conversations. To include someone's text in a reply, do the following:

- Select the text you want to quote and copy it (CTRL + C).
- Start a new reply and make sure that you use the full editor (click the Format button).

- Insert a line. Go back to the top of the text and type Shift and > (right arrow) together. Teams creates a highlighted area in the reply. Position the cursor in the area and paste the text you copied (CTRL + V). Teams inserts the copied text into the highlighted area.
- To insert your comment about the quoted text, move the cursor to the unhighlighted area and start typing.

Pasting Text into a Conversation

If you compose text outside Teams and then want to include that text in a conversation, you can paste up to the maximum supported message size of 25 KB of text (roughly 2,000 words in English or approximately 12,000 characters) into a conversation. Including tables and other complex structures affects the amount of text you can paste. The maximum size of a message is approximately 28 KB, but this size includes reactions, @ mentions, and other elements. If the message is too long, Teams generates a preview of the message and tells you to shorten the text before Teams can accept the message. You cannot drag and drop a message from one channel to another or from one team to another. If you make a mistake and post to the wrong channel, you must copy the message and repost it in the correct place.

Spell Checking: Teams has its own spell-checking dictionary, which it downloads to %AppData%\Teams\ dictionaries (you might find several language files there, one for each language you use Teams with). This dictionary is separate from any other used by Office applications, and you can't add new words (like technical terms) to it.

Translating Messages

Teams uses the Microsoft Translator service for inline translation of messages in channel conversations and personal chats. In many cases, the members of a team can communicate quite happily in a common language. For larger teams, such as those used to share ideas across an entire company, being able to express a thought in a person's native language reduces the barrier to collaboration, and that's why Teams supports inline translation for chat and channel messages.

If Teams detects that a message uses a different language to the user's default language, it applies the settings defined in the Translation section of Settings to know how to handle the message. In most cases, it automatically translates the text into the user's chosen language. However, the settings can define languages that the user is willing not to translate. Translation happens online, and when a message is translated, Teams displays a translation options icon to allow the user to access settings or view the message in its original language.

Languages have complex and regional accents, local sayings, idioms, jargon, argots, and technical terms often cause problems in translation. Some glitches might still happen even with simple text, but the translated output is usually good enough to convey the sense of a message. At the time of writing, Microsoft Translator supports [over 100 languages and dialects](#).

Translation can handle large messages, but a limit does exist. Teams supports posts of up to 25 KB. However, the buffer allowed for translations is smaller than this. In practical terms, you can expect to be able to translate messages of up to 1,000 words. The exact number depends on the language and size of the words. If you try to translate a larger post, Teams will tell you that the message is too long to translate.

The ability of a user to translate messages is controlled by the *AllowUserTranslation* setting in the Teams messaging policy assigned to their account. If the setting is \$True (the default), translation is available. To check the translation setting across all policies, connect to Teams with PowerShell and run this command:

```
Get-CsTeamsMessagingPolicy | Format-Table Identity, AllowUserTranslation
```

Identity	AllowUserTranslation
-----	-----

Global	True
Tag:Advanced	True
Tag:Advanced Users	True
Tag:Restricted - No Chat	False

You can also update the allow translation setting in messaging policies through the Teams admin center, where the setting is called *Allow users to translate messages*. Remember that disabling translation in a messaging policy affects all users covered by that policy.

Other Multilingual Features

Teams supports localized translations for the @Team and @Channel mentions. For instance, where English users type @Channel to draw attention to a topic in the channel, French users can type either @Channel or @Canal, while German users can type @Kanal. Teams recognizes the English and local language version of the term.

Normally Teams uses the default language configured on a device to know what language to use for spell check. The Teams desktop client for Windows can detect when users switch languages in chats and channel conversations. If a user sends several messages in a different language than their norm, Teams will switch spell checking to that language and prompt the user to confirm that this is OK. Unlike message translation, no data goes to the server. There's no administrative control over this feature.

The Activity Feed

The Teams Activity Feed is an app accessed through **Activity** in the top left-hand corner of the desktop and browser client. The role of the app is to highlight important items for the attention of a user. As people respond to chats and channel conversations with replies and reactions, notifications appear in the activity feed. Notifications for messages posted by bots or workflows, including email sent to channels, do not show up in the activity feed. Apps can use the [notifications API for the activity feed](#) to post notifications. For example, the Viva Insights app posts reminders to notify users to begin their virtual commute or note their current state of feeling.

The default view in the activity feed reveals all notifications related to the user. For example, someone uses an @mention to ask you a question or to bring something to your attention, or it's time to renew a team that you own. Along with a text snippet for each notification, Teams uses different icons as visual clues of why the event appears in the feed. The clues include @mentions, channel mentions, team mentions, replies, and reactions. The number in the red circle beside the Activity Feed "bell" shows the number of @mentions and replies waiting for attention. These notifications age out after 30 days.

If you are a member of some busy teams, your activity feed is also likely busy. To help find notifications, Teams supports two filters:

- **Unread:** Show unread messages only.
- **@Mentions:** Shows personal @mentions in chats and channel conversations. If someone responds to one of your messages or mentions you in a conversation, Teams generates a notification in your activity feed. However, if its author or a team owner later removes a message, you might see an entry in the activity feed that doesn't point to anything. This doesn't happen very often, but it can.

The filter option above the two buttons supports filtering of activity notifications to a more manageable set.

Refining the Activity Feed

After you've worked with Teams for a little while, you'll probably have a lot of items showing up in the activity feed. In email terms, an overloaded activity feed is like an overloaded inbox – it's hard to know where to start

processing items, especially if you've been away from Teams for a while. One strategy often used to impose order on an activity feed is:

- Be very careful about what channels you follow. Unfollow channels that host discussions of lower importance and try to keep the channels you follow to the bare minimum. This will reduce the number of notifications you see.
- Process direct questions first. If someone uses an @mention to refer to you, it means that they want to bring something to your attention, so you should scan these entries and decide which ones need attention.
- Check replies to conversations you participate in next. You've joined these conversations, so you probably want to find out how they end.
- After you've cleared items from important channels, questions, and replies, you can leave other channel conversations until you have time.

The notifications section of the Teams settings app allows users to control notifications for personal and team @mentions, replies, and likes and reactions. A user can turn these settings off to reduce the volume of notifications posted to the activity feed. They can also use the [...] menu for a notification for a reaction (thumbs-up, heart, etc.) or generated by an app to turn these types of notifications off. Notifications for an app are dealt with separately. In other words, if you want to disable notifications generated by ten different apps, you must find a notification from each app and use the menu option to instruct Teams to turn the notifications off for that app.

The Importance of @Mentions

To make sure that an item shows up in a user's activity feed, you can address them with an @mention. Four options are available.

- **Direct @mention:** To bring something to the attention of a specific team member, input the @ sign followed by the name of the team member in a personal or group chat or channel conversation. For example, **@Kim Akers**. You can include a list of people, each prefixed by @. Teams checks mentions against a cached set of member and channel names (for channel conversations) and people you communicate with often (for personal chats). If you're in a channel conversation, you can't mention someone who doesn't belong to the team. If in a personal or group chat, you can't mention someone who isn't participating in the chat. Teams is intelligent enough to detect the names of team members as you type text into messages. If Teams finds a match against one or more members is detected, it displays a list of suggested names for you to select and add as a mention in the text.
- Teams also supports **@-less mentions**, which means that you don't need to prefix a name with the @ character. Instead, the client scans text as you write messages to check text against its cache. The initial letter of the member's first name (as in *Kim* for *Kim Akers*) must be capitalized otherwise Teams treats it as just another word. If it detects a match against the membership list, Teams displays a list of matching names. You can then select a name to make it into a mention.
- **@Channel mention:** Instead of the member's name, input the name of the channel. For example, @Budgets. Use a channel mention when you want to highlight something to the team members who include the channel in their channel list. You can also use @Channel (or its local language equivalent, like @Canale in Italian) and Teams will insert the channel name. Teams supports channel mentions for shared channels but not for private channels.
- **@Team mention:** Use the team name. For example, @Engineering. Use a team mention when you want to bring something to the attention of everyone in the team. You can also use @Team (or its local language equivalent) and Teams will insert the name of the team. Team and channel mentions are blocked in teams with over 10,000 members.

- **@Everyone mention:** This type of mention is available in group and meeting chats. An Everyone mention is a way to highlight a message by notifying it to everyone in the chat. It's akin to using the @Team mention in a channel conversation. If more than 50 participants are in a chat, Teams warns users when using the @Everyone mention due to the volume of notifications it generates.

Note that team and channel mentions are unsupported for teams with more than 10,000 members. You can also use the tags defined in a team to refer to subsets of team members. See the section below.

Team owners can control whether members can use channel and team @mentions through team settings. By default, team settings allow users to use mentions in conversations.

Toast Replies: When someone sends you a message or replies to you in a personal or group chat (or meeting), Teams sends a "toast" notification to tell you what's happening. You can then respond to that user by entering your reply in the toast, but only with the Windows and Mac clients. This is a great way to send a quick response, but the reply cannot exceed 1,000 characters and can only include text.

When someone involves you in a conversation with a mention, a notification appears in your activity feed. You can click the notification to go to the conversation and pick up the thread. Figure 11-9 shows how Teams uses different icons to highlight conversation threads, including a team mention, personal mention, and an item marked as important.

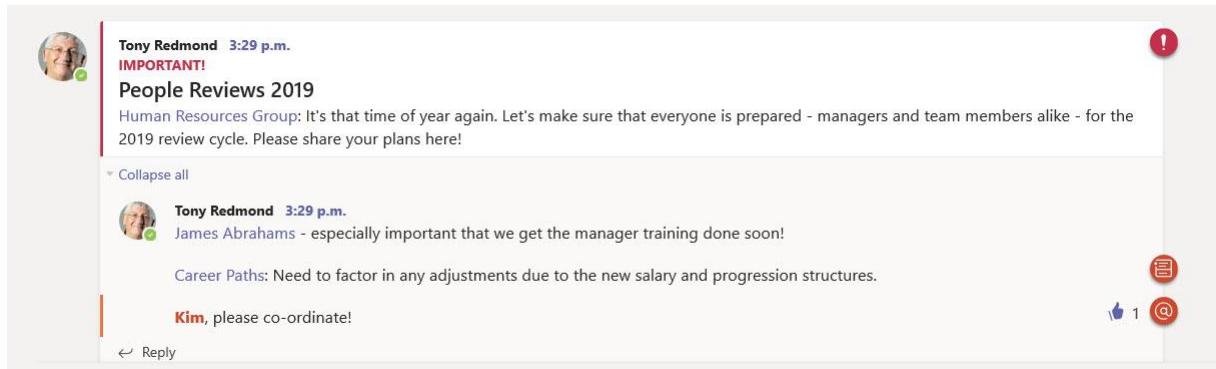


Figure 11-9: Visual indicators in conversations

Unlike most email systems, there is no equivalent of an "all users" distribution list that people can use to notify every account in the organization. If company-wide announcements are important to you, the closest equivalent is to create a team that has everyone as a member and use that team for general announcements. If you use dynamic groups, this is an easy way to keep the membership updated and ensure that new people automatically join the team when an administrator creates their account.

Emojis

Teams has access to over 800 different emojis and reactions to help users express their view about topics and discussions. A tenant can enable or disable the feature through the Teams admin center. If enabled, tenant users can create up to 5,000 custom emojis. Before they can create a custom emoji, users must be assigned a Teams messaging policy allowing them to create custom emojis (the *CreateCustomEmojis* setting is true). Other users can be allowed to delete custom emojis if the *DeleteCustomEmojis* setting in the messaging policy is true. Global and Teams administrators can always remove custom emojis.

Custom emojis can be created from PNG and GIF files. After uploading a file, the user creating the emoji must give it a suitable name (all lowercase letters). Files uploaded to create emojis are not checked for compliance with corporate standards or good taste. That oversight is for team owners and administrators to perform.

Share Someone's Contact Info

The Share someone's contact info option in the @mentions menu allows participants of 1:1 and group chats to share the contact details of one or more Teams-enabled member accounts in the tenant. Contact details for guest members cannot be shared. Teams does not notify people when their contact information is shared in chats. When someone clicks on the contact entry inserted into the chat message, it reveals the user's profile card. You can't share someone's contact info in channel conversations.

Tags and Tagging

@Mentions allow users to address messages to an individual member, a channel, or the complete team. Team and channel mentions aren't very precise because they flag a message to everyone in a team or channel.

Heavy use of these mentions can clutter the activity feed for people who don't need to know about something. Tags fill the gap between individual mentions and channel/team mentions by giving people a way to address a subset of members in a team. A tag has a descriptive name like "Managers" or "Individual Contributors" that team owners can assign to members to allow Teams to know who should receive notifications when someone uses the tag to address a message. Tags are different from hashtags because tags refer to a collection of team members while hashtags refer to a topic, place, or thing.

When you access a team, Teams builds a list of the team members and channel names in memory to allow personal and channel @ mentions. Tags are added to the roster of team members, which means that you can address the members of a tag by prefixing the tag name with an @. Because dynamic teams have non-fixed membership, you can't use tags with these teams.

Tag Management

Tag management is in the Teams admin center in the Tagging section of Teams settings. There you can choose to allow the following users to manage tags:

- Team owners.
- Team owners and members.
- Team owners, members, and guests.
- Microsoft default (whatever option Microsoft determines – currently, this is team owners and members).
- Not enabled (tagging is unavailable).

Team owners can override the organization settings. For instance, the organization might allow members to create tags, but some team owners might not want this to happen in their teams. Control for who can manage tags for a team is through the **Manage team** option (select Settings, then Tags).

Other points to remember about tags include:

- Tags are specific to a team and not shared between teams. Teams used to have a facility called suggested tags which could be used in all teams. Microsoft deprecated the feature in February 2024.
- A team can define up to 200 tags and each tag can be assigned to a maximum of 200 members.
- The name of a tag can be up to 40 characters (including emojis) and a description of up to 200 characters.
- An individual team member can have up to 25 tags.
- You cannot use tags in messages posted to multiple channels or in personal or group chats.
- Tags can be used to address members in any type of channel. Because channels can have different memberships, those addressed by a tag in one channel might not be the same set of members addressed by a tag (of the same name) in a channel of a different type.
- You can use tags to create new chats.

- You can't use tags as a search filter.

By default, Teams enables Tags to allow team owners to create and assign tags using the **Manage tags** option in the [...] menu (Figure 11-10). Click on a tag to edit the people with the tag (you can also launch a chat with the tagged people from here).

Name	Members	Description	Imported from	...
Administrator	1	The boss		
Editors	2	Wordsmiths extraordi...		
Writers	8	People who generate ...		Create a copy Delete

Name	Members	Description	Imported from	...
Guests	7	Contributors with gue...		
Technical Editor	2	The best of the best		

Name	Members	Description	Deletion date	...
Guest Contribu...	5	Contributors with gue...	18/01/2024	Restore
Managers	1		18/01/2024	Restore

Figure 11-10: A set of tags defined for a team

Another way to manage tags is through the **Manage team** option. You can view the list of team owners and members and see their assigned tags. You can then assign tags to people and see the set assigned to each tag. If a suitable tag doesn't exist, you can create a new tag and assign it to appropriate members.

Apart from the settings to control tags in the Teams admin center, there's no other management interface to deploy tags or have any insight into how team members use tags. The Microsoft Graph supports APIs to list the set of tags in a team and return the members of a tag. See [this article](#) for an example of how to create a report using these APIs about tag usage in a tenant.

Automatic group: Teams generates an automatic group (tag) for team owners to allow people to address team owners in channel conversations using `@Team Owners`. You don't need to do anything to maintain this tag and it is available for use in standard channels.

Praising Others

The Praise app allows users to highlight the work of co-workers with a message composed of a badge and some celebratory text. People can praise others in personal chats or channel conversations or using the Viva Insights app. Both tenant and guest users can give and receive praise. The flow of the application is simple:

- Select the Praise app for a new message or reply.
- If using Viva Insights, choose to post the praise in a chat or channel conversation.

- Select the badge from a set provided by Teams. Each badge expresses a tribute to give to a recipient like "Thank You" or "Problem Solver."
- Select the recipients. For personal chats, the recipients must be members of the chat. For channel conversations, the recipients must be members of the team hosting the channel.
- Add some words to show why you're praising the recipients.
- Review and send the message when you're happy with the content.

Teams treats praise messages as a graphical form of an @mention, so the message shows up in the activity feed of the recipients.

Searching Teams Content

Teams uses Microsoft Search to help users find messages, people, and files. To run a search, type something into the Search box and press return. Because this form of search looks through all the content in chats and channels available to the user, many matches likely result, divided into messages, people, and files. If you do not see what you are looking for, click the Filter icon to reduce the set of results to a more manageable number. Filtering supports preset date ranges like "Last month" or "Yesterday" and can restrict search to a specific team or channel or look for items with attachments. If you look for Files, you can restrict the search to a certain file type (for instance, PowerPoint).

When searching Files, as you enter characters into the search box, Microsoft Search scans for the most relevant hits based on multiple criteria such as the files you recently worked on or shared. These files are suggested as soon as Search finds them. Often, one of the suggested files is the file you're looking for and there's no need to progress to a full-scale search.

Refining Search Queries

Applying filters to search results can help you to find the right information, but it's even better to use precise search queries to find information, which isn't always the case. Most people mimic what they do with Google or another general-purpose search engine and search based on a word or phrase. Teams search is keyword-based and supports some (but not all) of the [KeyQL \(search\) syntax](#) for Exchange (email) items and used by Office 365 content searches. This means that precise queries can be constructed. For example, by adding a date range.

Let's start with a query to look for chats and channel conversations containing the phrase "Office 365 book" posted in the current month (the uppercased words in these examples are search operators):

"Office 365 book" AND Sent = "this month"

We could also use a specific date range:

"Office 365 book" AND Sent >= "1 June 2020" AND Sent <= "15 June 2020"

And limit the search further by including the name of the user who posted the message:

"Office 365 book" AND Sent >= "1 June 2020" AND Sent <= "15 June 2020" AND From:"Tony Redmond"

We could even refine the original search keywords ("Office 365 book") to say that two further phrases must be within ten words of each other:

"Office 365 book" AND "book" NEAR(10) "planet" AND Sent >= "1 June 2020" AND Sent <= "15 June 2020" AND From:"Tony Redmond"

Precise search queries work with the Teams mobile client too.

Contextual Searches

Teams refers to searches confined to a single chat or channel as "contextual." The CTRL + F (Command + F for macOS) command tells Teams to launch a contextual search within the currently selected chat or channel. The query entered in the command box is used for the search, including precise queries as described above, so the number of items returned by a search is likely much fewer than with a more general search.

Using a contextual search effectively applies a filter, and you can't apply other filters on the results of a contextual search as are available for normal searches (which is a good reason to use precise searches). Also, CTRL + F only searches messages in channels and chats, so the **People** and **Files** results returned by normal searches aren't available.

Search Suggestions

When a user inputs a term into the command box, Teams looks for the presence of a "/" to see if the user wants to execute a command. If none is found, Teams uses the term to generate suggestions matching the search term and displays them in a drop-down list known as the "suggestions well." The suggestions are organized into Top Hits (which include teams and documents stored in OneDrive for Business or SharePoint Online), People, Group chats, teams, and files. Selecting an item either brings the user to the location (chat or channel) or opens a file. Alternatively, the user can view full search results generated using the search term by pressing enter.

Copy Links

The Copy link option is available for channel conversations, individual messages within channel conversations, and chats. The option copies a deeplink for the target message to the clipboard. Users can include the deeplink in messages to direct others to a specific place in a channel or chat.

Removing Messages

Some organizations hate the idea of anyone being able to remove anything they posted electronically (to email, SharePoint, or Teams) and some think this is sensible. After all, you can always have second thoughts and want to remove something written in error. Teams controls the ability of users and team owners to remove messages from conversations at a tenant level and within individual teams.

The **Messaging Policies** section of the Teams admin center includes the tenant-wide controls for message deletion.

- **Allow owners to delete all messages** controls whether team owners can remove messages in any channel in the teams they own.
- **Allow users to delete their messages** controls whether people (including guests) can delete messages that they post.

The intention behind owner control is to allow them to police conversations within a team and be able to remove anything posted that is inappropriate, insulting, or otherwise objectionable. Within a specific team, an owner can select **Manage Team** from the ellipsis menu, and then **Settings** to access the settings for that team. Navigate to **Member Permissions** to select whether:

- Everyone can edit their messages.
- Everyone can delete their messages.
- Owners can delete all messages.

The settings apply to all channels within the team. If the tenant-wide settings do not allow users to remove or edit messages, Teams hides these settings at the team level.

If allowed by the team settings, message authors can delete their messages from channel conversations. Team owners might also be allowed to delete messages sent by any team member. In either case, Teams records a deletion by hiding the message and replacing it with "*This message has been deleted.*" Only the selected message is hidden. Teams leaves messages before or after the deleted item intact in the conversation. Teams doesn't support the removal of a complete thread (all the messages that compose a conversation).

The message author can restore deleted messages and reveal them in the conversation by using the *Undo* option (*Undo* isn't available to team owners). Hidden messages remain in place indefinitely. Retention policies are the only way to remove messages permanently. As explained in the Compliance chapter, Teams retention policies remove messages older than a specified age from the Teams message store. The deletion of messages by a retention policy cannot be reversed.

Teams does not remove the compliance records for deleted messages. These items persist as evidence that the contributions to the conversation occurred and can be found by eDiscovery searches. You can't search for hidden messages using the phrase "*This message has been deleted*" because this is a system message that is not indexed.

Attachments pose another issue. When someone includes an attachment in a message, Teams uploads the file to that user's personal OneDrive for Business site (for personal chats) or the channel folder in the SharePoint document library belonging to the team. If the team owner or author later removes a message that has an attachment, Teams removes the message but leaves the attachment intact. The logic of leaving the file in place is understandable, but it might be the case that the attachment holds the objectionable content that you want to eliminate. If so, checking and cleaning up SharePoint and OneDrive content become extra steps in the removal process.

Searching for and removing content from multiple teams is another issue. This might happen if someone posts something inappropriate to one or more teams or people copy content posted to one team into others. To purge the content, you then must find and remove each post individually. Unlike the purge action for content searches, Teams does not have a method to scan all teams in a tenant to find and remove specific content.

When Members Leave

Team conversations are persistent, so they exist even when people involved in conversations leave the organization. The contributions of removed users to private chats and channel conversations remain in place. The user no longer exists in the membership list (or the tenant directory), which means that other members can no longer @mention the user. Because their account is no longer in the tenant directory, the removed user shows up as an "unknown user" as a participant in private chats. However, Teams keeps their display name for their contributions in the conversation history.

If you restore a user account within 30 days of deletion, they regain their membership in groups and teams and can function as they did before the deletion of their account.

Personal (1:1) and Group Chats

To this point, we have focused on using team channels as the basis for conversations. Channel conversations are under the control of the organization because channels only exist inside teams. By comparison, chats occur when two or more people converse on an ad-hoc or persistent basis. Chats are under the control of the participants, who decide when to start the conversation and who should take part. You cannot "promote" a personal chat to move the conversation to a channel in a team.

Chats can happen between tenant accounts, tenant account and guest accounts, or between a tenant account and a Teams user in another tenant. Guest users can also create new personal chats and include other users

and guests in the conversation. In fact, a guest can create a chat that only guest users join. However, guests can only communicate with the members of the teams they belong to. A guest can't chat with a tenant user who doesn't share membership of a team with the guest.

Like channel conversations, personal chats are persistent and are always available. The content of personal chats is always confidential to the participants. In other words, no one outside the chat can see what's happening unless they join the chat. Even then, a newly added participant can be restricted to just seeing chats after they join.

Personal chats are either one-to-one (1:1), meaning that two people take part, or group chats, meaning that between three and 250 people participate, including federated and guest participants. Both kinds of chats are accessed through the **Chat** section of the Teams client, which lists the set of active conversations for the last month. This doesn't mean that Teams erases or drops old chats. They're merely hidden and ready for display if you restart a conversation.

Although you cannot arrange unpinned chats into a preferred order, you can if you use the Pin option. Up to 15 conversations can be in the pinned chat list, which can be arranged into whatever order you choose.

Within a chat, any participant can choose to pin an individual message to appear at the top of the chat. This is a useful way to highlight important information about a chat such as its purpose. On the downside, any chat participant can unpin the pinned message. Because no one in a chat has more rights over chat contents than other participants, there's no way to lock a pinned message. Table 11-3 lists the most important differences between channel conversations and personal chats.

	Channel Conversations	Chats
<i>Participants</i>	Open to anyone in the team owning the channel. Shared and private channel conversations are open to channel members.	Open to those invited to join the chat, from 1:1 or group chats with 3 to 250 participants. Users can start chats by addressing tags, distribution lists, Microsoft 365 groups, or mail-enabled security groups. Teams also supports Chat with Self, a feature to all users make notes to follow up.
<i>Purpose</i>	Discussion of ideas, concepts, and announcements.	More detailed discussion (often preliminary) about topics that might later be shared in channels.
<i>Structure</i>	Each conversation is a separate thread.	Each chat is a single conversation thread.
<i>Notifications</i>	Based on @mentions and channel favorites.	Messages in a chat generate pop-up notifications for the participants.
<i>History</i>	Full history of channel conversations available to all team members.	Previous conversations can be shared with new members, but don't have to be.
<i>Sharing</i>	Files shared in the team's SharePoint site.	Files shared in sharer's OneDrive for Business account or by uploading to the sharer's account.
<i>Calendar</i>	Scheduled and "Meet now" ad-hoc meetings.	On-demand audio and video calls (with screen sharing). Can schedule meetings with chat participants.
<i>Pinning</i>	Pinned channels appear at the top of the channel list. Team members can pin individual messages which appear in the channel information pane.	Users can pin up to 15 chats to appear at the top of their chat list. Anyone in a chat can pin a message to appear at the top of the chat. Anyone can unpin the pinned message.
<i>Apps</i>	Channels can deploy apps in tabs and menus and as bots.	Chats can include apps from the Teams app store and add tabs to invoke other apps.
<i>Search</i>	Use Teams search to find messages in channel conversations.	Use Teams search to find messages in chats or use the Filter function to find specific

		conversations. A specific filter is available to find chats from meetings.
<i>Read Receipts</i>	Unsupported.	Available for 1:1 chats and group chats with up to 20 participants.
<i>Quoted Replies</i>	Unavailable unless the user cuts and pastes a reply into a new response.	Supported through the reply option in the [...] menu. Teams inserts approximately 200 characters from the chosen message into the reply.
<i>Smart Replies</i>	Not available.	Supported for 1:1 chats with other tenant members.
<i>Loop components</i>	Supported for tenant users.	Supported for chats with tenant users.
<i>Scheduled send</i>	Unsupported.	Supported for chats with tenant and external users.
<i>Video Messages</i>	Can be posted to channels from the iOS client.	Up to 1-minute-long video clips supported in 1:1, group, and meeting chats
<i>Forwarding messages</i>	Available for chats and channel conversations in the mobile clients.	Available for chats in the desktop and browser clients.
<i>Share contact info</i>	Unsupported	Supported for 1:1 and group chats.

Table 11-3: Differences between channel and personal conversations

Tenant participants can record a 1:1 meeting if both use Teams clients and the Teams calling policy assigned to the account of the person who wishes to start the recording permits this action. Recordings don't work when calls involve PSTN lines or federated connections to Skype consumer users. After a recorded chat finishes, the recording is available in the meeting chat.

Limitations of Large Chats: Although Teams supports large group chats, to save system resources, some limitations apply to group chats of more than 20 participants:

- Outlook out-of-office replies and Teams status messages are not displayed for participants.
- The indicator showing that someone is typing a message is disabled.
- Video and audio calls can't be started in the chat.
- Sharing of documents (using OneDrive for Business) isn't allowed.
- Read receipts for messages don't work.

Teams disables these features to reduce the strain on the service. Fetching out-of-office information for many participants requires a lot of interaction with Exchange Online mailboxes while tracking who's read a message for the same number consumes many processing cycles.

Starting Chats

To start a new chat, select the **Chat** app, and then use CTRL + N (Windows) or click the New Chat icon in the menu bar. You can then add participants to the chat by typing their names in the To: line. You can add the following as chat participants:

- User accounts (member and guests).
- Tags defined for addressing subsets of team members in regular channel conversations.
- People in other tenants by entering their User Principal Names (as explained below, these people can only participate in federated 1:1 chats).
- The name of an existing group. In this context, "group" means the name of an existing group chat, a Microsoft 365 group, an Exchange Online distribution list, or a mail-enabled security group. When you use a distribution list to start a group chat, Teams expands the membership of the distribution list (including nested distribution lists) to find members that it can add to the chat (user and guest).

accounts). This is a one-time operation. If new people join the distribution list, they don't also join the chat.

If you want to chat with a team, do so by creating a conversation within a suitable channel in that team.

If you start a new chat with a set of people with whom you have already chatted, Teams recognizes that a chat with those people exists and displays the messages from the earlier discussion to allow you to continue from that point.

You can also start a chat or continue a conversation with someone by typing @ and their name in the command box, followed by the message you want to send. This approach works well when you want to send a quick note without switching context away from something else, like a meeting or a channel conversation. You can't address more than one person through the command box. Finally, you can add a new participant to an existing chat by @mentioning their name.

Read Receipts

Read receipts are a well-known concept in email. When someone reads a message marked with a read receipt, the email service creates a notification for the original sender to tell them that the recipient has read the message. Teams uses a different concept. In personal chats and group chats involving up to 20 participants, Teams tracks who has seen a message and marks its status with a small icon to the right of the message. The icon is either a checkmark (the message is *Sent*) or an eye (the message is *Seen*).

Read receipts only work if they are enabled for all participants in a chat. Read receipts can be blocked by the messaging policy assigned to user accounts. If enabled by policy, users can turn off read receipts through the Privacy settings for their account. Read receipts don't work for federated chats and they are not supported in channel conversations.

Tabs in a Personal Chat

In the desktop and browser clients, personal chats have two default tabs:

- **Chat:** shows the messages in the conversation.
- **Shared:** access to files and links shared with chat participants. As explained below, shared files are in the OneDrive for Business accounts of the people who share them. Federated participants don't see the Files tab.

Group chats do not display the activity tab, nor is the activity tab available for federated chats.

The idea of the activity tab is that it gives you an insight into what the person you're chatting with has been doing recently in teams where you share common membership. The lookback period is approximately two weeks. If you see something interesting in the list of messages, you can click it to go to the channel to see the full conversation. There's no risk that you'll see something you shouldn't because the messages that show up here are from teams that you both belong to.

Any tenant user in a chat can add a tab. For instance, you might decide that you want to discuss a website or a PDF file on a website with the other participants in a chat. To add a tab, click the plus sign in the menu bar to add tabs for:

- Documents that you have shared in the conversation (Word, Excel, PDF, PowerPoint).
- Link to videos stored in Stream.
- Link to a website page.
- Link to Power BI report (such as usage analytics for the tenant).
- Apps authorized by the tenant.

The intention behind adding tabs to a conversation is to give fast access to information being discussed or needed for the conversation. Participants can quickly move from the conversation to a tab and back again without pause. Teams opens objects as soon as the tab is accessed to make it even easier to access the content.

Sharing Files in Chats

Sharing a file to a personal or group chat is like posting to a channel. If you include a file in a chat that's stored on your workstation, Teams uploads the file to a folder called *Microsoft Teams Chat Files* in your personal OneDrive for Business account and shares the file with the other users in the conversation. On the other hand, if you share a file that's already in OneDrive for Business, the file is left where it is, and its access is amended to include chat participants.

Because OneDrive for Business is used to hold files shared in chats, it follows that the tenant sharing controls for OneDrive for Business apply, such as the default sharing link type and access. To avoid oversharing, it's a good idea to set the default OneDrive for Business sharing scope to people within a chat and to make the access type view-only. This is done by running the *Set-SPOTenant* cmdlet from the SharePoint Online management module:

```
Set-SPOTenant -OneDriveDefaultShareLinkScope SpecificPeople -OneDriveDefaultShareLinkRole View
```

If you make a mistake and share the wrong file or share a file with the wrong set of people, you must remove the access permissions from the file in OneDrive for Business as Teams does not support removing a file from a conversation. If Teams detects that the permissions on a shared file do not allow chat participants to access the file, the sharer is asked to adjust the sharing link for the file to include them.

Retrospective sharing isn't currently supported, so if someone joins the conversation after you share a file, they will be able to see that a file was shared with the chat (in the chat history or in its Files view), but you must share the file with the newly-added participant before they can access its content.

Group Chats

A personal chat expands to become a group chat once a third participant joins the chat. Anyone taking part in a group chat can add someone else to the conversation by clicking the **Add people** icon in the top right-hand corner, which you might do to include an expert to answer a question that has come up in the conversation. Chat participants can also add someone else to a chat by @ mentioning them in the conversation.

One-to-one chats use the name of the person with whom you chat. The same is true for group chats, except that the chat ends up named something like "Ben, Hans, Sean, Lotte+6," which isn't very informative. When you start a group chat, you should give it a name (Figure 11-11) to let people know the topic covered in the chat. You can also edit a chat name after the conversation starts. It is always good to assign a name to group chats as it makes it easier to find the right chat in the list the next time you want to share a thought. If necessary, anyone taking part in a chat can rename it at any time to reflect the current scope and focus of the conversation. Group chats have pictures that Teams generates from the photos of chat participants. You can change the chat photo if you want by clicking on the chat photo and selecting one of the available icons or emojis. Alternatively, you can upload a JPEG or PNG file of up to 4 MB to use for the group chat picture.

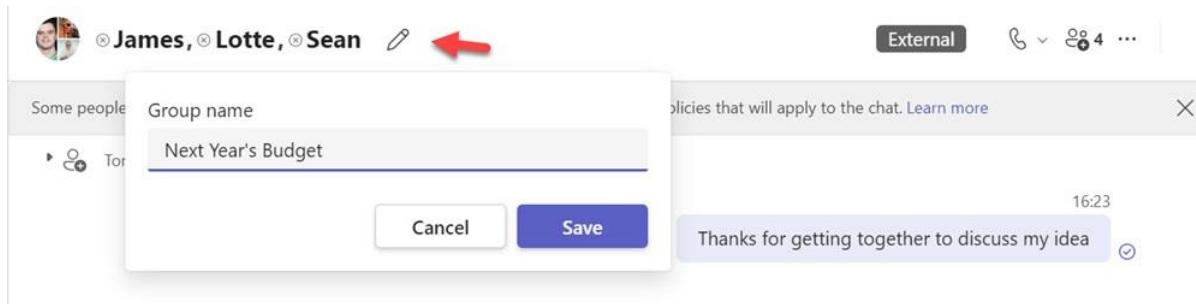


Figure 11-11: Giving a name to a new group chat

You cannot add a guest to a chat unless their account exists in the tenant directory, meaning that they must have previously joined a team. When you add someone to a group chat, you decide whether they can see all or some of the prior message history. For instance, if you bring someone into a conversation to answer a specific question, you might allow them to see messages from the last five days so that they understand the context. Users of the consumer version (aka, "unmanaged users") can add people from Microsoft 365 tenants to a group chat. When this happens, the Microsoft 365 user gets the chance to decline joining the chat.

Personal chats behave differently from group chats in that you cannot reveal previous messages with someone you add to a 1:1 chat. The reason is simple. Whatever's discussed in a 1:1 chat is available only to the other person in the conversation. Chats are persistent and so if you could reveal prior messages to someone joining a conversation, you might impinge on the other person's privacy by revealing something that they prefer to keep confidential. A viable argument exists that people should control their data and decide how to share conversations, but in this case, Microsoft decided that it was best to limit the sharing of prior messages in a conversation to group chats. When a 1:1 chat evolves to become a group chat, Teams creates a new chat and those participating in the chat then have full access to anything discussed thereafter.

Leaving, Deleting, and Muting Chats

If you make a mistake and discover that the wrong set of people are in a group chat, any of the tenant accounts participating in the chat can remove the person who should not be in the conversation. A setting in the Teams messaging policy controls the option to remove users from group chats, so it is possible that some participants can remove people while others cannot. Guest accounts cannot remove other participants from group chats.

To remove someone from a group chat, click on the list of participants, find the person you want to remove, and click the X beside their name. Someone removed from a group chat can see the messages sent in the chat up to the point they are removed but once removed, they cannot send or receive any further messages. If you remove someone in error, you can add them back to the chat and they can pick up from where they left off. Remember to allow them to see the full chat history to ensure that they don't miss anything that happened during their removal from the chat.

If you don't want people to be able to remove other participants from group chats, change the **Allow a user to remove users from a group chat** setting to *Off* in the Teams messaging policy assigned to the user accounts you want to restrict.

Participants who do not want to be in a chat can leave it at any time by selecting it from the list of personal chats and then **Leave** from the right-click menu (you can't leave a chat when only two people are in the chat). When you leave a chat, you no longer see new messages posted to the chat, but you can still see any message posted up to the time you left. Alternatively, if you simply want to remove a chat from the list of active chats, you can **Mute** the chat (another choice in the right-click menu). The chat is still there, and you can take it up again at any time, but notifications for new content in the chat do not show up in your activity feed.

The **Delete** chat option is available for 1:1, group, and meeting chats. When you delete a chat, Teams removes the chat from the chat list and removes your access to the messages in the chat thread. In effect, it's like you never participated in the chat and it's a good way to clean up old and obsolete chats and unclutter your chat list. Removal only affects your access to the messages in the thread. It does not affect the ability of other chat participants to see the messages or access anything shared in the thread, such as a file or loop component. These items remain accessible to you and the other chat participants unless the owner of an item updates its sharing list.

You can rejoin a group chat after deleting it if one of the remaining participants add you back. For personal chats, if the other person sends a message, Teams creates a new chat and adds you to it. In all cases, you cannot see messages sent before you join the chat. There's no way to restore access to these messages either.

Chat with Self

Chat with Self means that a user starts a chat by entering their own name as the chat participant. It is a similar capability to the functionality found in other messaging platforms that allow people to send themselves messages as a form of aide memoire.

There have always been situations where someone ended up as the only person in a chat, such as when everyone else left a group chat either voluntarily or following the deletion of their account, but Teams did not allow users to start a chat with only themselves until June 2022. Unlike the other instances that created a single-person chat, each user can only have one Chat with Self thread. They cannot transform the chat into a regular chat by adding other participants.

If someone needs to share information in their chat with self, they can create a Loop component in the chat and make it available by sharing the link to the loop file in OneDrive for Business to allow others to open and interact with the component.

External Access: Federated Chat Outside the Tenant

External Access or federated chat is the ability to have 1:1 chats with Teams users in other tenants, Skype consumer users, or [Teams consumer users](#). Federated chat is not the same as chatting with a guest user.

- Chats with guest accounts take place within the tenant boundary. All data shared during the chat and the compliance records generated for chat messages remain within the tenant. In a federated chat, the other user is signed into their home tenant. Any information shared during the chat is available using that identity and the substrate creates compliance records for chat messages in the mailbox belonging to the external user.
- Federated chat limits the features available to external chat participants. Guest accounts enjoy extensive access to resources (personal chats, channel conversations, documents, apps, and so on) in your tenant, including access to private channels. External participants are limited to the information in the chat.

Although guest accounts seem like a much better way to communicate with someone from another tenant and some organizations insist on this method being exclusively used for external chat because they want information to be retained within the tenant boundary. However, guest accounts have some downsides when it comes to chat, the biggest being that the external user must switch into your tenant to chat. Federated chat allows users to communicate when signed into their home tenant and is therefore less disruptive to how someone works.

The [following conditions](#) govern external access:

- The tenant must enable external access. This setting is managed through the Users section of the Teams admin center.

- Federation must be permitted with external domains. Each tenant can construct allow or block lists to limit the connections to domains users can make. The default is to allow open communication and if an allow or block list is not defined, the tenant allows inbound connections (or federation) from any other tenant.
- The remote user's tenant also allows external access.
- The remote tenant does not block your tenant by not including the domain in an allow list or explicitly blocking connections from the domain.

Because Microsoft believes that Teams users should be able to connect with people in any other tenant, open federation is the default for Teams. The problem here is that attackers can use social engineering techniques through federated chat to attempt to compromise user accounts. To reduce the risk of such attacks, Microsoft removed the ability of tenants with trial Teams licenses to use federated chat. If you're concerned about the potential for spamming and social engineering attacks, it's recommended that you create an allow list to limit federated chat to known domains. The configuration and management of the external access allow list is discussed more thoroughly in the Managing Teams chapter.

The [Microsoft 365 admin center includes diagnostics](#) to help resolve difficulties in Teams federation which might give you some hints about why external access to a specific address does not work.

When external access is allowed and fully configured, users can enter the user principal name (or email or SIP address) for external users into the search box to have Teams search their tenant's directory to find their account. Teams checks if federation is available between the tenants, and if so, uses the domain name in the address to connect to the other tenant to look up the user. If it finds a match, Teams adds the external user to the chat. For 1:1 or group chats involving an external user, clients highlight that you're using federated chat by including the **External** label at the top of the chat. Teams also flags external participants in the participant list of group chats.

External chat participants use rich native federated chat. In other words, they can compose and send messages like normal chats containing formatted text, links, emojis, stickers, and so on. They can also call or participate in meetings with other chat participants.

By default, external federation allows people outside the tenant to see the presence information of those that they chat with. If don't want to share presence information outside the tenant, enable privacy mode by running the `Set-CsPrivacyConfiguration` cmdlet:

```
Set-CsPrivacyConfiguration -EnablePrivacyMode $True
```

It can take a couple of hours before a change to privacy mode becomes effective. When enabled, privacy mode affects the availability of presence data for all tenant users. There's no way to hide presence data for some users and reveal it for others.

Chats and Calls with Skype Consumer Users

External access also includes communication with Skype consumer users. This connection is natural because Teams and Skype consumer share the same media stack. The feature is disabled for tenants by default, so the first step is to enable the *Users can communicate with Skype users* setting in the **External access** section of the Users settings in the Teams admin center. Once enabled, it takes an hour or so before Teams is ready to connect to Skype.

Teams and Skype consumer users can use chats and VOIP calls to communicate. Because Skype consumer users don't belong to a verifiable organization, when a Skype consumer user reaches out to connect with a Teams user for the first time, the Teams user has the option to accept or block the connection. The Teams user is also able to view the message sent from Skype as an aid to decide whether they want to connect. Both

Skype and Teams users find each other using their email addresses (you can't use a Skype ID or phone number to find a consumer user). In the case of Teams, the connection is like finding a Teams user in another tenant. You input the email address into a new chat, Teams won't find the address in the local directory, and you must instruct Teams to search externally to find the user.

Chats between Teams and Skype consumer accounts support only plain-text messages. Unlike federated chat between tenants, you can't use text formatting and emojis. The two platforms do not share presence information, so you can't find out if a Skype consumer user is free or busy.

Urgent Messages and Priority Notifications

Urgent messages make Teams prompt the recipient with priority notifications every two minutes for twenty minutes (or until the recipient opens the message) to grab their attention and hopefully respond to the message. The idea is that you can use these messages to signal critical events to recipients, like the arrival of a high-priority patient at a hospital emergency departure. The *AllowPriorityMessages* setting in Teams messaging policies controls who can send urgent messages. By default, the setting is **On**, so all users can use the feature. If you have people who abuse priority notifications and make all their messages urgent, you can create a new messaging policy with *AllowPriorityMessages* set to **Off** and assign that policy to their accounts.

To create an urgent message, create a new message in a chat, open the actions menu (+) and select set delivery options. Now set the message priority to Urgent. Unlike notifications for normal Teams messages, you cannot use a priority notification to create an inline reply. Teams wants you to read the urgent message, to complete the priority notification cycle.

Urgent messages are for direct communication with an intended recipient and are unsupported for channel conversations. However, you can send an urgent message to a group chat so that everyone else in the chat receives a priority notification. Only users with a tenant account (including guests) can receive urgent messages. External or federated recipients can't receive urgent messages, and Teams blocks the feature in 1:1 chats and group chats if the participants are external.

Scheduled Send

Scheduled send (delayed send) allows users to set a time in the future (up to seven days in advance) when Teams will deliver a chat message to recipients. The feature is available on desktop and mobile clients, but not for the browser client. To schedule a chat:

- Compose the message as normal.
- Right-click the Send button (or long press mobile clients) and select the date and time for Teams to deliver the message.
- Send the message.

Scheduled send is available in 1:1 and group chats. It doesn't support chats with federated Skype consumer users, but it is available in chats with Teams consumer users. The Teams messaging policy doesn't have a setting to control scheduled send as it is core chat functionality.

Loop Components and Teams Chat and Channel Conversations

[Teams chat](#) and channel conversations support the insertion of Loop components in messages. The difference between the two is that Loop components used in chats are stored in the *Microsoft Teams Chats Files* folder in the sender's OneDrive for Business account (so only those with OneDrive accounts can send Loop components). Loop components used in channel conversations are stored in the channel folder of the SharePoint Online site belonging to the team. Loop component files have a .loop extension. To make a

Loop component available to chat participants, Teams shares the file. If necessary, the owner can share the file with others.

The Teams desktop, browser, and mobile clients support Loop components, including:

- Agenda. Build an agenda for a meeting (including a Teams meeting).
- Table. Just like a table in Word.
- Bulleted list and Numbered list. Work like any other bulleted and numbered list in a Microsoft word processor.
- Checklist. Write down all the things people need to do. Like a task list, but with no assigned task owners and target dates.
- Paragraph. Free text component that's good for capturing ideas and sharing information like web links.
- Task list. Build a set of tasks or follow-up items and assign tasks and expected completion dates to chat or meeting participants. Users can open a task list component in Planner.

Loop components are also used by Teams for "[collaborative meeting notes](#)." This form of notes is a Loop component containing an agenda component, task list component, and a bulleted list component.

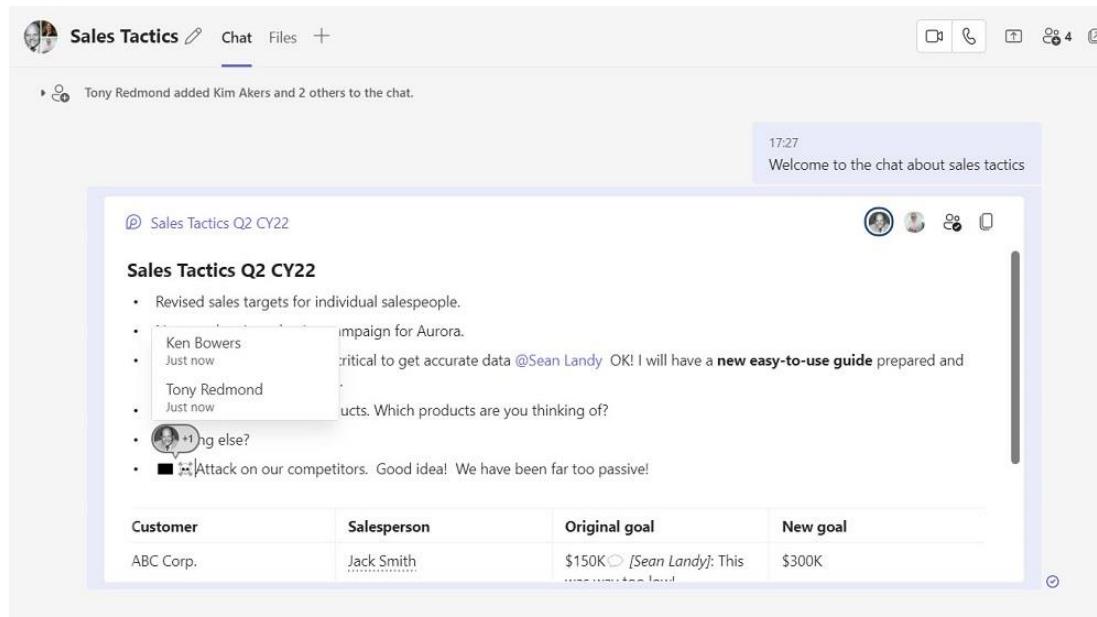


Figure 11-12: A Loop component in active use in a Teams chat

The major advantage of a Loop component is that once sent in a message, updates to the content of the component synchronize and appear for participants in almost real-time. It's like the way updates appear in Office documents using co-authoring with the notable difference that the updates appear much faster than in Office. According to Microsoft, using a Loop component for dynamic collaboration avoids the need for back-and-forward debate in chat because those involved can work out details within the component. All participants see what's happening and it's easier to follow what develops. Figure 11-12 shows a bulleted list Loop component in a group chat with three active users. The component includes an embedded table, and one of the table cells has a comment. This is a good example of how to use a Loop component to have an active discussion in chat.

Points to note about the use of Loop components in Teams include:

- Loop components are unavailable in chats with external (federated) participants.
- External users (including guest members of teams) can't interact with Loop components.
- You can paste text from other applications into Loop components. However, the resulting formatting might not be perfect.

- You can copy Loop components into other Loop-enabled applications, like OWA.
- Unlike normal chat messages, translation of content in a Loop component is not available.
- Share to Outlook doesn't work for chat messages with Loop components.
- DLP for Teams doesn't detect policy violations in Loop components.
- Microsoft search processes the content of Loop component files, meaning that you can include Loop components in content searches. However, search preview cannot open Loop files retrieved by a search. Loop files exported in search results are accessible.
- Compliance records captured for chats containing Loop components reference the file stored in OneDrive for Business and don't contain any of the content. As such, these records are useless to features like communication compliance policies that rely on being able to analyze the content of compliance records.

Microsoft will likely resolve some or all these issues over time.

Video Messages

Using the *Record video clip* option in the desktop and browser client, users can send short (up to one minute) video messages posted to one-to-one, group, and meeting chats. Mobile clients use the Teams camera (beside the compose box for new messages or replies) to capture video messages.

Microsoft enables video messages by default. To disable the feature, update the Teams messaging policies assigned to the user accounts that you want to block and make sure that the *AllowVideoMessages* setting is `$False`:

```
Set-CsTeamsMessagingPolicy -Identity Global -AllowVideoMessages:$False
```

To help recipients understand the content of video messages in crowded or noisy locations, Teams generates captions and a transcript. Recipients can see the captions as the message plays and the sender can download the transcript (in VTT format) or the video file.

Background effects are available for video messages generated using the iOS mobile client. Currently, the iOS client is the only client capable of posting video messages direct to channels. All types of channels are supported.

Video messages posted to channels are stored in the SharePoint Online folder for the channel. Those posted to chats are stored in a Microsoft video service. See [this article](#) for more information.

Teams Meetings

Meetings are a very popular part of Teams. In some cases, meetings are the primary reason why organizations use Teams. A Teams meeting is an online virtual workspace with an identity (a unique URI) in the Teams meeting service. Although meetings have start and end times, they are persistent workspaces that participants can join immediately after creation, even if the scheduled time for the meeting is many days away. A participant can join a meeting multiple times with different devices. A meeting has associated objects, like the participant list, including those nominated in different roles (organizer, presenters, and attendees), optional recording and transcription, and a chat thread. Collectively, these form the complete meeting. Participants can join meetings in a variety of ways, including the "deeplink" pointing to the online meeting space or a meeting code. They can join from Teams clients or from a car using Apple CarPlay through a connected iPhone.

Teams Meetings User Interface

The major components of the Teams meeting UI include:

- The **menu bar** is across the top of the screen. Options available here allow users to view meeting participants, change meeting settings like enabling their camera or applying background effects, and add apps like Q&A.
- The **gallery of cards** representing meeting participants. If their cameras are on, cards show the video feed from participants. Otherwise, cards show the photos from participant accounts or their initials if a photo is unavailable. Teams has different views to present cards, including the basic 3x3 view (available on desktop and Chrome-based browsers), a large gallery view, and "together mode."
- The meeting **canvas**, used to present information in a meeting. The canvas supports sharing of information such as:
 - Presentations (using PowerPoint Live or regular PowerPoint).
 - Applications running in a window.
 - A meeting participant's complete screen.
 - Workbooks shared through Excel Live. Features like autosave and co-authoring allow meeting participants to have full access to these workbooks.
 - Whiteboards.

Broadly speaking, the meeting (and calling) experience available in the Teams desktop and browser (Chrome and Edge) clients support equivalent features. Other browsers, like Safari and Opera, might only support a simplified meeting experience in terms of the range of available options. Apple iPads support the use of external webcams and cameras for meetings, but only if the device runs iPadOS 17 or later and the external device is connected before the meeting starts.

Creating New Meetings

Users create and manage Teams meetings through either the Teams **Calendar app** or an Outlook client. Control over the ability for users to create Teams meetings is set via the meeting policy assigned to accounts. Guest users can't create meetings. Four settings in the general section of the meeting policy assigned to accounts exert control over the kind of meetings users can create:

- Allow the **Outlook** add-in: If the setting is on, Outlook (Windows and Mac desktop clients, Mobile, or OWA) can schedule online Teams meetings (you can [configure settings to make Teams online meetings the default](#)) and Outlook automatically loads the [Teams meeting add-in](#) when the client starts. Outlook desktop and mobile clients can support several mail accounts in a profile, with one account assigned as the default (used to send outbound email). The Teams meeting add-in runs in the context of the default account, so it's important that the account chosen as the default is the one used to create Teams meetings. Outlook can only create private meetings, so the Teams meeting policy assigned to their account must allow the user to create private meetings (any meeting not published in a channel is private).

The Teams meeting add-in uses the Edge WebView2 component, and it receives updates during the automatic update cycle for the Teams desktop client. It also depends on the .Net framework. The workstation should run the latest version (4.8 at the time of writing). On Windows PCs, you can check the version of the .Net framework with PowerShell. This command returns *True* if 4.8 or above is installed.

```
(Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full").Release -ge 528040
```

Apart from creating new Teams private meetings, the add-in also allows users to update meeting settings (like who can join without going through the lobby, who can present during the meeting, etc.). The add-in includes a *Meet Now* button to allow users to create impromptu personal meetings. The user must be signed into their home tenant to allow the *Meet Now* option to work, so if they're connected to a different tenant, they must switch back to use *Meet Now*. See this post for [more](#)

[information about the Teams meeting add-in for Outlook for Windows](#). A version of the add-in is available to [allow Google Calendar and Google Workspace users to schedule and manage Teams meetings](#).

- Allow **channel meeting** scheduling: If on, the user can create a meeting in any standard or shared channel in teams they belong to by:
 - Selecting a channel when creating the meeting in the Teams calendar app.
 - Using the *Schedule a meeting* button in the compose reply options.
 - Using the *Meet Now* option in the channel header.
 - Creating a new meeting in the channel calendar.

Channel meetings appear as a new topic within the channel to make the meeting available to team members. Chat messages from the meeting also appear in the topic and are visible to all members, including those who do not take part in the meeting. You can add participants to a channel meeting who don't belong to the team. These attendees can join the meeting but cannot access resources shared through the channel. One advantage of channel meetings is that meeting resources like documents and recordings are in the channel folder of the document library in the team's SharePoint site instead of an individual user's OneDrive for Business account, as is the case for private meetings. This can be important when people leave the organization along with their OneDrive for Business accounts, which might contain documents relating to important meetings. Although it's possible to give someone else access to a user's OneDrive for Business account when they leave to review and recover information, this is a step easy to overlook.

- Allow scheduling **private meetings**: If set, the user can create a private (or personal) meeting. As noted above, a private meeting is a meeting not scheduled for a channel. Like personal chats, you dictate who receives invitations to join the meeting. If a participant cannot join the video or audio part of a meeting, they can still contribute to the conversation. Invitations for private meetings come from the meeting organizer's mailbox. Teams considers meetings created with the Teams add-in for Outlook as private, even if you add a team as an attendee for a meeting. You can invite people outside your organization to a meeting, even if they do not have a guest account in the tenant, by adding their email address as a participant. This is known as an *anonymous join* and generates an invitation to the email address to allow the recipient to join the meeting.

Being able to create private meetings also allows users to create offline meetings. These are meetings without an online presence, so they don't have an online meeting space, chat, attendance report, or the other objects that make up a regular Teams online meeting. Offline meetings are intended to allocate time slots for events like personal appointments, meals, breaks, and in-person meetings and function exactly like similar Outlook events.

- Allow **Meet Now** in channels: If on, the user can create an ad-hoc meeting. These meetings are like channel meetings in that they occur in a channel. To start an ad-hoc meeting, click the *Meet Now* icon under the compose message box. Team members can join the meeting if they wish. Another policy setting (*Meet Now in private meetings*) controls whether users can create unscheduled meetings outside channels.

Teams meetings support desktop sharing (including the ability to only share a specific window rather than the entire screen), recordings, muting noisy attendees, and transfer control to other participants so that they can run a meeting. Participants can use [Whiteboard as a collaborative space](#) to share and develop ideas during meetings.

To record a meeting, a Teams bot joins the meeting to capture the audio, video, and screen sharing activity in a feed sent to Azure Media Services. When the recording is turned off (or the meeting ends), the video file is stored in OneDrive for Business (personal meetings) or SharePoint Online (channel meetings). Any of the

meeting participants can play the recording. The owner of the recording can share it to allow others access to the content. The Videos chapter has more information about the management of Teams meeting recordings.

Up to 1,000 participants with full access to all resources can join a Teams personal or channel meeting (the limit is 300 if breakout rooms are used). Full access means that attendees can use video and access meeting resources such as the whiteboard, and chat. After the meeting reaches its capacity, Teams can switch automatically to admit view-only attendees. See the later section covering meeting overflows and view-only attendees.

Sharing Files in Teams Meetings

People accustomed to Outlook often notice a difference in the way files are handled when scheduling meetings with Outlook and Teams. Outlook allows the attachment of files to meeting invitations while Teams does not. The Teams calendar app doesn't display attachments added by Outlook. If you want to share files with meeting participants, the organizer can include links to the files in the meeting invitation or participants can upload them to the Files section of the meeting. If the text isn't too long, the organizer can include it in the body of the meeting invitation.

Any tenant user can share a file before, during, or even after a meeting. If the attachment is a text file and isn't too long, you can also cut and paste the text into the body of the message invitation. Guest users who have OneDrive for Business accounts can also share files once the meeting starts (permissions might need adjustment to allow access to these files). Other participants can share links to files in the meeting chat during the meeting.

Files shared in meetings are in the *Microsoft Teams Chat Files* folder of the sharer's OneDrive for Business account. Teams uses sharing links to control access to files by meeting participants. One thing to note is that the sharing link applied to a file shared in a meeting doesn't give access to people who subsequently join the meeting. If new attendees join, file sharers must update the permissions to allow them access.

Streaming Meetings and View-Only Attendees

Organizations can update Teams meeting policies to enable the use of Teams streaming services for overflow attendance at large meetings. When enabled, Teams will allow people to join a meeting after the meeting reaches its capacity. These people are view-only participants and have limited access to meeting content. Up to 20,000 view-only attendees can join a meeting. This limit will reduce to 10,000 on June 30, 2024 ([see the limits for meetings](#)).

View-only attendees can:

- See the video feed for the current presenter or content they share from their desktop.
- Hear the audio feed for other full participants.

They cannot:

- Use the gallery, large gallery, or together mode views to see other participants.
- Interact with other participants through meeting chat, polls, or file sharing.

View-only attendees can join using any Teams client. They cannot join using a Teams Room system or Cloud Video Interop (CVI) services. View-only attendees don't appear in the participant list, which means that the meeting organizer can't remove them from the meeting. They don't appear in the attendance report generated by Teams after the meeting. Because Teams uses streaming services to deliver the video and audio content to view-only attendees, the content is approximately 30 seconds behind the live meeting.

Control for view-only attendance for meetings is through the *StreamingAttendeeMode* setting in the Teams meeting policy assigned to the organizer. By default, this is False. To enable view-only attendees, update the policy to True. For example:

```
Set-CsTeamsMeetingPolicy -Identity "Allow Meeting Recording" -StreamingAttendeeMode Enabled
```

As always, it can take several hours before a policy change becomes effective.

Using Teams Meeting Policies to Control Features

Teams meeting policies include settings to control aspects like meeting and call recording, transcription, screen sharing, PowerPoint sharing, and use of a whiteboard. The settings of the default meeting policy enable users to create all supported types of meetings within Teams. If necessary, you can create new meeting policies to disable access to some meeting features and assign the policies on a per-user basis. For example, you might decide that only specific users can record meetings. To do this, you would:

- Set *Allow cloud recording* to *Off* in the default Teams meeting policy. This setting blocks the ability of users to record meetings. To enable meeting recordings, assign users a meeting policy with the setting turned to *On*.
- Create a new Teams meeting policy where the *Allow cloud recording* and *Allow transcription* settings are enabled (set to *\$True*). This will allow meeting organizers assigned the policy to record meetings and generate automatic transcripts. The transcription setting is only available in PowerShell, so you will need to run a command like:

```
Set-CsTeamsMeetingPolicy -Identity Global -AllowTranscription $True -AllowCloudRecording $True
```

- Assign the new Teams meeting policy to selected accounts.

Although you can assign the new meeting policy to accounts through the Teams admin center, PowerShell is usually the best way to assign a policy if a large set of accounts is involved. This example shows how to fetch a set of mailboxes based on a filter against one of the custom attributes and then use the *Grant-CsTeamsMeetingPolicy* cmdlet to assign a custom Teams meeting policy to each account:

```
[array]$Mbx = Get-Mailbox -RecipientTypeDetails UserMailbox -Filter {CustomAttribute1 -eq "Meetings"}  
ForEach ($M in $Mbx) {  
    Try {  
        Grant-CsTeamsMeetingPolicy -PolicyName "Allow meeting recording" -Identity  
        $M.UserPrincipalName  
        Write-Host $M.DisplayName "is allowed to record Teams meetings" }  
    Catch {  
        Write-Host "Problem occurred when assigning the Allow meeting recording policy to"  
        $M.DisplayName } }
```

By default, Teams meeting policies disable recordings for 1:1 calls. If you want to change this, use the *Set-CsTeamsCallingPolicy* to update the *AllowCloudRecordingForCalls* setting to *\$True*. More information about the settings in Teams meeting policies is discussed in the Managing Teams chapter.

Another important setting in Teams meeting policies controls if meeting participants must give explicit consent for inclusion of their audio and video feeds in Teams meeting recordings and transcripts. For example, this command enables explicit participant consent for the default meeting policy.

```
Set-CsTeamsMeetingPolicy -Identity Global -ExplicitRecordingConsent Enabled
```

When consent is required for a meeting and recording or transcription is enabled, Teams starts the call with all participants muted and their cameras off. As participants join, Teams prompts them for consent for inclusion in the meeting recording and transcript. A participant gives consent by unmuting their microphone,

enabling their camera, or sharing their screen. These actions are captured in the meeting attendance report. When consent is not given, Teams blocks the following for the user:

- Audio feed.
- Video feed.
- Screen and content share (such as working on a shared Excel worksheet).

Participants who do not give consent can still see and hear contributions from other participants. See [this article](#) for more information.

Teams Meeting Etiquette

Like any other business activity, some preparation on the part of meeting attendees and a sense of how people should behave in meetings make online gatherings run smoother. Here are some basic points about Teams meeting etiquette:

- **Be on time:** There's nothing worse than people showing up late for meetings, even if the meetings are online.
- **Start the meeting muted and stay muted unless you need to talk:** There's no need to share background noise and other distractions that might be happening around you, like a jet passing overhead. Keep your microphone muted until you have something to say and make sure that your microphone is unmuted a second or so before you speak. Always mute if you need to cough, sneeze, burp, or otherwise do something that others might find unpleasant.
- **Use a camera if your PC has one:** People are more connected and involved in meetings when everyone is visible. If your network connection supports the video load, turn on your PC's camera when you join meetings, after positioning the camera so that your face is visible and head-on. Once the meeting starts, it's acceptable to turn your camera off when listening to a presentation or need to step out to do something. No one needs to see a video feed of an empty seat. Well-lit rooms are better than dark rooms for video calls as the lighting helps camera performance. Use lighting above or to the side, never behind you. Above all, you'll look better when people can see you.
- **Blur your background:** No one needs to see just how messy your office is. Remove the distraction by blurring your background. Alternatively, you can choose to use a custom background image. If you do, make sure that your chosen image is professional and appropriate.
- **Understand Q&A protocol:** Some presenters like taking questions during a meeting. Others hate the idea because they believe questions are distracting and spoil the flow of their presentation. These presenters prefer to take questions in a structured manner when they're finished. It's good to set ground rules before presentations begin. When asking questions, make sure they're directed to someone as open-ended questions often result in a cacophony of competing voices.
- **Use meeting chat intelligently:** Every meeting includes a group chat. You can use the chat to capture questions to make sure that they are noted and either addressed during the meeting or followed up afterward. Making notes in the meeting chat is also a great way to make attendees aware of resources, such as posting links to supporting material.
- **Raise your hand:** Teams has a virtual raised hand feature that you can use to indicate to other participants that you want to speak. Use it. And presenters should keep an eye on the meeting roster to see if anyone raises their hand. Teams automatically lowers raised hands after a participant gets to speak.
- **Use reactions to communicate with the presenter:** Reactions like thumbs-up or like are good ways to inform a presenter what you think of their material and delivery. Meeting reactions (see later) are also excellent ways to avoid a barrage of responses in meeting chats to common presenter queries like "Can you hear me?" or "Can you see my slides?"

- **Restrain multitasking:** You can multitask during a meeting, but if your video is on people might know that you're not concentrating on the meeting. Is that an impression you want to give?
- **Silence your phone:** If you're in a meeting, you should be involved. Don't disturb the flow of discussions by allowing your mobile or landline to ring during the meeting. And if you do need to take another call, make sure to mute your microphone as it's highly unlikely that the other meeting participants want to listen to your call.
- **Ask before recording:** Teams is good at capturing the audio and video content for a meeting in a recording. Before you record a meeting, make sure that all participants are happy with the idea. And let them know that the recording will be available in OneDrive for Business soon after the meeting ends. The recording and transcript allow participants to check what happened during the meeting. Remember that only tenant users have access to these meeting resources.
- **Add color to the call:** Sharing app content to make your point is good, unless you have some boring PowerPoint to share (or boring Excel). If you're going to share content, make sure it's relevant, accurate, and restrained to just what people need to know.
- **Invest in a good headset:** There's nothing worse when someone in a meeting uses poor audio equipment that forces participants to strain to hear what they're saying. Do everyone a favor and invest in a good headset to use for Teams calls, preferably one that the manufacturer attests will work well with Teams.

A good way to remind people about the etiquette for online Teams meetings is to include some text in calendar invitation messages. As [explained in this post](#), a mail flow rule can insert a disclaimer in calendar messages. The disclaimer text can point to a website or contain some basic rules like those explained above.

Creating Teams Meetings with Outlook and the Calendar App

If Teams is enabled for an account, the Teams meeting add-in is automatically loaded when Outlook starts. The add-in is available for Outlook desktop (Windows and Mac), OWA, and Outlook mobile to allow users to create and manage private Teams meetings. Each meeting has a link to the online location or thread which is included in meeting notifications and reminders. The link is a [Globally Routable User Agent URI \(GRUU\)](#), a URI formatted to allow Session Initiation Protocol (SIP) clients to connect to an online event. In the case of Teams, the URI is a deeplink to the location in the Teams infrastructure where the meeting is hosted. Meetings created through the calendar app insert the same kind of URI.

You can think of the online location as the workspace where audio and video feeds come together to instantiate the meeting. It's one of the resources belonging to the meeting along with the participant list, recording, notes, whiteboard, and so on. Once created, the online space is available for any participant to join, even if the starting time for the meeting is long in the future. This facility exists to allow people to prepopulate a meeting with resources, like notes or shared files, before it begins. Likewise, a meeting persists after its formal end time to allow participants to access its resources after the meeting finishes.

To allow meeting participants to navigate to the online workspace, Outlook populates several properties of the calendar event such as *OnlineMeetingConfLink* and *SkypeTeamsMeetingURI* with joining information. Outlook and the Teams calendar app use these properties to recognize the event as an online event and to show the Join button in meeting reminders and other places in the client UI. Clicking the Join button (or the *Join Microsoft Teams Meeting* link in the body of the meeting item) starts the process of joining the meeting, which might involve navigating through a web page to choose how to join and waiting in the meeting lobby for admittance.

All instances of a recurring meeting use the same joining information. In other words, the same online workspace hosts all instances of a recurring meeting.

Users can copy the deeplink for a meeting from the body of the invitation or the Teams calendar app (it's available in several places, including if you right-click on a meeting). People often retrieve the deeplink to send it to other people who might want to join the call. Any client can use the deeplink to join the meeting.

Apart from using its deeplink to connect to a Teams meeting, Teams meeting invitations include a meeting identifier (like 385 011 801 214) and password (like *mKrtmd*). Meeting participants can use this information to join a meeting by entering the details in a Teams client or the [Teams join a meeting page](#).

Tip: If you edit an Outlook meeting and update the Join Microsoft Teams Meeting link, you can add the string `&webjoin=true` to the end of the link to force users to join the meeting with the browser client instead of getting the option to choose between joining with the browser or desktop client.

Private Meetings

A private (or personal) meeting is one scheduled by an individual user with other tenant accounts, external users, distribution lists, and Microsoft 365 Groups (for the groups included in the GAL). After entering the invitees, Exchange Online sends a copy of the meeting invitation to each participant, who can accept or decline the invitation. Like Outlook, the Teams calendar app has a scheduling assistant to help find the right time for a call.

When you add a distribution list to an invitation, Exchange Online expands the membership and sends notifications to the individual recipients. Distribution lists can contain recipients like other groups, mail contacts, mail users, and even public folders, so you might not know the full set of users who receive invitations to a meeting. Microsoft 365 groups don't support nested groups and are composed of mailboxes and guests.

Teams meetings are events in the personal calendars in the mailboxes of participants. The Teams calendar app synchronizes data from the personal calendar. If reminders are set for meetings, Outlook notifies users when meetings are about to happen. Except for an icon posted alongside a channel name when a meeting is in progress, Teams clients flag active meetings when they start, and participants can join a meeting from the notification, the Outlook reminder, or from the details in the events in the Outlook or Teams calendars.

You can also schedule recurring meetings by selecting a value such as Daily, Monthly, or Yearly from the Repeat drop-down list.

Meeting Recap

A notable feature available to private meetings is the recap, which is how Teams highlights important resources following a meeting. After a meeting is over, participants can access the meeting recording and transcript, and the organizer can access the attendance report here. Channel meetings and Meet Now meetings support recordings, but don't generate a transcript. Organizers with premium Teams or Copilot licenses see more recap information, including meeting notes, follow-up tasks, and a timeline showing when individual participants spoke during the meeting.

Transcription and Recording

Meeting organizers have the option to capture a recording or transcript as records of what occurred during the meeting. Meeting recording is available for all forms of meetings. Organizers, co-organizers, and presenters can initiate the recording from the desktop, browser, and mobile clients. Teams stores meeting recordings as MP4 files in OneDrive for Business (personal meetings) or SharePoint Online (channel meetings).

Enterprise Teams licenses include support for live captions, CART captions, captions in other languages, and automatic transcription. This functionality includes access to captions for anonymous meeting participants. If permitted by the meeting policy assigned to the meeting organizer, participants with the organizer, co-organizer, or presenter roles can start transcription for private meetings using the Teams desktop client.

Microsoft says that they will introduce the feature for channel and Meet Now meetings in the future. Users can opt to display captions on the left or bottom of the screen and can choose their preferred color, type face, and font size. If they have a Teams Premium license, users can choose to see captions in a different language to the default language selected for the meeting.

To generate live captions and create the transcript, Teams uses a bot to listen to the audio feeds of participants and an AI-based learning model to analyze what's said during the meeting. Transcription supports multiple languages including Arabic, Chinese, German, French, Italian, Russian, Spanish, and Dutch with more languages becoming available over time. Support means that the AI can recognize and parse the spoken contributions of people in those languages. The AI can capture but cannot understand participant contributions in other languages, so the output won't make much sense. The ability for users to view captions in a language different to that selected for the meeting is a Teams premium feature.

Transcription includes speaker attribution, meaning that Teams includes the name of the speaker alongside their contributions. Attribution makes it easier for people to know who said what during a meeting. If users prefer, they can disable attribution in the *Captions and transcripts* section of Teams client settings. When this happens, Teams inserts generic speaker identifications (like "Speaker 1") instead of their real names. Live captions includes a profanity filter that participants can enable to force Teams to mask words deemed to be profane or obscene. The effectiveness of the profanity filter depends on knowledge of objectionable words, the quality of microphones used by meeting participants and their enunciation. Microsoft 365 Copilot uses the meeting transcript for its analysis of the proceedings. Users with a Copilot license can interact with Copilot to ask questions about what occurred during a meeting.

Once a meeting finishes, Teams generates the final copy of the transcript and makes it available in the meeting recap. Users can then download the transcript in Word (DOCX) or Video Text Track (VTT) format. Guest users don't have access to the Teams calendar app, so they can't access the transcript. Only the meeting organizer or a Teams administrator can remove a transcript.

Transcripts and recordings are stored as MP4 files in the Recordings folder of the meeting organizer's OneDrive for Business account. Depending on the options chosen by the meeting organizer, the recording in the MP4 file created for a meeting can be:

- Video (including audio) with or without a transcript.
- Transcript only.

If a meeting is transcribed without video, AI captures the text for participant contributions and then discards the video and audio tracks, meaning that the MP4 file only holds the transcript. The text of transcripts is indexed and discoverable.

Attendance Report

After private meetings finish and the meeting policy assigned to the organizer's account permits, Teams generates an attendance report for the meeting organizer. Settings in the meeting policy also control who appears in the attendance report (the default is everyone, but participants can opt out) and what to show in the attendance summary (just who attended or everyone invited). The Teams back end generates the meeting data from the information gathered in the Graph as people join and leave the call. Teams stores the data for these reports in [a hidden folder of the meeting organizer's Exchange Online mailbox](#). The meeting organizer can view the information through Teams by opening the meeting and going to the attendance tab (Figure 11-13). Alternatively, they can download the data to a CSV file. Meeting attendees cannot access the attendance report. However, the organizer can download the data and share the CSV file with attendees if they wish.

It's possible that the meeting organizer will restart the meeting several times with each instance having a different attendance. Teams generates a separate version of the attendance report each time a meeting starts.

The organizer can choose which version to view using a drop-down menu in the attendance tab. Downloading the CSV file uses the data for the latest instance of the meeting. If the organizer goes to the meeting chat, they can select whichever instance they wish to download that data.

Administrators can access limited information about a meeting through the Teams admin center by selecting the meeting organizer in the Users section and then selecting the meeting from the Meetings & Calls tab. The data presented in the admin center is to help debug meeting connection problems and it doesn't include any possible sensitive information such as the meeting title. However, you can see who joined the meeting.

The screenshot shows the 'Attendance' tab selected in the Microsoft Teams meeting summary. Key statistics displayed are: 8 Attended participants, the meeting started at 16:28 and ended at 17:21, the total duration was 52m 43s, and the average attendance time was 46m 19s. Below this, a table lists the participants with their names, first join time, last leave time, in-meeting duration, role, and engagement metrics (including emoji reactions). The participants listed are Tony Redmond, Vasil Michev (MVP), Michel de Rooij (MVP), Brian Desmond (Ravens...), Christina Wheeler, Juan Carlos Gonzalez Martin, Paul Robichaux | Keepit, and Ben Lee (Guest).

Name	First join	Last leave	In-meeting durat...	Role	Engagement
Tony Redmond Tony.Redmond@i...	16:28	17:21	52m 37s	Organiser	💡 - 📺 1 🎙️ - 🔥 - ❤️ - 🍏 - 😊 - 🤪 - 🍃 -
Vasil Michev (MVP) (Guest)	16:30	17:21	50m 38s	Presenter	💡 5 📺 - 🎙️ - 🔥 - ❤️ - 🍏 - 😊 - 🤪 - 🍃 -
Michel de Rooij (MVP) (Guest)	16:30	17:20	49m 59s	Presenter	💡 2 📺 1 🎙️ - 🔥 - ❤️ - 🍏 - 😊 - 🤪 - 🍃 -
Brian Desmond (Ravens...) (Guest)	16:31	17:20	49m 57s	Presenter	💡 2 📺 1 🎙️ - 🔥 - ❤️ - 🍏 - 😊 - 🤪 - 🍃 -
Christina Wheeler (Guest)	16:31	17:21	49m 29s	Presenter	💡 6 📺 5 🎙️ - 🔥 - ❤️ - 🍏 - 😊 - 🤪 - 🍃 -
Juan Carlos Gonzalez Martin	16:35	17:21	45m 19s	Presenter	💡 1 📺 1 🎙️ - 🔥 - ❤️ - 🍏 - 😊 - 🤪 - 🍃 1
Paul Robichaux Keepit (Guest)	16:38	17:21	42m 38s	Presenter	💡 1 📺 1 🎙️ - 🔥 - ❤️ - 🍏 1 😊 - 🤪 - 🍃 -
Ben Lee (Guest)	16:49	17:19	29m 55s	Presenter	💡 1 📺 - 🎙️ - 🔥 - ❤️ - 🍏 - 😊 - 🤪 - 🍃 -

Figure 11-13: Teams meeting attendance report

Using Lobby Bypass

The *automatically admit people* setting in the meeting policy assigned to a meeting organizer's account dictates who can join a meeting. Depending on the setting, some participants can join the meeting and bypass the virtual lobby. Others must remain in the lobby until the meeting organizer, a co-organizer, or a presenter admits them. Available options include the ability to admit everyone in the organization automatically (this includes guest users) or everyone in the organization and other federated Microsoft 365 tenants. Organizers can update the settings of an individual meeting to fine-tune the types of participants who must wait in the lobby. The following values are available:

- **Everyone:** All users, including anonymous users, can join the meeting without waiting.
- **People in my organization and guests:** Everyone with a tenant or guest account can join without waiting.
- **People in my organization, trusted organizations, and guests:** Only people with accounts in the tenant directory, or those with accounts in federated (trusted) organizations, can join without waiting.
- **People in my organization:** Only tenant users can join without waiting.

- **People who were invited:** Only those who receive an invitation to the meeting (they are on the attendee list) can join without waiting. It's a good idea to amend meeting settings to disable the ability for users to forward invitations to other people for meetings with restricted attendance. The flag prevents [email clients which can block forwarding of meeting invitations](#) from showing the forward option. However, those who receive invitations via forwarding can still join automatically, which is why it's a good idea to check the participant roster during confidential meetings.
- **Only organizers and co-organizers:** Only the meeting organizer and co-organizers can join automatically. Everyone else must wait for admittance.

Options such as "Only me" or "People I invite" (including a distribution list to specify the participants) allow organizers to exert more precise control over the lobby. For instance, for confidential meetings it's a good idea to update meeting options so that only the organizer or those invited explicitly can join automatically. All other participants must wait in the lobby for admittance, which removes the risk of an external person joining the meeting without anyone noticing and so gain access to confidential information.

Channel Meetings

Channel meetings differ from personal meetings because they are scheduled by someone on behalf of the channel using the calendar app or the channel calendar app. Because it's designed to create personal meetings, the Teams meeting add-in for Outlook doesn't support the scheduling of channel meetings. When a channel meeting is created, the team owning the channel becomes the meeting owner and the meeting is created in the group calendar of the team's group mailbox instead of the organizer's calendar. The group calendar stores meetings for all channels in a team, and the channel calendar app applies a filter to display only the events belonging to the channel into which the app is installed.

Because they act as the meeting organizer, the original creator of a channel meeting can change its details, such as adding extra attendees, altering the time, or deleting the event. Channel meetings are open to any member of the team the channel belongs to and therefore members don't need permission to attend these meetings. Another way of looking at this is that people don't need to attend the meeting unless they are interested in the topic. It's there for them to attend, but there's no compulsion to be there.

When someone creates a new channel meeting, they have the option to send personal invitations for the meeting. This means that everyone with access to the channel receives a meeting invitation by email. Alternatively, individual members can be added to the participant (invitation list) for the meeting to receive a personal invitation. If Teams doesn't generate personal invitations, members learn about the meeting by seeing the conversation about the meeting appear in the channel. When the meeting is active, Teams posts a new topic in the channel with a join button for members to participate. A camera icon is also shown beside the channel name in the team list. Unless they are added to the attendee list, only members receive invitations to channel meetings if they are subscribed to the group for calendar events. Users can update their subscription settings for a Microsoft 365 group by opening it in OWA and editing the **Manage group mail** settings from the [...] menu. The group is only available in OWA if it is not hidden from Exchange clients. However, most of the groups used by Teams are hidden, and administrator intervention is often necessary to update group subscriber lists. See this [article for more information](#) about how to use PowerShell to update group subscriptions so that team members receive invitations for channel meetings.

Any member of a team can attend a channel meeting. The organizer can invite people from outside a team to join a channel meeting. These participants can attend the meeting, but they won't be able to participate in the meeting chat, or access shared documents, or the transcript because they don't have access to resources stored in the channel.

Private channels can't host channel meetings. Although they belong to a team, private channels don't have a group mailbox, so they can't schedule the meeting in a calendar. Another restriction to remember is that after

you schedule a meeting in a channel, you can't edit the meeting to move it to another channel. If you create a meeting in the wrong channel, you must remove the original meeting and reschedule it in the correct location.

Don't Use Channel Meetings for Sensitive Subjects: Because any member of a team can attend a channel meeting, it's a bad idea to use channel meetings to discuss sensitive or confidential topics. Doing so creates the risk of inadvertent information disclosure. For instance, any member of the team can view the recording of a channel meeting or access files shared in the meeting. Use personal meetings instead as this gives you the ability to control who attends the meeting and who can access content shared in the meeting.

Channel Meetings App

The channel meetings app is one of the Microsoft apps automatically available to a tenant. The app can be installed as a tab to allow team members to access meetings scheduled for the channel. Events for all channels are in the group calendar, so the app filters and displays the meetings for the channel into which it is installed. The interaction between users and meetings is like that available in the Teams calendar app. Because guests don't have permission to access the group calendar, the channel meetings tab isn't available to them. Any other member can use the app to schedule or view channel meetings. As with channel meetings scheduled through the Teams calendar app, the person who creates a meeting is its organizer and is the only one who can update meeting settings.

Meet Now Unscheduled Meetings

The Meet Now feature is a way for users to launch impromptu or unplanned meetings without having to schedule a formal event. *Meet Now* events can be launched in the Teams calendar app (to create a private meeting) or a channel (to create a channel meeting) on the desktop, browser, and mobile clients. The Teams meeting add-in for Outlook for Windows also includes a Meet Now button to create a private meeting. As with other Teams meetings of the same type, participants must be invited to private meetings while channel meetings are available to the members of the team which owns the channel.

The ability to use Meet Now is controlled by two settings in the Teams meeting policy assigned to user accounts:

- **Meet Now in channels:** Controls if the user can use Meet Now to create a new channel meeting.
Applies to all channels in all teams the user belongs to.
- **Meet Now in private meetings:** Controls if the user can use Meet Now to create private meetings.

When using PowerShell to manage policy settings, run the `Set-CsTeamsMeetingPolicy` cmdlet and set `AllowMeetNow` and `AllowPrivateMeetNow` to True (allowed – the default) or False (blocked). In most cases, being able to create meetings on demand is a welcome capability and organizations are happy to let the feature be used. The usual situation where Meet Now is disabled is in education scenarios where organizations often block students from organizing online events.

Planning Meetings

[Teams meeting templates](#) are a way for a user or administrator to create a specific type of meeting, such as a Virtual appointment or a controlled-content meeting. Teams also uses meeting templates to define settings for events such as webinars and town hall meetings. If you have Teams premium licenses, your organization can create custom meeting templates to define the settings for different kinds of meetings. The settings include details like if recording happens, if encryption is used, and so on. Meeting templates appear in the New Meeting menu. If a user selects a template from the list, Teams applies the settings defined in the template to the new meeting.

If you don't use a template to create a meeting, you can configure the meeting settings (like who can present in the meeting). Individual invitees can then configure aspects of their participation, such as their audio and video settings. All settings are subject to the meeting policy assigned to the meeting organizer. For example, the screen sharing mode control in the meeting policy assigned to the organizer determines if participants can share desktop and/or a window in a meeting while the allow chat setting controls if participants can chat during the meeting. Other important controls are those that allow anonymous participants (dial-in users) to start a meeting (without an authenticated user being present) and which participants can join a meeting automatically (without having to wait in the meeting lobby). This is an important control if your tenant commonly organizes meetings with external people because you might want to force organizers to be sure that a meeting is ready to begin before admitting certain types of participants. The available options to restrict the ability to join meetings automatically are described above under "Lobby bypass."

If your organization allows anonymous participants to join meetings, it's a good idea to consider if you want them to have access to the meeting chat. A setting in the meeting policy can turn chat on or off for everyone, or on for everyone except anonymous participants.

Guard the Meeting Link: As described earlier, clients use the deeplink pointing to the online meeting space to join the meeting and access meeting resources. Anyone with a deeplink for a meeting can join it and might gain automatic admittance if allowed by the meeting policy assigned to the organizer or the lobby bypass settings for the meeting. Uninvited attendees will be able to access the video and audio feeds, including any information shared during the meeting. In private meetings, they can access the meeting chat. This isn't possible in channel meetings because access is restricted to members of the team owning the channel. Because possession of a deeplink makes this access possible, it's important that the organization considers who can join a meeting automatically and organizers tune lobby bypass settings for confidential meetings to restrict access to those invited.

Meeting Roles

When planning larger or more structured Teams meetings, it is usually important to define specific roles for some participants. For regular meetings, including webinars, the roles are:

- **Organizer:** The organizer is the person who creates the meeting. The organizer has full control over the meeting, its participants, and meeting settings.
- **Co-organizer:** Optionally, a meeting can have up to ten co-organizers chosen from the tenant users invited to the meeting. Guest accounts can't be co-organizers. Users assigned this role can manage the meeting while it is active, including creating, starting, and removing breakout rooms (see later section). However, they cannot edit the meeting invitation or access the attendance report.
- **Presenter:** This is also an optional role. By making a tenant user or guest user from another tenant a presenter, the meeting organizer allows them to share content like presentations during the meeting. Presenters can also start and stop the meeting recording and manage participants (mute and remove participants, admit people from the lobby).
- **Attendee:** All other invited participants are attendees. These are full participants in the meeting (they can speak and chat). However, they can't share content, present, or manage the meeting in any way.

For Teams Town Hall events, the roles are:

- The **Producer** is responsible for making sure the presentation works. The producer is also responsible for managing the feeds in the event and monitoring the quality and stability of the event. This role serves the same purpose as the organizer of a regular meeting. Teams Town Hall doesn't have a producer role as the event organizer has these responsibilities.
- **Presenters** focus on content delivery.

- The **Moderator** follows questions asked by attendees to answer questions or to ask the speaker when they finish presenting. The moderator can be a person who holds the producer or presenter role.

The big difference between town hall events and regular meetings is that attendees are more restricted in live events as their role is essentially passive. By comparison, participants in regular team meetings can usually interact with each other unless meeting settings prohibit chat or a meeting organizer, co-organizer, or presenter mutes them.

[This article](#) describes what presenters and attendees can do during meetings. The short version is that presenters have all capabilities, but attendees can only join in the meeting chat (unless this feature is disabled), speak and share videos, and view PowerPoint presentations shared privately.

Updating Meeting Options

The *Roles that have presenter rights* setting in the Teams meeting policy assigned to the meeting organizer sets the default presenter right for meetings created by that person. The options are:

- Everyone can present.
- Everyone in the organization (including guests) can present.
- Only the organizer and co-organizers can present.

When the meeting is created, Teams sets the presenters for the meeting according to policy. Later, you can modify the roles assigned to meeting participants. For structured meetings, it's common to find that you need to nominate some people to be presenters before the meeting starts. To preassign the presenter role, you:

- Add the people you want to be presenters to the meeting participant list.
- After the meeting is created, you can update meeting options through the calendar app or the Teams meeting add-in.
- Select specific people to be presenters (the other option to nominate presenters are Everyone, people in the organization, and only me).

Once you limit who can present in a meeting, you also restrict people outside your organization from presenting because you can't preassign the presenter role to external participants (including guests). However, once the meeting starts, you can update the role of these participants to allow them to present.

For larger meetings, it's best to restrict the set of presenters to those you expect to speak during the meeting and use the (virtual) raise hand feature to allow other attendees indicate when they wish to contribute.

Presenters can see who's got their hands raised (if multiple people raise their hands, they are listed in chronological order based on when they raised their hands). If people are muted, the presenter can unmute them to allow them to speak and lower their hand in the list.

When a meeting is active, you can change a person's role. For instance, you can make an attendee a presenter and vice versa. Do this by viewing the meeting participants in and selecting *More options* for an individual participant. These controls are not available in channel meetings.

Galleries and Together Mode

The view of participants displayed in Teams meetings is known as a gallery. Teams creates a tile for each participant to display their video feed. If the user disables their video feed, Teams uses the photo from the user's account or their initials if no photo is available. Galleries have three view options:

- The **default gallery view** shows nine tiles in a 3x3 arrangement. If more than nine participants are in a call, Teams prioritizes those with video turned on and highlights the current speaker. If more than nine video-enabled participants are in a call, Teams shows the most active speakers in the tiles. The default gallery view is available to all clients except the browser client on Firefox, which can only display a 2x2 view. Teams meeting recordings use the 3x3 view. Further optimization happens for

users who join a meeting in a Teams Room with their personal workstation. Because the user can physically see the room device and other people in the room, Teams does not display the room video or the video feeds for other in-room attendees in the gallery.

- The **large gallery view** uses a 7x7 view (organized in pages) with navigation controls to move between pages of meeting participants. The default gallery view also supports navigation between sets of video feeds. Both desktop and browser clients support the large gallery view. The Teams client switches into the large gallery view when more than ten participants in a meeting have their cameras on.
- **Together mode** is available in meetings with more than five participants. The difference between Together mode and the gallery view is that the gallery shows tiles for participants while Together mode uses artificial intelligence to isolate the head and shoulders from the video feed for each participant before combining the feeds in a background scene. According to Microsoft, active participation increases when large meetings use together mode. Meeting organizers and presenters can select a background to place people into from a set provided by Microsoft, including some suitable for large meetings (like an amphitheater) and others suitable for smaller gatherings (like a boardroom). When they enable together mode, meeting organizers and presenters can choose *Select Together Mode for Everyone*. This option applies together mode with the selected scene for all participants. New participants join in together mode with the selected scene. Participants can switch to the regular gallery mode if they prefer.

Teams dynamically adjusts the view available to meeting participants based on factors such as the number of attendees, who enable their video and who uses audio only, available bandwidth, the client used and its configuration, the active speakers during meetings, and when people share content during the meeting.

Here's how using dynamic view affects what attendees see:

- Tiles for attendees with video feed enabled appear differently to those who only use an audio feed. Audio participants appear in smaller tiles (a reasonable call because a set of initials or a static photo in a circle isn't very visually compelling).
- To make sharing easier, dynamic view allocates more space to content shared in a meeting, like a presentation, app, or whiteboard.
- Users can pin or spotlight selected attendees to make their cards larger than those of other participants.
- The together mode view can appear alongside content.
- Users can "dock" the gallery of attendee cards on the top of their screen.

Special processing highlights sign language interpreters when used within meetings. To make it easier to follow the interpreters, they remain in a fixed location on the meeting stage and Teams displays them in a higher video quality (if possible). Sign language view is a user-specific setting and doesn't affect what other meeting participants see.

Dynamic view aims to make meetings more visually interesting than the flat gallery views used in the past. The hope is that user attention and engagement will be higher because Teams adjusts the view to concentrate on the most important content in the meeting.

Customizing Together Mode: Tenants can [create and package new background scenes for Together Mode in the developer portal](#) (here's a [description of how to build a new scene](#)). This capability requires a Teams premium license.

Background Effects: Images and Blurring

No one likes distracting other meeting participants with a video feed of a messy office. To help people disguise messy surroundings, they can use a background filter in personal and channel meetings. Background filters work by isolating the image of a user from their video feed and replacing the background with either:

- **Background blur:** The computer blurs the user's surroundings. Teams supports standard blur and portrait blur. The difference is that standard blur applies a much heavier obscuration mask on your background. Portrait blur highlights the person without blurring quite so much of the background.
- **Custom background image:** The computer merges the user's image with a background image. The user can select an image from a standard set provided by Microsoft, or use a custom image obtained from another source and uploaded to the workstation (or mobile device). In effect, the mechanism works like a video green screen.
- **The green screen effect** uses a preselected backdrop color to remove items from the user's background before merging the user's image with the background. Any items that do not match the backdrop color are also visible.

If their camera is on, users can select a background filter through the pre-join screen or by using the **Apply background effects** option during a meeting. **CTRL + Shift + P** is the Windows keyboard combination to invoke this option.

To apply the chosen filter, Teams works out what part of the image is the user and what forms the background, and then applies the filter to the background. On Windows PCs, the ability to apply background filters depends on the workstation having a chipset with AVX (Advanced Vector Extensions). Filters and effects based on AVX cannot be used with Mac computers with M1 or M2 chips. Background effects are unavailable for people using Teams VDI.

Background Filters Policy Setting

The ability for users to choose background filters is controlled by the *VideoFiltersMode* setting in the Teams meeting policy assigned to an account. The available options for the *VideoFiltersMode* setting are listed below with the values used to update the policy with PowerShell given in parentheses:

- **Off (NoFilters):** No filters are available.
- **Only background blur (BlurOnly):** Background blur is available (but only if certain hardware conditions are met).
- **Only background blur and default backgrounds (BlurAndDefaultBackgrounds):** Background blur and the set of curated background images selected by Microsoft can be used.
- **All Video Effects (AllFilters):** All filters are available, and the user can upload and remove custom images. This is the default value for meeting policies.

You can change the background filter setting by updating a Teams meeting policy in the Teams admin center. Alternatively, you can update the *VideoFiltersMode* setting for a meeting policy by running the PowerShell *Set-CsTeamsMeetingPolicy* cmdlet. For example, this command removes the ability to use background filters from any user who receives the *RestrictedFunctionality* meeting policy:

```
Set-CsTeamsMeetingPolicy -Identity RestrictedFunctionality -VideoFiltersMode NoFilters
```

Two standard filters designed to improve the appearance of users in video meetings are unaffected by the policy setting. The brightness filter lightens a participant's image in the video feed to make it clearer when the lighting in the area where they sit is dark. The effect is much like using a ring light. The soft-focus filter smoothens facial wrinkles and lines to make them less distinct. The filter works better for some people than it does for others. The filters can be enabled before joining a meeting or while the meeting is in progress.

Standard and Custom Background Images

The basic Teams license allows the use of two types of background images:

- **Standard images.** A set of curated background images chosen by Microsoft. These images are stored on a content delivery network (CDN) to make them available to all users. If you choose one of the standard images, Teams downloads a copy of the image to the device. Sometimes users can't reach the CDN to access the standard images. Usually, this is because of a VPN or other network restriction. To test, try and access one of the standard Teams background images, like [the contemporary office scene](#).
- **Custom images.** You can upload your JPEG or PNG images using the Teams client or by copying the files to the following folders.
 - **Windows desktop:**
C:\Users\userx\AppData\Local\Packages\MSTeams_8wekyb3d8bbwe\LocalCache\Microsoft\MSTeams\Backgrounds\Uploads
 - **Mac desktop:** /users/<username>/Library/Application Support/Microsoft/Teams/Backgrounds/Uploads (you may need to hold down the Option key before you choose Go from the Finder Menu to get the Library to appear).
 - **Mobile clients:** The iOS and Android clients allow users to upload their images to local storage.

When you browse the set of available images, Teams shows the standard images first followed by custom images (blur is a standard image). The images appear alphabetically within their respective folders. Users can remove images they upload by hovering over the image and selecting the Remove option. Organizations cannot remove standard images from the gallery. After a user selects a background filter (blurring or image), Teams displays that effect for every meeting they join with video-enabled until the user selects a new filter.

Microsoft publishes suitable images for use with Teams in a [public custom backgrounds gallery](#). Other companies create their custom background images for use with Teams and other conferencing software, and some release the images for public use (Teams can use images released for Zoom). Two examples are the images [made available by IKEA](#) (a major Teams customer) and [Star Wars](#). A collection of free-to-use background images intended for use as [PC wallpapers is available online](#). You can also download and use the images used on the Bing home page using [this PowerShell script](#).

Microsoft's guidelines for custom background images are that images should be a minimum of 360 x 360 pixels and a maximum of 2048 x 2048 pixels. Images at the minimum size will look horrible. Images with a 16:9 ratio sized at 1920 x 1080 pixels (the default size used by Microsoft and other sites) with the resolution scaled to produce files of around 1 MB are best. Files can be larger in both pixels and size as the uploading process will downscale them to fit. To generate the best images, you should size and crop images instead of leaving it to the computer to decide. When displayed in a video feed, the operating system will adjust the image to fit the screen display. Depending on the shape of the screen, some of the images might not be visible at the edge. To avoid problems, make sure that the important part of an image is in the center.

If you use Teams on several workstations and want the same custom background images to be available everywhere, you must load the images onto each workstation. Although they can control the level of access users have to background filters, tenants cannot mandate the use of a standard image.

Mobile Client Support

The Teams iOS client supports the ability to apply different background effects to the one-minute-long video clips sent to chats and channel conversations. The available options are:

- Select an image from the iOS picture library. Custom images used with the desktop and browser clients are only available if copied to the picture library.

- Apply heavy or light blurring to the current background.

Video messages created by the iOS client posted to a chat are treated like other video messages (see other section). Those posted to channel conversations are stored in the channel folder in SharePoint Online and play in the Stream video player.

Animated Backgrounds

Animated backgrounds are like regular background images except that some parts of the image move slightly. Animated background support is currently limited to a small set of images supplied by Microsoft.

Organization Images

Organization or corporate images are enabled through the Teams Advanced Communications add-on and Teams Premium license. Tenant administrators can upload images in the meeting policies section of the Teams admin center. The images appear before the Microsoft-curated set of standard images in the image gallery. If a user selects an image, Teams downloads it from the cloud to the same folder used to store custom images and uses it as the meeting background. The Teams desktop and mobile clients support organization images. See [this article](#) for more information.

Video Effects

The video stream for a user comes from their workstation camera, with or without a background effect. Video effects augment a video stream by applying a style (for instance, generating a black and white version of the stream) or by adding some elements to the stream (applying a frame). The Custom filters app enables a basic gallery of styles and frames produced by Microsoft. The app is enabled by default in commercial tenants and disabled for education tenants. Normal app permission policies control access to the Custom filters app: if someone cannot access the app, they cannot use video effects.

The architecture for video effects supports third-party apps that make new video effects available in meetings. The first such app is the Snapchat Lenses app. The second is the Maybelline beauty app. User access to these apps is like any other Teams app. The app must be unblocked in the Teams admin center and not blocked by a permissions policy.

Noise Suppression and Spatial Audio

The device settings in user profiles include controls over how Teams suppresses background noise during a meeting. Available for the Teams Windows and macOS desktop clients and the iOS mobile client, noise suppression uses the CPU to process background noise around the meeting participant using the device to eliminate background sounds like paper rustling, reverberation, or fans. The higher the level of suppression, the more computer resources are consumed. You can choose from:

- **Auto:** Teams manages background suppression and tune it up or down depending on the level of ambient noise.
- **Low:** Use this level when music or a low consistent level of noise is present in the background.
- **High:** Teams uses the maximum level of noise suppression. Someone working in a very noisy environment might select this setting.
- **Off:** Teams doesn't use background noise suppression.

The setting in a user profile becomes the default for all meetings. If needed, you can select a different setting during a meeting from the Devices option in the meeting menu.

Teams processes noise suppression for the audio feed from the device to the meeting. It does nothing to improve the sound received by headsets or phones. To ensure the best quality sound in meetings, use a Teams-certified device. Teams does not apply noise suppression to audio feeds for recorded meetings

(suppression is applied to the recording as a whole) or when live captions are used. For noise suppression to work, the client must be able to access the <https://aiinfrastructure.static.microsoft/> endpoint.

Spatial audio also consumes device resources to ensure that meeting participants hear the voices of other participants coming from their relative position on the meeting screen. In other words, if someone shown on the right speaks, the user hears their voice in the right-hand earphone. Spatial audio requires USB earphones connected by wire (not Bluetooth) or the device speakers. The meeting must be viewed in gallery mode to allow Teams to calculate the relative position of people. If the device runs low on resources, Teams will throttle spatial audio to reduce the strain on the system.

Mesh Avatars

[Mesh avatars](#) are digital representations of users that are somewhat based on their actual appearance (or as close to as the mesh avatar app can get). Currently in preview and available for meetings in the desktop and browser clients, users can decide to replace their real image as captured by the workstation camera with their avatar. A user can have up to three avatars, each with a different appearance (body shape, hair, clothes, skin tone, and so on), to use in different types of meetings. A video feed can combine avatars with background images and do not remain static during meetings. Avatars react to audio and "twitch" from time to time to provide some visual interest. If the user wishes, they can select a gesture (like applause) for the avatar to communicate or express emotion during a call. Avatars are only available in the home tenant and don't appear when users participate as guests in meetings hosted by other tenants.

Maintaining Focus During Meetings

A busy Teams user can receive multiple notifications during a meeting to inform them of @mentions, replies posted in chats, and so on. These notifications can become disruptive and distracting during meetings. Two controls are available to help. First, a user can opt to mute notifications during all meetings by selecting this option in the Meetings and Calls section under Notifications in Teams client settings. Second, if they prefer to control notifications on a meeting-by-meeting basis, they can use the *Mute notifications* option (in the [...] menu) during a meeting. This option disables notifications for the current meeting. An *Allow notifications* option restores notifications for the current meeting.

Teams displays the video feeds from individual users on cards in a gallery during meetings. User feedback revealed that the presence of a user's video feed in the set of cards shown in the gallery can distract and become a source of anxiety for some users. To resolve the issue, meeting participants can select their card and then use the Hide for me option from the [...] menu to transform their card into a chevron. Everyone else in the meeting sees the user's video feed as normal. By clicking the chevron, the user can restore their video feed and display it in their gallery.

Music Mode

Teams music mode leverages [the Satin codec](#) to transmit high-fidelity sound in meetings and calls. When music mode is used, Teams adjusts the sampling rate automatically up to 32 kHz at 128 kbps using the available bandwidth to deliver the best possible sound quality (the transmission of acceptable human voices requires a much lower bitrate). The lowest bitrate for good quality sound is 48 kbps. Because sound quality is linked to available bandwidth, Microsoft recommends that you use music mode only when connected to wired networks.

In environments like a studio with low background noise and microphone control, users (including guests joining calls in other tenants) can control the audio stream further by turning off noise cancellation and disabling echo cancellation if using closed-back headphones. If using professional microphones with external

gain adjustment, you can disable the auto-adjust microphone sensitivity setting. Microsoft recommends that you don't use Bluetooth headsets with music mode.

The important thing to realize about using music mode is that you must enable the feature in Teams settings before you join a call or meeting. You can also decide to enable echo cancellation, noise cancellation, or auto-adjust microphone sensitivity. If you forget to enable music mode before starting a call, you'll have to leave the call, enable music mode, and restart. With music mode enabled, you'll see a music note symbol in the control bar to toggle music mode on and off. You can leave music mode enabled for the entire meeting or turn it off once the music finishes to reduce the demand for bandwidth and codec processing. In addition, music mode doesn't suppress background noise as well as regular mode does.

Using Whiteboard in Teams Meetings

Whiteboard is an application intended to allow people to collaborate by drawing and refining ideas on a digital canvas (a board), or as Microsoft says an "*infinite canvas where imagination has room to grow.*"

Whiteboard runs as an Azure service and is enabled by default for all Office 365 enterprise tenants. If you want, you can disable Whiteboard through tenant settings in the Microsoft 365 admin center.

Users can access Whiteboard through the Office menu, which launches the [browser version](#), signing in with their account credentials to create, update, or remove boards. Versions of Whiteboard are also available in the Microsoft Store and [for iOS](#) and [Android](#).

Whiteboard in Teams is installable as [an app in a channel tab](#). It is also available in the share tray for Teams meetings. When invoked in a channel tab or meeting, you can choose to open Whiteboard in Teams or use the app (if installed on a Windows PC). If your PC supports digital inking, you can draw with your finger or a digital pen on a board, which works surprisingly well. Whiteboard includes support for note grids, has a wide range of colors for sticky notes, ink, and highlighting, along with templates designed to get ideas flowing, and can insert content from PowerPoint presentations stored in SharePoint Online and OneDrive for Business or links to content on external sites. The same capabilities are available in the Teams, Windows, or browser clients.

When you create a board for a meeting, it is associated with the meeting and all meeting participants can access the board during the meeting and afterward (the whiteboard is a meeting resource). Because a board is a common resource that everyone connects to, changes made to the board appear everywhere in real-time. Guest members can interact with boards during a Teams meeting, but full guest access to the Whiteboard service isn't currently available.

Often a discussion centered around a board will conclude that you want to share with other people who weren't in the discussion. A Post to Teams option is available in the Windows app to post a link to the board as a message in a selected channel. The link can be copied from Teams and used to share the board with other people via email or in a personal chat. Clicking the link opens the board in the app (if installed) or the browser. You can only share boards with other tenant users. It's also possible to invite other users to collaborate in Whiteboard through sharing invitations sent via email. The link can be read-only or allow full write access. When the recipient accepts the invitation, Whiteboard adds the board to their list of available boards and opens the board to allow them to contribute immediately. Invited users aren't allowed to delete boards.

If you don't want to send a link to allow access to a board, you can save a static view of a board as a graphic file (PNG format) and include the file in an email, document, or web page.

All boards created in Teams meetings are stored in OneDrive for Business and have the same "Whiteboard meeting" name. To avoid confusion, you can use the app to select a board in the list of boards and edit it to

assign a more meaningful name. For now, Whiteboard content is not captured by Teams compliance records, nor is the content indexed and available to content searches and eDiscovery cases.

Teams isn't limited to Whiteboard when it comes to discussing ideas on a digital canvas as [other brainstorming applications](#) are available in the Teams app store.

Meeting Reactions

Teams meetings allow attendees to react to whatever's happening in the meeting with a set of four emoticons. Like how the virtual hands-up feature works, the attendee selects the emoticon they wish to use (like a laugh or thumbs-up) and sends it. The reaction is visible to others on their attendee card or, if someone is presenting or sharing information at the time, reactions float up from the bottom of the screen.

Some organizations don't like meeting reactions. You can disable the ability of users to send reactions through the *AllowMeetingReaction* setting in the Teams meeting policy assigned to meeting organizers. In this example, we disable reactions for meetings organized by anyone assigned the default meeting policy:

```
Set-CsTeamsMeetingPolicy -Identity "Global" -AllowMeetingReactions $False
```

Note that meeting organizers can override the meeting policy by editing the settings of a meeting to allow reactions.

Meeting Polls

Meeting organizers and presenters of personal meetings can create simple single-question polls with up to six answers and make them available to attendees before and during meetings. Polls aren't supported for channel meetings or live events. The Microsoft Forms app for Teams is used to create and manage polls and the app must be added to a meeting before polls are available.

Polls can be published to attendees before and during meetings. When published during a meeting, users of Teams desktop and browser clients see the poll questions in a pop-up notification in the middle of the meeting window and can respond there. Teams publishes the poll as a card within the meeting chat, where it can be accessed by Teams mobile clients. Polls can be opened and closed as needed during a meeting and the results are displayed to users as responses come in unless the poll is marked as anonymous. Once complete, poll results can be exported and downloaded in an Excel worksheet.

Meeting polls are stored as a personal form in the user's account and can be accessed to view results through the Forms app (the forms used by Teams polls are read-only in the Forms app).

Teams Webinar

A Teams webinar is a special form of meeting created when a user selects *webinar* from the drop-down *New meeting* menu in the calendar app. Teams webinars support:

- Online events for up to 1,000 people.
- Registration controls for participants (some of the controls like waitlist, the ability to send follow-up messages to webinar participants, and manual approval require the organizer to have a Teams premium license).
- Custom theming for the registration page (Figure 11-14) and email notifications. The organizer can upload a banner image and logo for Teams to use.

Along with the normal meeting functionality, a webinar has a sign-up page created by the organizer to allow internal and external participants (if open to the public) to register for the event. The organizer can customize the sign-up page to collect information about attendees such as their name, company, and position. The webinar organization can add custom text, choice, or checkbox fields.

A webinar is an online event like a Teams meeting. Presenters and co-organizers receive calendar invitations to the event. Those who register through the sign-up page receive email containing the event details (including an .ics file). Teams keeps registration and attendance reports to allow webinar organizers to compare those who signed up with the eventual attendance.

Teams event policies in the Teams admin center control who can create webinars and the settings of webinars, including who can attend webinars (internal only or including external participants) and the ability to create town hall events. Teams Premium licenses support an enhanced set of capabilities, including the ability to operate a wait list. See the [Microsoft documentation](#) for more information.

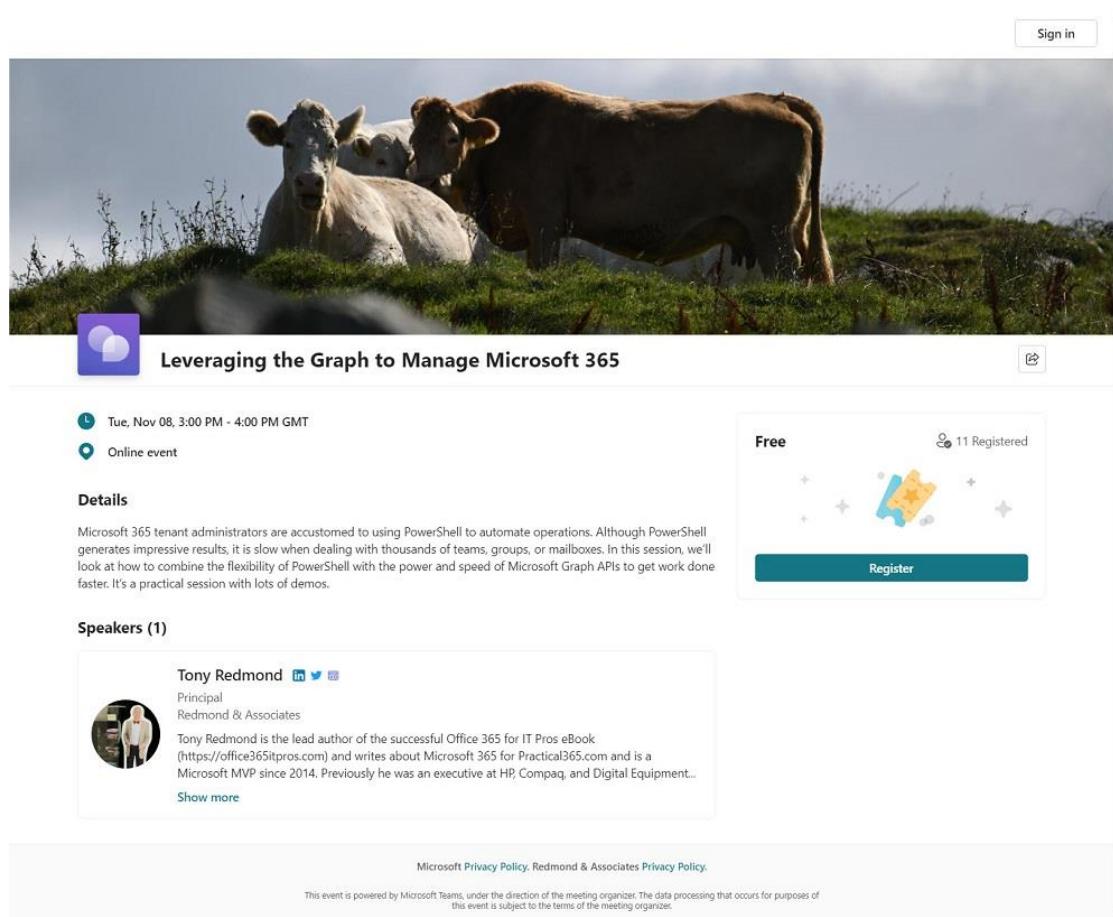


Figure 11-14: A customized webinar registration page

Breakout Rooms

Breakout rooms allow a Teams meeting to be split into several subordinate meetings (the breakout rooms) linked to the main meeting. The feature is designed to support scenarios like brainstorming sessions, online classes, and corporate events which often start by assembling all the participants to set the goals before dividing into smaller groups to work on specific issues, and then come back together to report findings and make decisions. The basic flow for breakout rooms is:

- A meeting starts as normal. The meeting organizer chooses the breakout rooms option in the meeting control bar to create the number of breakout rooms needed for sub-groups. A meeting organizer can add or remove breakout rooms after the meeting starts, up to the maximum of 50 rooms. To make their purpose clear, breakout rooms can be renamed. For example, a group working on a corporate merger might have breakout rooms for Finance, HR, and Legal. Meeting organizers can predefine breakout rooms including room assignments before a meeting starts.

- The meeting organizer assigns meeting participants to the different rooms. This can happen manually or automatically (Teams divides participants evenly among the available rooms). Organizers can move users between breakout rooms, including using a “participant shuffle” to randomly assign users to rooms.
- After assigning participants to breakout rooms, the organizer uses the Start rooms command to allow the participants assigned to each room to begin work. It’s possible to open rooms individually if you don’t want them all to begin at the same time. A setting controls whether people are moved automatically into their assigned rooms (the default) or receive a prompt to join. Those assigned to a breakout room cannot add other people – this can only be done by the meeting organizer.
- The organizer can set a countdown timer for the rooms. When the timer expires, participants rejoin the main meeting or leave the meeting.
- Participants meet in the breakout rooms and use normal meeting functionality such as chat, app sharing, turn on together mode, and collaborate with a whiteboard. To encourage people to participate, everyone in a breakout room is assigned the presenter role.
- The meeting organizer can visit the breakout rooms to help keep everything on track. When they join a breakout room, the organizer can work with the other participants.
- The meeting organizer can also make announcements to all breakout rooms. For instance, they might send a note to remind people that the breakout rooms will close in five minutes and that someone should be nominated to present findings. Announcements are posted to the meeting chat in each open breakout room. If participants in a room need to contact the meeting organizer, they can send an @mention message in the chat.
- To bring the meeting back together again, the organizer closes the breakout rooms (or the countdown timer expires). After a short delay, the participants from the breakout rooms rejoin the main meeting. If necessary, the organizer can reopen a breakout room to allow people to restart discussions. Attendees cannot close breakout rooms.
- After wrapping everything up with the complete set of participants, the organizer ends the meeting.
- Separate meeting chats and notes are kept for each room and the main meeting. Separate recordings and transcripts can be captured for each breakout. Access to the information shared or generated in a breakout room is limited to the participants in that room. For instance, if a file is shared in the Finance breakout room, the permissions on the file uploaded to the sharer’s OneDrive account are restricted to the people in the breakout room at that time. In the future, Microsoft says that it will be possible to share information more easily from a breakout room with the main meeting.

Managing breakout rooms depends on the pop-out meeting and chat experience, so the desktop client must be used by meeting organizers. Participants can use the desktop, browser, or mobile client. The ability to use breakout rooms in meetings depends on several settings in the Teams meeting policy assigned to the meeting organizer. See [this article](#) for more information.

It’s not always the case that those who schedule meetings are the people who run the meetings, and it’s also possible that a meeting creator might not be available when the meeting happens. To avoid the obvious issue that the meeting organizer is the only person initially allowed to manage breakout rooms, Microsoft says that it will be possible to assign multiple organizers in the future.

Real-Time Streaming from Teams Meetings

Teams personal (not channel) meetings support real-time streaming of content to streaming platforms like YouTube via the Real-Time Media Protocol (RTMP). The essential steps are:

- Create a suitable video feed within a meeting, using background images and other effects (like the brightening filter).
- Load the Custom Streaming app into the meeting.

- Get an RTMP URI and an RTMP key from the target streaming platform to identify the content coming from Teams.
- Connect Teams to the target streaming platform.
- Deliver the content and terminate it from Teams or the streaming platform when it's complete.
- Perform any post-production you want on the video before making it available long-term on the streaming platform.

The process is quick and easy and can be accomplished using regular PC hardware. Naturally, you can increase the quality of the video output by adding a better camera, lights, and microphones. It's a great way of making events like webinars and product announcements available from Teams to a public audience. See [this article](#) for more information.

Teams Live Events

A live event is a structured form of meeting intended for large-scale information dissemination such as company announcements, product launches, training, and so on. The ability to present is limited to those assigned the presenter role; attendees are limited to listening and interacting through moderated Q&A. Organizers can create events with live captions and subtitles, including [the ability to translate spoken words into captions shown in multiple languages](#). Live events support recordings. Those invited to events can play back recordings for up to 180 days after the event finishes. Recordings are not stored in Stream, but they can be [downloaded by event producers](#) and then uploaded to Stream.

Microsoft originally intended to retire Live Events on September 30, 2024 and replace Live events with [Teams Town Hall](#), Microsoft is in the process of building out the functionality of Teams Town Hall to achieve feature parity with Live Events. Progress in this respect has not been as fast as anticipated, and on May 28, 2024, [Microsoft announced](#) that they would not proceed with the planned retirement of Live Events. It's obvious that Live Events are on the way out, but the exact date is now uncertain.

Two types of Teams Live Events are available: quick start and external encoder (see below). Anyone equipped with a PC and webcam can create and run a quick start live event with audio, video, screen sharing, application sharing, and QA. These events, also called "produced with Teams," are limited in terms of the video quality and the type of information presented during the broadcast (for example, no overlaid graphics), but the output is more than good enough for many topics.

Teams Live Events are created in the Teams calendar app in a similar way to a personal or channel meeting. Instead of *Schedule meeting* (the default), select *Live event* from the **New meeting** drop-down menu. The person who creates a live event is called the organizer or producer. Event organizers must meet the following criteria:

- Their account is assigned an enterprise license (E3 or E5 or academic/government equivalent).
- The assigned license must include Teams and Stream. The need for a Teams license is obvious. Behind the scenes, Teams uses Stream for all the necessary video processing including storage, caption and transcript generation, and delivery of content in formats suitable for different devices.
- Their mailbox must be hosted in Exchange Online.

Setting up a Teams live event is straightforward. You can limit event attendance to:

- Specific people and groups.
- Organization-wide (anyone who can sign into your tenant can attend, including guest accounts).
- Public. Anyone can attend and no sign-in is required. These events are designed for public briefings and presentations.

When creating a live event, the organizer decides to produce the event using Teams, meaning that the content for the event comes from presenter workstations, or using an external app or device. The former

option is sufficient for internal meetings while the latter uses an external encoder (see below) to create more of a TV studio-like event, complete with special effects. The event recording is automatically available to the organizer and presenters. It is then up to the organizer to make the recording available to attendees via a website or another repository. You can choose to add captions in the spoken language translated in up to six other languages. Other options control the generation of an attendee report and if attendees can ask questions during the event. Q&A is not like the interaction chat used in other Teams meetings; attendee questions go through a moderation process before they become public (visible to event attendees).

Notifying Event Participants

Presenters automatically receive calendar invitations generated when the event is created. These links contain the special links to enable the presenter role during the event. Sometimes event organizers forget to send out notifications to their intended audience to tell them how to join the event. To do this, copy the deeplink for the event and paste the link into an email (use a standard non-Teams meeting invitation to have the event inserted into recipient calendars).

The reason for sending the deeplink generated for the live event via email or a calendar invitation is simple: distributing the deeplink like this avoids the possibility of including two sets of join information in the invitation (one for the live event, the other for a regular Teams meeting).

Live Events Policy Settings

Teams supports anonymous access to live events, but only if this is allowed by the live events policy assigned to the person who organizes the event. If the event permissions allow, anonymous attendees can access the event recording. Live events policies are managed in the Teams admin center.

The settings controlling public access and disable recording for download are both off by default. To enable these settings, go into Live events policies in the Teams Admin Center and change the global policy or create a new policy with these settings enabled and assign them to specific users. You can also control these settings in PowerShell using the `Set-CsTeamsMeetingBroadcastPolicy` cmdlet. For example:

```
Set-CsTeamsMeetingBroadcastPolicy -Identity Global -BroadcastAttendeeVisibility Everyone  
-BroadcastRecordingMode UserOverride
```

Live Event Presenters

Unlike regular meetings, where everyone can speak, share their video feed, and chat, only people assigned the organizer and presenter roles can speak, present information, and be visible during live events. Presenters can be:

- Tenant accounts.
- Guest and federated users.
- Anonymous external accounts. These are accounts without an Entra ID or Microsoft (MSA) account. If you want to use anonymous presenters for an event, you must set the [Allow external presenters](#) toggle when creating the event.

Attendees can ask questions, but only through a moderated Q&A facility. Because attendees have limited functionality in live events, the number of participants is much higher than for normal Teams meetings. The structured nature of Live Events means that some preparation is necessary to ensure the delivery of the best possible event. Steps to ensure a smooth event include:

- Having a dress rehearsal to make sure presenters understand the flow of the event and how they transition to speak. Presenters must join the event by signing into the host tenant. If they are a guest in that tenant, the presenter must switch to the host tenant before they join; if not, they will join as an attendee.

- Projecting an “Event will start soon” slide complete with information about the event and some music from five minutes before the event is scheduled to begin. This will reassure attendees that they’ve connected to the right event and will be able to hear the proceedings.
- Beginning the event with “house rules” to let attendees know how to ask questions and how presenters will respond to questions. During the event, someone should monitor incoming questions and note those that a presenter should answer. Moderators can reply to other questions straightway while other topics might need later follow-up.

Recordings

Organizers can record live events for later playback. The recording is stored in Stream and accessible for up to 180 days after the event, which makes it convenient for people to replay an event later and listen to specific parts of the discussion. Event organizers can download the recording and upload it to Stream if they want to keep it for a longer period. Live events can also be live-streamed to platforms like YouTube and Facebook using an encoder like [OBS Studio](#) (an open-source encoder).

Teams Live Events External Encoder

Largescale live events which need output of the highest quality are usually carefully-planned productions created with studio-quality recording, camera, and broadcast facilities. These events often involve external encoder software to connect to studio production equipment.

The hardware or software-based encoder must support streaming to a Real-time Messaging Protocol (RTMP) service. Supported encoders include Haivision KB, OBS Studio, Wirecast, and XSplit Broadcaster (here is a [link to the encoders](#) tested by Microsoft and a [write-up](#) by MVP Luca Vitali on how to set up external encoder integration with OBS Studio).

Teams Calling

Teams is the preferred communications solution for Microsoft 365 and supports two methods to enable users to make, receive, and transfer calls to landline and mobile phones connected to public networks (PSTN). You can buy Phone system licenses with a [calling plan](#) (various plans are available in different countries for national and international calls), in which case the phone numbers assigned to users come from a pool assigned and managed by Microsoft. Alternatively, you can use [Direct Routing](#) (or direct connect) to link Teams to your existing connection to the PSTN network via a Session Border Controller (SBC). The technology for Teams calling comes from the Microsoft Phone System (originally called Cloud PBX). Finally, you can use Operator Direct Connect. These options are covered in the Teams Calling and Devices chapter.

Users must have a Microsoft calling plan to place calls to PSTN numbers. Accounts without a calling plan can call other Teams users using VOIP, including those in other tenants. The Teams Calling and Devices chapter contains detailed information about how to deploy and manage the foundational elements for voice and audio meetings, including calling inside and outside the organization.

End to End Encryption for Teams Calls

Teams secures VOIP traffic with Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP). The combination is sufficient to secure most voice traffic, but if users need an extra degree of protection for ultra-confidential calls, the Teams Windows and Mac desktop clients can use end-to-end encryption (E2EE). In this scenario, the workstations at both sides of the conversation agree on an encryption key that they use to secure the call. Because of the additional layer of encryption, some Teams calling features don’t work, including call transfer, recordings, and live captions. However, E2EE calls support chat.

By default, the Teams enhanced encryption policy for the tenant disables E2EE calling. To enable E2EE, an administrator must:

- Update the default policy to allow users to make E2EE calls, or:
- Define a new Teams enhanced encryption policy that allows E2EE calls and assign the policy to specific users.

In this example, we update the default Teams enhanced encryption policy to allow users to make E2EE calls.

```
Set-CsTeamsEnhancedEncryptionPolicy -Identity Global -CallingEndtoEndEncryptionEnabledType DisabledUserOverride
```

Setting the policy to *DisabledUserOverride* allows Teams to display an option to use E2EE calls in the Privacy section of client settings.

If both users in a call enable E2EE, their call will be in E2EE mode, they'll know that this is happening by checking the shield icon at the top left-hand corner of the call screen. If it has a lock, E2EE is in force. Clicking the shield icon reveals a set of five 4-digit codes which should be the same for both users.

Viewing Organizational Information

If the **Show organization tab for users** setting (in the Teams settings section in the Teams admin center) is **On**, users can view the organizational information about tenant users by:

- Searching for their name, and then selecting the organization view.
- Typing /org followed by their name in the command box.
- Hovering over their people card.

The screenshot shows the Microsoft Teams People card for Sean Landy. At the top, there is a circular profile picture of Sean Landy, his name 'Sean Landy', and some basic details: '+ Pronouns' (he/him), 'Chief Happy Person', and 'Information Technology'. Below this are icons for email, phone, and LinkedIn.

Below the card, there are tabs: Overview, Contact, Organization (which is selected), and LinkedIn.

The 'Organization' tab displays the following information:

- A box for 'Tony Redmond', Chief Executive Officer, Global HQ.
- A box for 'James Ryan', Chief Story Teller, Information Technology, with a right-pointing arrow indicating more details.

Below these boxes, a section titled 'People reporting to James Ryan (13)' lists the following users:

Profile Picture	Name	Title
Jeff Guillet	Jeff Guillet	Chief ExPTA
John Jennings	John Jennings	
Ben Owens (DCPG)	Ben Owens (DCPG)	Chief bottle washer
Marc Vigneau	Marc Vigneau	Architect
Eoin Redmond (Ireland)	Eoin Redmond (Ireland)	Sales Manager
Benjamin James (IT)	Benjamin James (IT)	Senior Architect (Development)
John C. Adams	John C. Adams	Manager
Sean Landy	Sean Landy	Chief Happy Person
Chris Bishop	Chris Bishop	Director of Product Managem...

Figure 11-15: Viewing organizational information for a user

Like other Microsoft 365 applications, the people card reveals some personal information about the user such as their title, phone number, and if set, their email out of office message and their Teams status message. The people card also has links to a set of tasks:

- Switch to a personal (1:1) chat.

- Send a quick message to the person.
- Email the person. In this case, Teams launches the default email program configured for the device (for example, Outlook) with a new message addressed to the person using their email address defined in their Microsoft 365 account.
- Start an audio call with the person.
- Start a video chat with the person.
- View their organization information.

The organizational information about a person (Figure 11-15) comes from the reporting relationships, job title, and other information held in their Entra ID account. The information is only as good and as accurate or complete as it is in the directory, so it's a good idea to invest effort in populating and maintaining the directory. As mentioned in the User management chapter, it's important to maintain information about user accounts in Entra ID to ensure a high level of directory accuracy for consumption by applications like Teams.

When viewing information about a person, you can also see details of personal chats you have had with them (Chat), if you share files from your OneDrive for Business site with them in a 1:1 chat (Files – documents shared in group chats do not show up here), and recent posts from them to channels in teams to which you belong (Activity). Guests can only see the Conversation and Activity tabs.

Presence and Status

Teams keeps two indicators about someone to help users understand the current situation for that person.

User presence shows their availability to connect and appears in the user's people card and profile picture in places like the activity feed. **User status** is a free-text message configurable by the user for Teams to display to others.

User Presence

User presence is set in two ways:

- **User-configured:** The user picks a status and sets it in the Teams client. The presence values are Available, Busy, Do Not Disturb, Be Right Back, Appear Away, and Appear Offline. Users set their presence status by entering a command in the command bar (for instance, `/dnd` is the shorthand code used to set your status to *Do Not Disturb*) or by clicking their picture in the top right-hand corner and setting their presence there. Federation allows guest users to see user presence. If Teams cannot determine someone's online presence, Teams shows their presence status as "Offline." Users can also set their presence to Offline if they want to appear unavailable and uncontactable to other people. Teams supports the ability to set a duration for a presence, meaning that you configure a presence to last for a period from 30 minutes to a future custom date (for instance, after you return from an extended vacation). When the presence duration lapses, Teams reverts to an app-configured presence. You can't use the Available status when you set a duration.
- **App-configured:** A presence status chosen by a user always has priority and Teams uses this status whenever possible. If the user doesn't set their presence status, Teams tries to determine a presence based on their activity. For example, if someone is in a meeting or a call, Teams knows this and can change their presence status to reflect this activity. Teams synchronizes out-of-office information and calendar data with the user's Exchange mailbox and uses this information to figure out their status and current presence. For instance, if the user blocks some time in their calendar for an appointment or meeting and marks the time as busy, Teams knows that they are unavailable during their period. Time blocks booked by Viva Insights for "focus time" cause Teams to automatically set a user's presence to Do Not Disturb. In addition to synchronizing calendar data, when a Teams client is signed

in, it uses the [Graph presence subscription API](#) to detect calendar updates to take new events into account when calculating the user's presence.

Teams publishes presence changes immediately (or very soon afterward) following an update. When someone's presence is set to Do Not Disturb, Teams does not deliver notifications for normal messages and @mentions, while continuing to deliver notifications for urgent messages or those from people on the user's priority access list (managed in the **Privacy** section of **Settings**).

If someone is waiting for another person to become available, they can select that person and use the notify when available feature to have Teams watch the person's presence. Once the status changes to available, Teams sends a notification to let the user know that the person is available. The notification is only advisory and no automatic attempt is made to connect the two parties.

See [this page for more information](#) about the icons displayed by Teams to reflect a user's presence status. Of course, just because Teams reports someone as being available doesn't mean that they are. They might just be asleep!

User Status Message and the Profile Card

Teams shows a user's profile card (Figure 11-16) when users hover over their profile picture in chats and conversations. The profile card is also referred to as the Live Persona Card, or LPC. It contains:

- User information: Name, job title, department.
- Current presence status as calculated by Teams.
- User status (see below).
- Local time for the user and the time difference between the user and the person viewing the profile card. This information comes from the user's calendar time zone setting. Local time information is available for guest accounts if a federated organization sharing policy to share free/busy calendar information exists with their home tenant. Users can update their calendar time zone through Outlook settings, or administrators can run the `Set-MailboxCalendarConfiguration` cmdlet. See [this article](#) for more information.
- Primary SMTP email address.
- Fixed and mobile phone numbers.
- Physical office.
- Direct reports and manager.
- If the user defines their work locations for the week using OWA settings, the work location (Office or Remote Location) for the current day is included in the profile card. Users can update their work location for the current day by clicking on their profile photo. This action has no effect on the settings defined in OWA.

The user profile card consumes information stored in Entra ID and the user's Exchange mailbox. The information displayed will be inaccurate if the properties of the user account are incorrect, or the settings defined for OWA are wrong.

In addition to the information Teams extracts from Entra ID, users can publish their personal status message. This is a free-form 280-character value status message intended to give other people a more descriptive insight into their status. To update the status message in the desktop and browser clients, click the user photo in the top right-hand corner and select **Set status message**. Plain text and emojis are usable in a status message. Mobile clients support setting the status message through the user menu (top left-hand corner). When a status message is available, Teams displays it under the user's photo.

Like the presence status, a user status has a lifetime, which can be Today (until midnight), 1 hour, 4 hours, This week, Custom, or Never (the status never expires). After its lifetime expires, Teams removes the status

message. Users can choose for Teams to display their status when someone sends them a message or @mentions them in a message. In these cases, Teams displays the status message over the compose message box. It also displays a reminder about the status message and its lifetime in chat.

In Figure 11-16, the user's presence is set to *Appear Away*, and their status gives some information about their ability to respond to messages. The people card also shows when the user was last active in Teams.

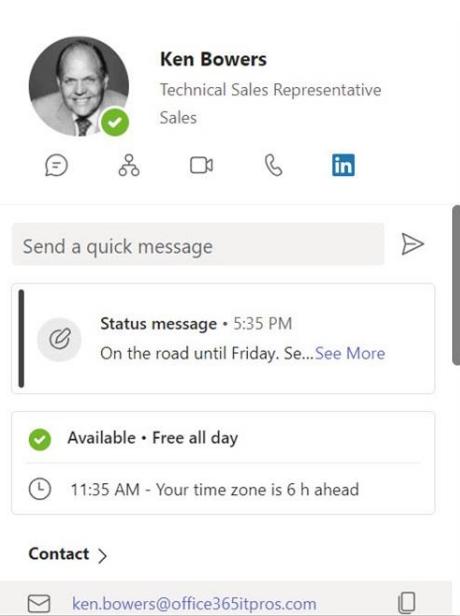


Figure 11-16: The user profile card holds lots of information

If an Exchange out of office notification is set for a mailbox, Teams includes this information in the people card unless the user explicitly sets a status message. If the user creates an out of office notification first, it takes precedence until the user clears the notification in Exchange. On the other hand, if the user sets their status in Teams first, subsequently setting an out of office notification in Exchange won't overwrite the status. Guest users can see the status message for other users in host tenants, so it's not a good idea to include anything confidential in a status message. Users can set the Exchange out of office notification from the Teams desktop and browser clients to update the mailbox autoreply configuration to make sure that all clients use the same settings.

Guests can also set a status message, and they can set a different message in each tenant where they have an account. The status message set by federated contacts in other tenants aren't available during chats.

User Photos: In the User management chapter, we cover how to upload photos for user accounts. Teams uses the 64 x 64 pixel version of the user photo in most places (like the user profile picture in the title bar or the images displayed alongside messages) and the 96 x 96 pixel image in the LPC. The LPC appears when someone hovers over someone's profile picture. Teams caches the 96 x 96 images for 60 days. When the cached images expire, Teams makes a network call to fetch the latest version. Signing out and back into Teams clears the cache and causes Teams to request new LPC images.

Files: Linking Teams and SharePoint Online

The process to create a new team includes provisioning a new SharePoint Online team site containing a document library with a folder for the General channel. The purpose of the folder is to hold documents posted to the General channel. The creation of a new channel also creates a new folder of the same name in the document library. Users access the contents of the document library through the **Files** channel tab. This is one of two default tabs created for every channel that team owners or administrators cannot remove or rename.

Accessing the Files tab opens the folder holding channel files. Team members can upload documents to the folder or drag and drop files from File Explorer or the Mac Finder to move items into the folder. Naturally, any files created in the folder through the SharePoint browser interface or using Office apps are also available. Users can edit Word, Excel, and PowerPoint documents within Teams or open the file with the Online version of the app. The editing experience is similar but opening the file with Office Online or the desktop application allows the user to continue to do something else with Teams during the edit.

The Files tab supports navigation to sub-folders belonging to the channel, but if users want to move to another folder in the document library, they can click **Open in SharePoint** (available in the Files tab or the [...] menu for Posts) to open the site with SharePoint's browser interface. They can then access other folders in the document library, such as the folders belonging to other channels, or, if you team-enable an existing group, folders previously created in the default document library. It's important to understand that Teams does not integrate other document libraries in its navigation. If a site spans multiple document libraries that you'd like to access from Teams, you need to create individual channel tabs pointing to the root folder of those libraries (see below).

Another example of where you might create a channel tab pointing to a SharePoint resource is where you want to expose the site Recycle Bin to users to allow them to recover items deleted in error.

Using Tabs to Access SharePoint Resources

To enable access to other SharePoint resources from within Teams, you can add tabs to bring users directly to a specific folder in a document library, a list, or a page in the SharePoint site belonging to the team. Here's how:

- Select the channel you want to make SharePoint resources available to team members, and then click the plus sign (+) to invoke the **Add a tab** dialog. Now select the **SharePoint** tab to add a link to a document library, published page, or list in a site. You can add links for SharePoint content in the site belonging to the team or any other site in the tenant, providing that team members have access to the content.
- If you select Document library, you can select a document library from the team's site; or select **Any SharePoint site** and input the URL to the library you want to make available through the tab. The easiest way to get the URL is to open the target location in a browser and copy the URL from there to Teams. Make sure that team members have the necessary permissions to open the target.
- Give a name to the tab to help users understand its purpose (you can rename the tab later if necessary) and then **Save**.
- If you select the SharePoint tab, Teams retrieves a set of available pages to choose from. Select the page in the team site to display (for example, Home or News) and **Save** the setting. The tab will take the name of the chosen page (you can rename the tab if you want to).

An example of linking to a specific page is when you want to publish news articles to Teams. You can bring news articles into Teams as cards created by the News connector, but if you link to the News page for the site, you see all the news items posted, including the web parts (images, etc.) used for each item, and can comment on an item. In other words, you can interact with the page instead of just seeing a static snapshot of the content.

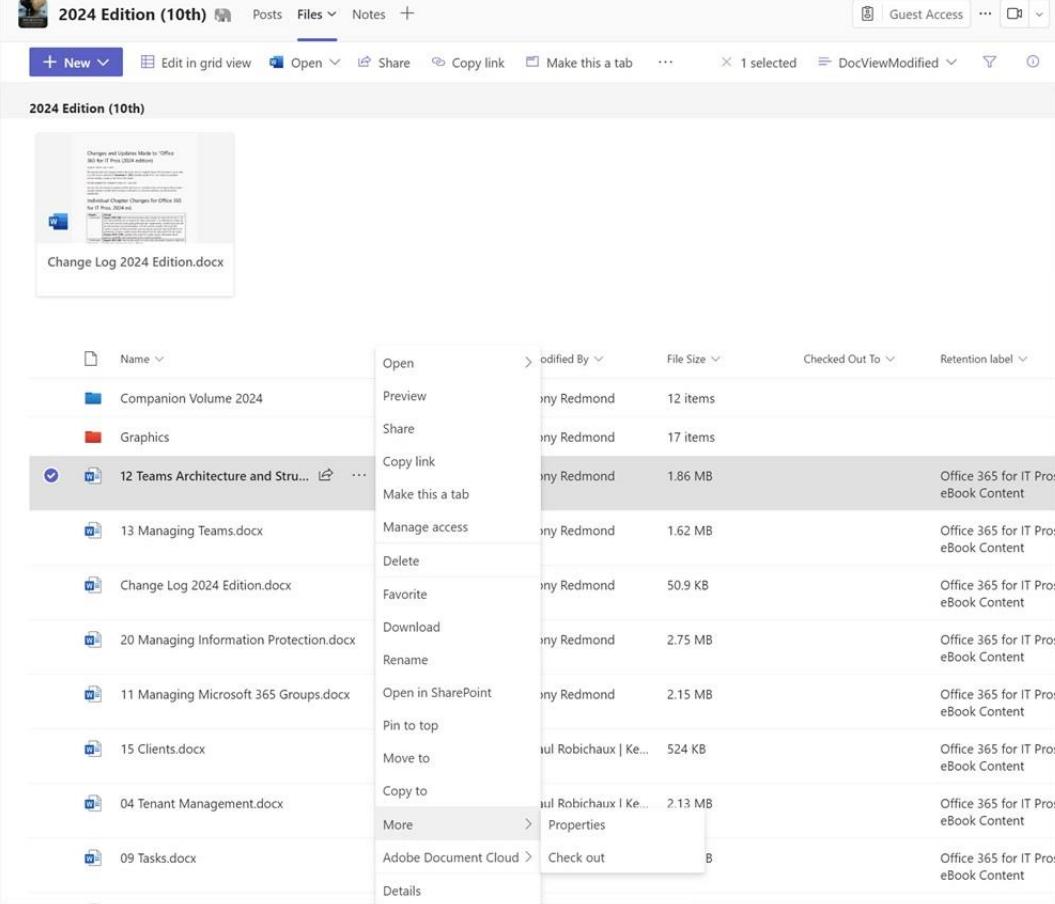
The Files Channel Tab

The Files Channel tab is a standard tab available for all channels to enable access to the files stored in the folder belonging to a channel in the team's SharePoint Online document library. Figure 11-17 shows the source Word documents for this book. The original version of the Files channel tab presented a simplified view of documents when compared to the view available in the SharePoint browser interface. Microsoft has

made steady progress towards the goal of giving the Files tab parity with the browser interface, and the two are much closer now, with support included for features such as column formatting and customization. By default, Teams uses the OneDrive file viewers to open and work with files. For Office documents, users can configure clients to open files as follows:

- Desktop: Use Teams (the viewers), Office Online, or desktop apps. Only the latest version of the Office apps (Office 2016 or later) is supported.
- Browser: Use Teams or Office Online.

The Files channel tab lets users open, move, copy, rename, download, and delete files to work with documents without the need to open the SharePoint browser client. You can also check out documents. Co-authoring is supported because Teams supports both the [WOPi](#) and [FSSHTTP](#) protocols.



The screenshot shows the Microsoft Teams interface with the 'Files' channel tab selected. At the top, there's a navigation bar with 'Posts', 'Files', 'Notes', and a '+' button. Below the navigation bar, there are several action buttons: '+ New', 'Edit in grid view', 'Open', 'Share', 'Copy link', 'Make this a tab', '...', 'Guest Access', and 'DocViewModified'. A status bar at the bottom indicates '1 selected' and '1 item modified'.

The main area displays a list of files in a SharePoint document library named '2024 Edition (10th)'. The list includes:

Name	Open	Last Modified By	File Size	Checked Out To	Retention label
Companion Volume 2024	Preview	ony Redmond	12 items		
Graphics	Share	ony Redmond	17 items		
12 Teams Architecture and Struc...	Copy link	ony Redmond	1.86 MB		Office 365 for IT Pros eBook Content
13 Managing Teams.docx	Manage access	ony Redmond	1.62 MB		Office 365 for IT Pros eBook Content
Change Log 2024 Edition.docx	Delete	ony Redmond	50.9 KB		Office 365 for IT Pros eBook Content
20 Managing Information Protection.docx	Favorite	ony Redmond	2.75 MB		Office 365 for IT Pros eBook Content
11 Managing Microsoft 365 Groups.docx	Download	ony Redmond	2.15 MB		Office 365 for IT Pros eBook Content
15 Clients.docx	Rename				
04 Tenant Management.docx	Open in SharePoint	ony Redmond			Office 365 for IT Pros eBook Content
09 Tasks.docx	Pin to top				
	Move to	paul Robichaux Ke...	524 KB		Office 365 for IT Pros eBook Content
	Copy to	paul Robichaux Ke...	2.13 MB		Office 365 for IT Pros eBook Content
	More >	Properties			
	Adobe Document Cloud >	Check out	B		Office 365 for IT Pros eBook Content
	Details				

Figure 11-17: The Files channel tab displays files in a folder in a SharePoint document library

Some limitations exist in the Files tab compared to the SharePoint interface. For example, you can't access the version history for a document, so you can't restore a previous version. You can't add a Flow or an alert to a document. In these cases, you're forced to open the library in SharePoint to perform these actions. It's worth saying that Microsoft has steadily closed the functionality gap between the Files channel tab and the SharePoint browser interface over the years to a point where the channel tab delivers the features most users need to work with documents.

Tenant users can synchronize files in the SharePoint document libraries used by Teams just like any other SharePoint site. The situation is different for guest users, where a OneDrive for Business feature called [B2B Sync](#) must be used to allow guest accounts to synchronize documents.

Disabling the Files Channel Tab

Some organizations prefer to use non-Microsoft file storage. You [can enable cloud storage for individual users](#) using services like Box, Dropbox, Dropbox for Business, Google Drive, Egnyte, and Citrix ShareFile. Teams apps are available for Box, Egnyte, and ShareFile to allow users to manage content in these repositories within Teams. Organizations that focus on non-Microsoft file storage can instruct Teams not to display the Files channel tab by using a Teams Files policy. The policy controls two settings:

- **NativeFileEntryPoints**: Default enabled. If disabled, Teams removes the options to upload files from OneDrive for Business, other cloud storage services configured for the user account, and SharePoint Online (Teams and channels).
- **SPChannelFilesTab**: Default enabled. If disabled, Teams does not display the Files channel tab in any channel. However, Teams continues to configure SharePoint sites for new teams and folders in the SharePoint sites for new channels.

For example, to see the current Files policies defined in the tenant, run:

```
Get-CsTeamsFilesPolicy
```

```
Identity          : Global
NativeFileEntryPoints : Enabled
SPChannelFilesTab   : Enabled
```

Only one policy exists, the global (default) policy. You could update it to affect the Files behavior for all users, but it's usually better to create a custom policy and assign it to user accounts. For example, this policy disables both files settings and assigns the new policy to a user account:

```
New-CsTeamsFilesPolicy -Identity DisableFilesChannelTab -SPChannelFilesTab Disabled
-NativeFileEntryPoints Disabled
Grant-CsTeamsFilesPolicy -PolicyName DisableFilesChannelTab
-Identity Lotte.Vettler@office365itpros.com
```

Fifteen minutes or so after applying the policy to user accounts, Teams will respect its settings.

SharePoint Site Membership

You should let Teams manage the membership of the SharePoint sites connected to teams. If you are a SharePoint expert and understand the consequences of making changes to site membership, feel free to do so. However, remember that if something doesn't work afterward, you will have to support what you've done.

Another thing to consider is that Microsoft might synchronize site membership between Teams and SharePoint in the future. This happens for private channels today where every four hours (approximately) Teams synchronizes membership of the private channel to SharePoint and overwrites the existing site membership. In other words, if you change the site membership in between synchronizations, Teams will reset the membership the next time synchronization occurs.

Sharing Links

The **Copy link** option creates a sharing link to the folder belonging to a channel or a selected document. The organization's sharing policy for SharePoint Online dictates which types of sharing links are available for use. See the SharePoint Online chapter for more information about sharing links.

To use a link, click **Copy link** and then adjust the link settings to control who can use the link, if they can edit the file, and so on. When the link is ready, click **Copy**. The sharing link is then available in the clipboard. You can then paste the link into a chat or email and send it to the intended recipients.

Tabs to Link to Specific Documents

Apart from tabs connected to SharePoint sites, team owners can add tabs for fast access to a selected document. Open the SharePoint library with Teams, select the document, and then use the **Make this a tab** option. Teams creates the tab to point to the document. Alternatively, add a tab and then select the file type (Word, PowerPoint, etc.), and then select the document you want from the document library belonging to the team (you cannot select a file from another document library). When you create a tab for a file, selecting the tab invokes an Office viewer to display the content of the file. You can also edit the file in either the online app or by launching the desktop app if it is available on the workstation.

OneDrive in the Navigation Rail

The **OneDrive** link in the left-hand navigation rail exposes a different set of files to the Files tab for a channel. Instead, the default (Recent) view for this link lists the recent files worked on by the user stored in SharePoint sites and their OneDrive for Business site. Some other shortcuts appear under Files:

- **Home** reveals a list of files in SharePoint document libraries belonging to teams that the user recently accessed. Guests do not see this link.
- **My Files** shows the set of files in the user's OneDrive for Business account.
- **Shared** shows the set of folders and files that the user has shared with other people.
- **Downloads** shows files downloaded from web sites.

If you connect a **cloud storage service** to Teams, like Google Drive, a shortcut to that service appears in the Files section.

OneNote

When you create a tab in a channel to access OneNote, you have the choice to create a new notebook, browse to find existing notebooks to link to the tab, or paste [a notebook link](#) to bring users to a specific notebook, or a section, page, or paragraph within a notebook.

Sharing Files

When someone shares files in a public conversation, Teams captures copies of the files in the folder of the group document library for the channel. However, when someone shares files in a private chat, Teams first uploads the file to a folder called "Microsoft Teams Chat Files" (under the Files folder) in the owner's OneDrive for Business site and then shares it with the other chat participants.

SharePoint News Connector

SharePoint news items are a special form of web page created in a SharePoint site. The SharePoint News Connector creates notifications about news items in a channel after they are posted. You can only create notifications for news items posted to the SharePoint site belonging to a team. News items posted to other sites are ignored. After the notification messages appear in the channel, users can click on a message to go to the full news item in the SharePoint site or use the item to begin a conversation.

To create a connector, select the SharePoint News app (adding it if necessary) to the team. You then select the target channel for news items. Teams creates a webhook to connect the site with the channel and any time afterward someone publishes a news item on the site, it appears as a channel post.

Email Folders

If people send an email to a channel, the email travels through a connector. SharePoint Online captures copies of the messages sent through the connector in sub-folders of the channel folder, created as needed on

a month-by-month basis. For instance, messages sent to a channel in July 2022 are in the *EmailMessages_7_2022* sub-folder of the channel folder.

Cloud Storage

If allowed by the Teams settings for the tenant, the Files tab supports access to different cloud services such as Dropbox, Box, Egnyte, Citrix ShareFile, and Google Drive (including personal drives) that the tenant might use instead of OneDrive for Business or SharePoint. The process of connecting to a cloud service means that you provide credentials to connect to an account in the service and use that account to select a folder in the storage accessible to the account. Once configured, a link to the cloud service appears in the list of files. Users must be able to authenticate with the external service and access the files in the chosen storage location. Once connected, users can view, edit, upload, and remove files managed by the cloud service. They can also start a new conversation about a file in cloud storage, just like they can discuss files stored in SharePoint.

Teams for Frontline Workers

Teams for Frontline Workers is a Teams-based app built by Microsoft to replace the old StaffHub app. Designed around the premise that frontline staff such as sales associates and construction workers are often organized into scheduled periods of work activity, the app is also known as Shifts. In addition to the app, the [Shifts Graph API](#) is available for organizations to integrate Shifts into existing workforce management tools. Neither the app nor the API is available in the free version of Teams.

All Teams clients support the Shifts app. To access the app, click the More apps (...) button in the Teams navigation menu and look for the app in the Teams app store. It is also possible to assign a [Teams app policy](#) to selected users so that Shifts shows up in the app bar (along the side in the desktop and browser clients, at the bottom for mobile clients).

Inside Shifts, team owners can select a team to host a schedule and begin creating shifts (periods of work) and worker categories (called groups) to organize the shifts. Like a calendar, you can view shifts by day, week, or month and see which of the members are already scheduled and those who are still available. Because the schedule is built around the people defined by team membership, a team can only support a single schedule. If you need to maintain several schedules, you must create a team for each schedule.

After creating a schedule, team owners and members permitted to manage schedules can assign members of the team to shifts and note absences such as scheduled vacations. To make things easier to build a schedule, you can copy the data for an existing shift from a previous period. If you add someone to a shift who isn't already a member of the team, the app adds them to the underlying group. Although Shifts allows you to create a schedule for a dynamic team, you shouldn't use these teams with Shifts. Two problems are apparent. First, if the query against Entra ID changes the team membership, some shift assignments might be affected. Second, if you try to add a new user to the team and assign them some time slots, Shifts accepts the assignments, but the person is not added to the membership and so can never see the schedule.

After populating the shift with assignments, you use the **Share with team** button to publish the information to the team. Publication can be to the complete team or just those who are affected by any changes made to the schedule since it was last shared. Sharing notifies team members that details of a new schedule are available. Members then open the Shifts app to review their schedule and request any adjustments they might want to make. For example, someone might want to ask for time off, or swap one of their scheduled shifts with someone else. These requests go to the team owner, who can approve or deny the requests.

Can Teams Replace Email?

Although messaging is an important part of Teams, it's obvious that other parts of the app are equally if not more important to different people. Meetings and calls, for instance, became the most important part of Teams for many organizations during the Covid-19 pandemic, while the development of Teams as an app platform has been remarkable. Nevertheless, some proponents of Teams focus on messaging and believe that you can reduce the use of email within an organization by replacing email with chat and channel conversations. Among the advantages cited for this approach are:

- Conversations and documents exist in the team rather than in multiple mailboxes. Thus, users have just one place to find information. Conversations are in channels while documents (including attachments in emails sent to the channel) exist in Files (a SharePoint document library).
- Conversations do not fork. It is easy for a small subset of recipients to begin a separate conversation after receiving email. This does not usually happen inside a channel because the conversation stays there and is visible to all team members.
- The volume of email declines when some traffic moves to Teams and email evolves to serve different purposes. Internal conversations stay in Teams while email handles external communications that Teams cannot handle (because no way exists to send outbound email from Teams). If necessary, people can initiate internal conversations by sending emails to a channel and continue the discussion in the channel from that point.
- Group chats are a good way to get together small teams of people to dissect and understand a problem before bringing a decision to a wider audience.

The advantages its supporters envisage for Teams are aspirational, and no guarantee exists that everyone is willing to change the habits of a lifetime and move from their preferred email client to Teams overnight, even as Teams adopts some of the characteristics of email in features such as message moderation and auto-replies. It's also fair to say that it is as easy to create a chaotic mess of Teams conversations spread across a sprawl of channels as it is to create an unordered messy inbox. Much of the success in any transition to a new technology comes from the effort put into user training and support. Left alone, users will find their bad habits for Teams.

It's also important to consider how different email clients affect the transition. People often refer to their client and how they use it instead of the email application. Their view of email comes from how they use their client(s). Outlook desktop is a great case in point as many people have built their working habits around how Outlook functions. People who use simpler email clients, like the Windows Mail client or a POP3 client, are perhaps less likely to be quite so attached to their client.

Teams Messaging Can Work Better than Email

There's no doubt that Teams messaging (chat or channel conversations) can be a better tool to drive issues forward and get things done than email is. Take the situation shown in Figure 11-18 where a channel conversation has 269 replies and there are 207 members in the team. If the communication happened over email and everyone replied as they did to the conversation, 55,890 (1 topic + 269 replies x 207 recipients) messages would circulate among the team. Not only would people have to spend a lot of time deleting some of the thread messages unread, but they also must cope with out-of-office notifications. Finally, consider the length of the final message and the impossibility of navigating through all the appended replies, auto-signatures, and other junk to get to the gist of the conversation. A well-organized threaded conversation in one place is a much better host for fast-paced to-and-fro communications.



Figure 11-18: A Teams channel conversation with many replies

Channel conversations can be as chaotic as a cluttered inbox, especially when multiple team members contribute to different conversations over a short period. It can be very easy to lose sight of something important in a flurry of messages. It is also important to understand that Teams is an internal-facing collaboration mechanism. Even with guest users joining in, the data associated with Teams always remains in the home tenant. Compare this to the way that email serves as the lingua franca for the internet where anyone with an email server can use it to communicate and collaborate with anyone else. Another important factor to consider is the added functionality available in email, such as the ability to protect messages and attachments with rights management and encryption, not to mention features to make it easier for users to organize messages, like rules, categories, flagging items for follow-up, and so on. These features take years to develop and deploy, and Teams is still a young application.

Those who champion Teams should consider that all applications have their flaws. Among those seen in Teams are:

- Chaotic, badly organized conversations composed of short, incomplete, and shallow sentences that fail to form fully thought-out ideas. A conversation might have many replies from many individuals and be devoid of analysis and insight.
- Conversations that veer away from the subject at hand because they are hijacked by people who fail to understand the topic.
- Conversations can be dominated by the speedy, the quick-witted, those who have a point of view that they want (and need) to express, and those who suffer from verbal diarrhea. Some members of a team might choose not to contribute to a fast-paced conversation that, although open to them, is taking place between others.
- Conversations about anything that comes into peoples' heads that mask real work.
- Conversations about topics driven by people who have no authority to speak on a subject or no accountability for an outcome. It is truly amazing how easy it is to waste time in such discussions.
- A rush to decision based on a feeling that chats should develop quickly.
- The fear of losing out if you fail to keep pace with all the conversations that happen in all the channels in all the teams you belong to. Apart from flagging a conversation as important and favoring and following channels, it's hard to prioritize the firehouse of chats daily, let alone sort out what might have occurred when you return from a vacation.

Email can suffer from some of the same problems, but because your inbox is under your control, it can be easier to sort, ignore, prioritize, and respond to what flows into the inbox.

Some organizations will find the transition from inward-circulating email to Teams easy and some will decide that they are best off staying with email and favor Outlook Groups as their collaboration platform instead, especially when regulations or legal requirements dictate the use of some of the compliance functionality presently missing in Teams. Interestingly, it can be easier for users of other collaboration platforms, like Lotus Notes, to move to Teams than to break habits formed around Outlook.

Usage reports, such as those available in the Microsoft 365 admin center or the Teams admin center, can help you understand if any email traffic moves to Teams. However, when you examine usage data, remember that some traffic handled by Teams might replace conversations previously carried in other apps. It is also important to measure after the first burst of activity subsides and people start to use Teams consistently. You will then know whether overall traffic is static or growing and what modality is most popular with users.

Delegation of Access

Unlike many email systems, Teams does not support the concept of delegation of access for messaging, a feature that underpins common email functionality such as the ability for someone to:

- Send messages on behalf of or as (impersonate) another user.
- Schedule meetings on behalf of another user.
- Manage another user's workspace (their mailbox).

Teams is very different from email, so there's no reason why Teams should slavishly copy functionality from email systems across to its methods of messaging and collaboration. Nevertheless, the desire to move some volume of communications from email to personal chat and channel conversations plus the growth in Teams online meetings creates some need to support the manager-assistant scenario.

There's no good answer for delegation of access in Teams today, only workarounds. For more information, see [this article](#). Teams Calling does support delegation for call handling.

Other Email Strengths

Other areas of functionality where email is ahead of Teams include:

- Printing. Teams clients do not include the ability to print messages or the calendar.
- Single focus: If someone has guest accounts in multiple tenants, they must switch to each tenant to check chats, channels, and apps. Compare this to the single inbox for all new emails, no matter where they originate.
- Secure communications: Chats and channel conversations are excellent methods for internal communications that extend to some external communication through guests and federated chat. Teams messaging does not include the secure (protected) functionality commonly found in emails such as S/MIME or other encryption (like sensitivity labels).
- Complex messages: Email is better suited to composing longer and more complex messages of the type used for formal business communications.
- Calendar: Outlook's calendar is more functional than the version available in Teams.
- History: Email allows users to keep all messages if desired in online or offline locations.

Different people will assign different levels of importance to each of the points listed above. The important thing is to help users decide when it is best to use Teams and when to use email. Although messaging might seem to be a common thread, they are very different tools.

Can an Organization Cope Without Email?

Overall, it is hard to see Teams replacing email anytime soon. Teams is a great vehicle for communication, but if it wasn't available, organizations could continue to work with people inside and outside the company because other communication media exist, including email. If an organization decided to remove email, it could continue to communicate internally using Teams, but its ability to communicate externally with partners, clients, and other companies would be significantly and fundamentally reduced (in some cases, eliminated). With [over 3.9 billion users worldwide](#), email is ubiquitous, secure, and backed by a range of well-understood and widely-deployed standards. Moving on from such a foundation will be difficult.

Teams and Email Interaction

Because email isn't going away anytime soon, Teams includes several methods for the two modalities to interact:

- **Share to Teams** uses an Outlook add-in to send a message to a Teams channel or chat (including the ability to create a new chat). Share to Teams works with Outlook for Windows (Microsoft 365 apps for Enterprise), Outlook for Mac, and OWA. It isn't available on Outlook mobile.
- **Share to Outlook** is a Teams client option that calls OWA to create and send a message containing a copy of a channel or chat conversation. The message can go to any email recipient, including distribution lists and external recipients.
- **Chat with Teams** and **Reply with IM** are Outlook desktop options available when Teams is the registered chat application for Windows. Teams launches a pop-out chat window connected to the author of the selected message. Chat participants can include Teams users from other domains.
- **Reply to Teams Missed Activity Mail** gives users who receive missed activity notifications the ability to respond to conversations in Teams using [Outlook actionable messages](#).
- **Email-enabled channels** have special email addresses to allow the delivery of messages through a connector to become channel conversations. Organizations can restrict who can send email to an email-enabled channel. See the Managing Teams chapter for more information.
- **Drag and Drop from Outlook desktop** allows users to drag and drop a message (and any attachments) into a Teams channel conversation. The feature doesn't work with chat.

The Share to Teams and Share to Outlook features depend on cloud mailboxes, so users with on-premises Exchange server mailboxes or guest users cannot use the feature.

Share to Teams

The Outlook desktop client installs the Share to Teams add-in automatically when a user signs into the Teams desktop or Teams browser client. The add-in uses single sign-in to allow Outlook or OWA to post messages into target Teams channels, personal chats, or group chats. To share a message, click the Share to Teams icon in the Outlook menu bar. Outlook checks the connection to the user's home tenant (if the user switches to be a guest to another tenant, they need to switch back to use Share to Teams) and for the presence of the Teams desktop client. If the Teams desktop client is available, Outlook opens a window in the Teams client and loads the current message into a form to allow the user to add addressees (Figure 11-19). After someone uses the feature a few times, Teams learns about the people and locations commonly used for sharing and suggests these as potential sharing targets.

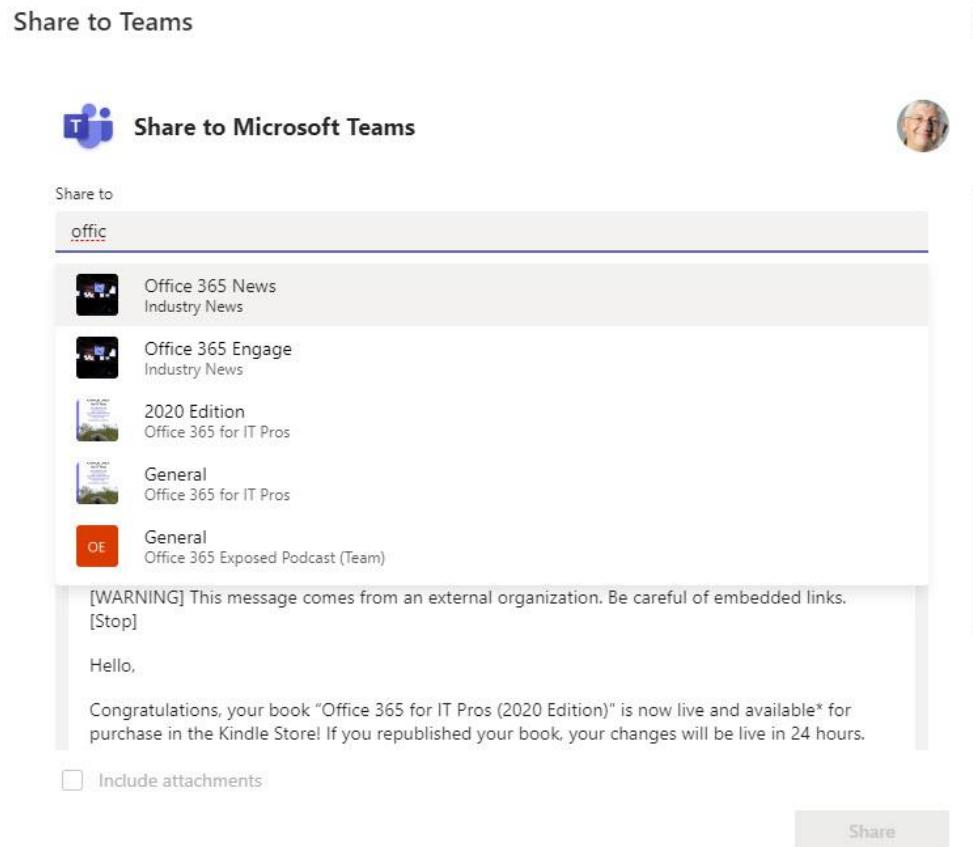


Figure 11-19: Selecting recipients to share an Outlook message with Teams

Valid sharing targets are:

- Individual users: Outlook posts the message to a private chat.
- Several users: Outlook posts the message to a group chat.
- Channels in Teams: This includes private channels the user belongs to. Posting to multiple channels is not possible.

To add context to the post in Teams, the user can insert some cover text to explain the message to the channel members. If the message has attachments, you can choose to include or omit these files. When the message is ready for posting, click **Share**.

Behind the scenes, Outlook shares messages through the same mechanism as used to post a message to a channel via email. Depending on the recipients, sharing creates a new topic in the target channel or a new message in a personal or group chat and posts the message. When Outlook posts a message to a channel, Teams saves the message and any attachments in the *Email Messages* folder for the channel in the SharePoint document library belonging to the team. Messages posted to a private or group chat are in the Microsoft Teams Chat Files folder of the sender's OneDrive for Business account. Teams shares these messages with the group participants to allow them access.

Share to Teams does not support messages encrypted with Microsoft Information Protection sensitivity labels, Office 365 message encryption, or S/MIME.

If you don't want users to use the add-in, you can disable it using PowerShell by running the *Disable-App* cmdlet. This code finds the identifier for the Share to Teams add-in and uses it to disable the add-in for a mailbox. If necessary, to disable the add-in for multiple accounts, use an input array of mailboxes and pipe the objects to the *Disable-App* cmdlet:

```
$ShareToTeamsApp = (Get-App | Where-Object {$_.DisplayName -eq "Share to Teams"}).AppId  
Disable-App -Identity $ShareToTeamsApp -Mailbox Chris.Bishop@office365itpros.com -Confirm:$False
```

Share to Outlook

Sharing to Outlook means “*forward a conversation from a Teams conversation or personal chat to one or more email recipients.*” To share, select **Share to Outlook** from the [...] menu, which only appears if the user mailbox is in Exchange Online. Guest accounts can’t use Share to Outlook because they don’t have a mailbox that they can sign into.

When you forward a personal chat, Teams shares the selected message rather than the entire chat. For a channel conversation, Teams extracts a copy of the complete conversation (this can be slow for a conversation with many replies). Teams loads the HTML content into an OWA message compose form for the user to add address information and make any changes necessary to the message body. If a user’s mailbox is not enabled for OWA, Teams won’t be able to call the OWA message compose form.

You can add any valid email address, and you can choose to send the message from any mailbox for which you have permission, including shared mailboxes and Microsoft 365 Groups. Because an OWA component creates and sends the message (unsent messages are in the Drafts folder), OWA features like support for sensitivity labels are available. And of course, email clients can print the messages sent from Teams, thus solving the lack of printing support in Teams clients.

Messages forwarded from Teams travel through the Exchange Online transport pipeline and are subject to any mail flow rules enforced there.

Reply to Teams Missed Activity Mail

Depending on a user’s missed activity email settings, Teams sends periodic email reminders to make sure that users know what’s happening in a chat or channel conversation, like being @mentioned. Teams missed activity notifications are actionable messages which include two action buttons:

- The **Go to conversation** button uses an embedded deeplink to open Teams positioned ready to reply to the message, much like users can join a Teams meeting from an Outlook calendar event.
- The **Reply** button opens a dialog to allow the user to reply to the Teams conversation without leaving Outlook. Being able to compose and send an inline reply to a conversation without having to switch context from email is especially valuable in terms of helping users to maintain focus. Actionable messages support only simple text replies (no attachments, emoticons, reactions, or text formatting). One of the nice things about this feature is that you can reply from email even when you have not signed into Teams in the tenant that hosts the conversation.

Outlook desktop, OWA, and Outlook mobile support actionable messages for Teams responses. Email clients that can’t process the JSON content within the message which defines the actions and the transactions with Teams to perform responses replace the two action buttons with a **Reply in Teams** button. This button works like the **Go to conversation** button in that it uses the deeplink in the message to open the Teams client. In addition, if someone is using Outlook desktop and is not signed into their home tenant with the Teams desktop client, Outlook offers only the Reply in Teams option. To restore full functionality, the user must switch back to their home tenant and then restart Outlook desktop.

A tenant can block actionable messages by setting *SmtpActionableMessagesEnabled* in the Exchange Online organization configuration to False. By default, this value is True, meaning that applications like Outlook can interact with actionable messages. To block this capability, run the *Set-OrganizationConfig* cmdlet:

```
Set-OrganizationConfig -SmtpActionableMessagesEnabled $False
```

The block affects messages generated by all Microsoft 365 workloads, including Teams.

Reply with IM

The idea behind the Reply with IM feature is simple. You receive an email in Outlook and instead of having endless rounds of to-and-fro replies, you continue the conversation in an instant messaging platform that's more suitable for an interactive debate. The Reply with IM option is in the [...] menu of Outlook's read message window or in the Respond section of the Outlook menu bar (Microsoft has a habit of moving these options around). Reply with IM launches a conversation with the sender while Reply All with IM includes all the recipients in the conversation.

To use the feature with Teams, a user must be:

- Configured in [TeamsOnly mode](#). The value of the registry key `HKEY_CURRENT_USER\Software\IM Providers\DefaultIMApp` should be "Teams." This value is set when you choose to register Teams as the chat app for Office in Teams settings. You can [update the registry using this script](#).
- Signed into the Teams tenant hosting the users you want to chat. In other words, if you want to chat with people from your home tenant, make sure that you sign in there.

There are some details to remember when using Reply with IM:

- If an existing chat with the recipients exists, Teams will use that. Otherwise, Teams creates a new chat.
- Teams doesn't take the message subject and use it to name the chat, even when it creates a new chat. Apart from the recipients, Teams copies nothing from the message into the chat, so you must cut and paste information from the message body into the chat if you want to provide context for the conversation.
- Reply with IM supports federated (external access) chat with Teams users from other Microsoft 365 domains. However, it does not support chat with Teams consumer users.
- If one of the message recipients is blocked for chats by Teams, you won't be able to send messages to the chat.
- If you are signed in as a guest to a Teams tenant where an external recipient is homed, Reply with IM can launch a conversation with that person.
- Rather bizarrely, if a shared mailbox is in message recipients, Teams includes the shared mailbox in the chat (you can clean things up by removing the shared mailbox from the chat).
- If the message recipients contain a group, Teams drops the group when it starts the chat.

Despite some oddities, Reply with IM works well and is a useful feature to have when a chat is a more appropriate host for a conversation than keeping it in email.

Drag and Drop from Outlook Desktop

Outlook for Windows supports drag and drop of a message and any attachments from any folder to a Teams channel conversation. You can't drag and drop a message to a personal or group chat and the feature isn't available in OWA or Outlook for Mac.

To get the message into Teams, Outlook uploads a copy of the message (as a .msg file) into the channel folder in the SharePoint site belonging to the target team and creates a link to the email in the Teams message. The user can then add extra context for the message, just like they would for any other attachment shared in a channel before posting. Users can also drag and drop messages from Outlook to the Files channel tab. This action uploads the message to SharePoint without creating a message in the channel.

SharePoint Online stores messages as .msg files. These are copies that preserve the structure of the messages. The viewers included in Teams and SharePoint Online only display the text of the message and don't support access to any attachments. If users want to see the attachments, they must download a copy of the .msg file and open it with Outlook.

Although Outlook can upload messages protected with sensitivity labels (or S/MIME or another protection mechanism) to Teams, users can't read the content unless they download the message and open it with Outlook. When this happens, Outlook can call the protection mechanism applied to the message to access its content. For example, if a sensitivity label with encryption protected the message, Outlook can obtain the necessary use license, check if the user has the necessary rights to view the content, and if so, decrypt and display the message.

Another way of handling protected email is to copy the decrypted text from Outlook and paste it into a Teams message. If you want to include the message header to show recipients, forward the message to someone (but don't send it) and copy the text inserted into the forwarded copy. Any attachments (which will also be protected) must be downloaded and posted to Teams separately.

Chapter 12: Managing Teams

Tony Redmond

Keeping Teams in Good Shape

Applications require management if they are not to fall into a state of utter chaos over time. Teams is no different. Here we discuss the tools available to manage Teams from the policies managed through the Teams admin center to day-to-day management tasks like creating and removing teams. We also cover guest user access to Teams and the compliance and auditing infrastructure that helps to manage the content stored in Teams.

Creating a Deployment Plan for Teams

Before describing different aspects of Teams management, it's worth listing the areas to consider in a deployment plan. Here are some things to consider:

- What **training** will you deliver to users? How will you keep that training updated to match what users see in the Teams clients?
- What training is available for administrators and team owners? How will you keep the training updated with new developments in Teams and Microsoft 365?
- Are the default settings for messaging, calling, and meeting **policies** appropriate, and if not, what changes are necessary? What method will the organization use to assign policies and what policies will different sets of users receive?
- Will you allow all users to **create new teams**, or will the organization impose control over team creation? If so, how can users request the creation of new teams, and who will approve their creation?
- Will you impose a **naming convention** for Teams? If so, what is an appropriate and useful naming structure?
- Are **org-wide** or similar large-scale Teams needed? If yes, who will manage these teams, and what is their purpose?
- Will you use the **Groups expiration policy** to control the retention of inactive Teams? This feature requires Entra ID P1 licenses, but it can be very helpful when managing large numbers of teams. Another policy to consider is the ownerless groups policy.
- Will Teams **affect how you use other applications** like SharePoint Online or Exchange Online? For instance, if you use a hybrid Exchange organization, do you need to upgrade on-premises servers or should you move some mailboxes to Exchange Online?
- Will you allow **external access** to Teams? If yes, will you use the Entra ID B2B Collaboration (guest accounts) or B2B Direct Connect (for shared channels)? How will you manage external access to confidential information held in teams? Will you require owners to validate the need for continued external access to their teams periodically?
- Do you need to migrate **meetings and voice applications** from other platforms? Will this affect the devices you use in meeting rooms or on user desktops? Do you need to invest in calling plans to allow users to make PSTN calls with Teams?
- How does Teams affect the **data governance framework** for the company? Will Teams be within the scope of data lifecycle policies like Data Loss Prevention, Retention, and communication compliance?
- What **first-party apps** will be used with Teams (Planner, SharePoint, Insights, OneNote, etc.) and how will users be trained to use these apps effectively?

- What **third-party apps** will be used alongside Teams and by whom? How is access controlled to these apps and how do they feature in the data governance framework?
- Will **workflows** be used with Teams? If yes, what purpose will these components serve?
- Will the organization invest in the development of apps, bots, and channel tabs for Teams? If yes, who will receive training and what training will they receive?

It's a long list that you should tailor to meet the needs of your organization. It's also important to realize that some of the defaults Microsoft chooses for Teams (such as allowing everyone to create new Teams) are there to accelerate the adoption of Teams instead of making long-term management easier. This is especially true for larger organizations where the number of Teams is more than a single administrator can remember. With that thought in mind, let's consider the details of how to approach the management of Teams.

Teams Management

The [Teams admin center](#) (Figure 12-1) is the focus of team and policy management. Because the admin center is under active development, some of the settings described here might not be the same as presented in your tenant. The Teams Calling and Devices chapter covers the settings for Teams Voice and the Phone system, including aspects such as calling plans, resource accounts, and holidays.

Name	Standard channels	Private channels	Shared channels	Team members
Exchange's Grumpy Old Pe...	5	0	0	31
Ultimate Guide to Office 365	11	0	1	11
Yammer Replacement Tea...	2	0	0	4
Microsoft To Do Tips and T...	1	0	1	2
Windows File Server Repla...	2	0	0	8
Company Forum	1	0	0	1
Sales Department team	3	0	0	4

Figure 12-1: The Teams admin center

Not only does the admin center allow tenants to manage the creation and maintenance of individual teams, but it also supports the management of a wide range of user and organization policies to control how different aspects of Teams work, such as messaging, meetings, and guest access. As explained later, while tenant administrators have full access to all the settings and policies, a set of Teams administrative roles is available for assignment to users to grant them the ability to manage specific parts of Teams. See the Tenant management chapter for more information on these roles.

Teams in the Microsoft 365 admin center: If you look at the Teams and Groups section of the Microsoft 365 admin center, you can apply the *Groups with Teams* filter to see the list of Groups in the tenant that are teams-enabled (a small Teams icon also appears in the Teams status column). You can edit details of

teams such as description, or membership through the Microsoft 365 admin center, but you need to use the Teams admin center or PowerShell to update team-specific settings.

The **Admin** app is available in the Teams app store. Microsoft created the app to help administrators of small to medium Microsoft 365 tenants manage Teams more easily. In these tenants, administrators often take care of Microsoft 365 as a whole, whereas in larger enterprises administrators might be more specialized. Also, in large enterprises, it's common to see the principle of account separation at work, where people use permissioned administrative accounts to manage Microsoft 365 and personal accounts to interact with Exchange Online, SharePoint Online, OneDrive for Business, and Teams. The app allows administrators to manage user accounts, teams, licenses, and some organization-wide settings for Teams. Although the Admin app is convenient for a limited set of tasks, management through the Microsoft 365 admin center and Teams admin center is often more effective.

How Teams Global Policies Work

Microsoft creates a default policy called *Global (org-wide default)* for most of the policies used to manage teams. The purpose of a default policy is to dictate how a certain aspect of Teams works, like messaging, meetings, or app setup.

The screenshot shows the Microsoft Teams admin center interface. On the left, there's a sidebar with various icons. In the center, a user profile for 'Ken Bowers' is displayed, including a photo, name, title ('Technical Sales Representative'), email ('Ken.Bowers@office365itpros.com'), and directory status ('Online'). Below the profile, there are buttons for 'Start a chat', 'Send email', and 'United States'. At the bottom of this section are tabs for 'Account', 'Teams', 'Voicemail', 'Meetings & calls', 'Teams devices', and 'Policies'. The 'Policies' tab is selected. To its right, a modal window titled 'Edit policy assignment' is open. This window contains a list of policy types and their current assignments:

Policy type	Effective policy	Assignment type
App permission policy	Global (Org-wide default)	Default assignment
App setup policy	App Policy 2	Group assignment (Teams)
Audio Conferencing policy	Global (Org-wide default)	Default assignment
Call hold policy	Global (Org-wide default)	Default assignment
Call park policy	Global (Org-wide default)	Default assignment
Caller ID policy	Global (Org-wide default)	Default assignment
Calling policy	Frontline_Manager	Group assignment (Teams)

Below this table, there are dropdown menus for selecting different policies for each category. At the bottom of the modal are 'Apply' and 'Cancel' buttons.

Figure 12-2: Editing the policies assigned to a Teams user

The default policies apply to all users until the organization creates a custom version of the policy and assigns that policy to some or all accounts. This mechanism allows a tenant to manage functionality on a user-by-user basis. Although you can edit the default policies to reflect the way that you want Teams to work for your organization, some administrators prefer to leave the default policies intact and create custom versions of Teams policies instead. They take this approach because they believe this gives them more control and avoids problems if Microsoft changes something in a default policy in the future. However, if you use custom

policies, remember that you must apply those policies to new accounts after creation. This is one reason to depend on the default policies whenever possible.

You can manage Teams with default policies applicable to all users or create policies with different settings and assign them to specific users using the Teams admin center or PowerShell, including batch policy assignments to process large sets of users. Individual accounts have a mixture of default and custom policies. In Figure 12-2 we see a user account assigned a mixture of default (global) and custom policies.

Changes made to user policies need to synchronize with Teams clients before they are effective. Normally, this process takes an hour or so, but it can take longer.

Microsoft Management of Default Policies

Microsoft manages default versions of Teams policies to support their ability to update policy settings for introduction of new functionality. A tenant uses the Microsoft versions of default policies until the first time an admin views or updates a default policy through the Teams admin center or PowerShell. When this happens, Teams copies that default policy to the tenant to allow the tenant to use a custom version of the default policy. From that point forward, any change Microsoft makes to the global policy will not affect the tenant because the custom version of the policy takes precedence.

As an example, Microsoft updated the default meeting policy to force external users to wait in the lobby before admittance to Teams meetings. They did this by changing the *AutoAdmittedUsers* setting to "EveryoneInCompany" and the *AllowPSTNUsersToBypassLobby* setting to False. The net effect was to allow only tenant users to join meetings without going through the lobby. Microsoft updated its copy of the default meeting policy, and the change was picked up by tenants that had never changed the default meeting policy. A tenant-specific version of a default policy always takes precedence over Microsoft's version. Therefore, Microsoft's update did not affect tenants who had their copy of the default meeting policy and any customizations applied by a tenant remained in force.

Teams Policies

Teams policies (which sound much more comprehensive than they are) control whether users are allowed to:

- Discover private teams.
- Create private channels.
- Create shared channels.
- Invite external users to join shared channels.
- Accept invitations to join shared channels hosted in other tenants.

Microsoft's usual approach is to enable new features in the default policy to make functionality available to users immediately after the release of new software. If you prefer a more phased approach that takes training and help desk preparation into account, you can disable features in the Teams policy until the organization is prepared for their introduction. Microsoft often exposes the setting to control a new feature sometime before releasing the feature to users, which means that administrators have the time to assess if they want to make the feature available.

To assign a policy to an account, choose the account, and then select the Policies tab. You can then edit the set of assigned policies. If the organization uses policy packages for policy assignments, you can select a policy package to apply to the account.

In addition to viewing policies on a per-user basis, some of the policies managed through the Teams admin center include the option to see user and group assignments. This is a useful way to find out the set of accounts that a selected policy covers. For instance, if you select meeting or messaging policies, you can select a policy and then click the View users link in the *Assigned to users* column to see the set of users that

have the policy. Another useful feature is the ability to select users from the list to update their policy assignments. If the tenant uses group policy assignments, a View groups link is available in the *Assigned to groups* column.

The Teams admin center also includes an option for bulk unassignment of policies. This feature is available through the Actions menu of the Manage users section and supports seven different Teams policies, including the messaging and meeting policies. You can select up to 500 user accounts to revert from a custom policy to the default (global) policy for the selected policy type. For instance, if the organization had a special messaging policy used by a group of users that is no longer valid, this is a good way to move those users back to the default policy in one step.

Frequently Changing Names for Policy Settings: The information about Teams policies set out here is intended to give readers a view about what features Teams policies can control. However, Microsoft changes the names of policy settings frequently and has done so since it first shipped Teams in 2017. As such, use this section as a guide and confirm the setting that you want to use by reading the online [Teams settings and policies reference](#).

Messaging Policies

New users automatically receive the tenant's default messaging policy. The messaging policy controls the actions a user can take when working with Teams chat and channel messages and can override team-specific settings. If you don't want to use the settings in the global policy, you can change them or can create new messaging policies through the *Messaging policies* section of the Teams admin center, which also includes the ability to assign different policies to specific users. For example, you might want to restrict the ability of some users to send voice messages. To achieve the goal, define a new messaging policy that disables voice memos and assign it to accounts you want to restrict.

A messaging policy includes the following settings:

- **Owners can delete sent messages:** Allow team owners to remove all messages from channel conversations.
- **Delete sent messages:** Allow users to delete messages that they sent in channel conversations.
- **Edit sent messages:** Allow users to edit the text of messages they sent to channel conversations.
- **Chat:** If you disable this feature, Teams hides the Chat app from the navigation bar and limits users to channel conversations. Removing chat takes a big piece of functionality from Teams (see below) and is not recommended.
- **Delete chat:** Allows users to delete entire chat conversations from their chat list. Other participants in the chat continue to have access to the conversation.
- **Read Receipts:** This setting can be enabled for everyone, turned off for everyone, or user-controlled. If user-controlled, users can choose to use read receipts in 1:1 and group chats (read receipts are limited to group chats with up to 20 participants).
- **Upload custom emojis:** Allows users to upload PNG or GIF files to create custom emojis.
- **Delete custom emojis:** Allows users to remove custom emojis from the set for the tenant. A tenant can have up to 5,000 custom emojis.
- **Translate messages:** Controls if users can translate messages from their entered language to the language of the user.
- **Giphy in conversations:** Allow users to add [animated GIF files](#) to conversations. Clients make connections to the Giphy service to fetch available files. The choice to use GIFs links to the content rating, which can be set to "Strict" (nothing offensive to young audiences), "Moderate" (parental guidance needed), and "no restrictions" (all bets are off).
- **Memes in conversations:** Allow users to add the [memes](#) available to Teams to personal or channel conversations.

- **Stickers in conversations:** Allow users to add the stickers available to Teams to channel or private conversations.
- **Create Voice messages:** Controls if users can create voice messages in chats, and channel conversations.
- **Immersive reader for viewing messages:** By default, people can view messages in Microsoft Immersive Reader. When the tool is used, Teams displays message text in a full-screen window. The text is enlarged to make it easier to read and the reader can also choose to have the text read for them in a male or female voice.
- **Remove users from a group chat:** Controls if users can remove another person from a group chat.
- **Send urgent messages using priority notifications:** Controls if users can send priority messages. The number of these messages that a user can send is limited by the license assigned to their account.
- **On mobile devices, display favorite channels above recent chats:** If set, this setting forces the iOS and Android clients to display favorite channels on the top of the screen.
- **Suggested replies:** Teams can use AI to analyze the context of a message and generate up to three appropriate responses. This feature is available only in one-to-one chats.
- **Chat permission role:** This setting applies when the organization is configured for supervised chat, usually in an educational environment.
- **Users with full chat permissions can delete any message:** This is a setting for what's known as supervised chat that usually occurs in the education sector. Users with full permission monitor the ebb and flow of chats and intercede to remove messages considered inappropriate.
- **Text predictions.** If on, Teams attempts to predict words to insert in chats.
- **Video messages.** Allows users to send video messages up to 1 minute long in chats.

Organizations with communication compliance policies can use the **Report a concern** setting (for PowerShell, this is the *AllowCommunicationComplianceEndUserReporting* parameter set with the *Set-CsTeamsMessagingPolicy* cmdlet) to allow users to report messages they believe to violate corporate policies. By default, the setting is True. The option to report a concern is available only for personal and group chats and not for channel conversations. See the Compliance chapter for details about communication compliance policies.

Whereas control is available to stop users inserting GIFs, stickers, and memes into conversations, no control is available to prevent the use of emojis into channel conversations or chats.

Disabling Chat

Disabling Chat through a messaging policy removes access to the Chat app throughout Teams, but this approach is not recommended. Disabling the Chat app means that users won't be able to:

- Collaborate with other Teams users on an ad-hoc basis, including both personal (1:1) and group chats. Losing the ability to use group chats means that people won't be able to discuss issues and resolve points among a small number of people before bringing the issues for a wider general review in a channel conversation.
- Use federated connections to Teams users in other tenants or Skype consumer users.

Guest users cannot be assigned Teams policies, so if you want to stop guests from using chat between themselves or with tenant users, you must disable Chat in the Guest access section in the Users settings.

Although some feel that it is a good thing to remove chat to force users to conduct conversations in channels, the experience of Teams deployments indicates that users are more likely to seek other options for personal conversations outside Teams, such as WhatsApp. Moving these conversations outside Teams impacts the effectiveness of the organization's compliance policy because chats are then not captured and available for eDiscovery.

Disabling Meeting Chat

Meeting chats are different from personal chats. A meeting chat is associated with a Teams meeting and is governed by the meeting policy assigned to the participants. The *Allow chat in meetings* setting is usually enabled to permit users to join the meeting chat. If disabled, users cannot chat with other participants during the meeting. This is a big loss because chat is an excellent way for participants to post questions and responses during presentations, or for meeting presenters to share additional information (such as the URL to a web page) with participants.

Meeting Policies

The meeting policy assigned to a user account controls what that user can do in meetings. The General policy is the default, but you can create as many other policies as you like in the *Meeting policies* section under *Meetings*. Some settings apply to meeting organizers (like who can present in a meeting) and allow organizers to change how meetings work through meeting options. Other settings apply on a per-user basis to control the functionality available to individual accounts when they join meetings.

The settings in a meeting policy are in the following groups:

- **Meeting Scheduling:**
 - **Private Meeting scheduling:** Users can create private Teams meetings, meaning that only invited attendees can access the meeting.
 - **Outlook add-in:** Allow users to schedule Teams meetings via the Outlook add-in for Teams.
 - **Meet now in private meetings:** Allow users to create ad-hoc meetings when in private meetings.
 - **Channel meeting scheduling:** A channel meeting is available to anyone who can access the channel. For public teams, this means that anyone in the tenant can join the meeting.
 - **Meet now in channel meetings:** Allow users to create ad-hoc meetings in a channel.
 - **Meeting registration:** Meeting organizers can require participants to register before attending a meeting (used with webinars).
 - **Who can register:** Controls if meeting registration is limited to internal participants only or can include external participants.
 - **Attendance and engagement report:** Controls if Teams generates an attendance report for meetings.
 - **Include attendees in the attendance report:** Controls if participants can opt-out of the attendance report.
 - **Attendance information:** Controls the level of detail shown in the attendance report. Full details ("show everything") means that Teams captures and reports the start and end time for individual user participation in a meeting.
- **Meeting Join and Lobby**
 - **Anonymous users can join a meeting:** Controls if meetings support anonymous participants (not signed into a Microsoft account).
 - **Anonymous users and dial-in callers can start a meeting:** This setting allows anonymous users (people unknown to the organization) to start a meeting if they are the first to join. The default is *Off*.
 - **Who can bypass the lobby:** Defines the types of users who can join a meeting without having to wait in the lobby. For example, People in my organization and guests.
 - **People dialing in can bypass the lobby:** Controls if people who join a meeting using a phone line can bypass the lobby.
 - **People can join external meetings hosted by:** Controls the ability of users to join meetings hosted in external organizations. The options are anyone (all organizations), only people in

trusted organizations (only meetings in organizations listed in the external domains list or multi-tenant organizations).

- **Meeting engagement:**

- **Meeting chat:** Controls the availability of chat during meetings to participants. Typically set to allow chat for everyone except anonymous users.
- **External meeting chat:** If on, tenant users can participate in meeting chats hosted by non-trusted Microsoft 365 organizations. A non-trusted organization is one that isn't covered by the tenant's external access settings.
- **Q&A:** Defines if the Q&A app is available during a meeting.
- **Reactions:** Set the toggle on to allow participants and guests to use reactions (like applause) during meetings.

- **Content Sharing:**

- **Who can present:** This setting controls who can act in the presenter role during a meeting. The usual value is *Everyone*, which means that meeting organizers decide who can present, but the ability to present can be restricted to meeting organizers and co-organizers or users from the host organization and guests.
- **Screen sharing:** Teams allows users to share content from their PC to meeting attendees on the entire screen or as a single application. If you want to prevent this, disable the setting. The default is "Entire Screen."
- **Participants can give or request control:** Allow a meeting participant to give control of a meeting to another participant, or request control if they don't already have control.
- **External participants can give or request control:** An external participant is a guest user or an anonymous user who joins a meeting. The setting is *On* for the default policy, but *Off* for other meeting policies that you create.
- **PowerPoint Live:** Allow meeting participants to share PowerPoint presentations. Sharing a PowerPoint presentation is an alternative to sharing a complete desktop and consumes less bandwidth when network resources are scarce. See [this page](#) for more information.
- **Collaborative annotations:** If on, meeting participants can annotate content that supports this feature, like Whiteboards.
- **Live share:** When on, meeting participants can edit an Office document from within the Teams meeting window.
- **Whiteboard:** Allow meeting participants to use the whiteboard app.
- **Shared notes:** Allow meeting participants to share notes during the meeting.
- **Organizer can restrict participants from copying or forwarding meeting chat messages:** When on, meeting participants are unable to copy or forward items in the meeting chat. This is a Teams premium feature.
- **Participants can share content in external meetings hosted by:** This setting controls the ability of meeting participants to share content in meetings hosted by external organizations. The options are Any org, trusted orgs and guests, and No other orgs (no sharing of content is allowed in external meetings). This is a Teams premium feature.

- **Recording and Transcription:**

- **Meeting recording:** Allow Teams to record meetings. Teams stores MP4 files for meeting recordings in OneDrive for Business and makes the recordings available to meeting attendees after meetings finish. A separate setting in calling policies controls if users can record 1:1 calls. The *AllowCloudRecordingForCalls* setting is *Off (\$False)* by default and can only be enabled (set to *\$True*) in PowerShell by running the *Set-CsTeamsCallingPolicy* cmdlet.
- **Recording automatically expire.** Controls if Teams automatically sets meeting recordings to expire after a set expiration period (in days). Note that the retention period of a retention label applied to a meeting recording overrides the Teams retention period.

- **Require participant agreement for recording and transcription:** If on, meeting participants must agree to meetings being recorded and transcribed. If they don't, participants lose access to audio, video, and content sharing.
- **Store recordings outside of your country or region:** The default is for Teams to store meeting recordings in SharePoint Online or OneDrive for Business hosted in the host tenant's datacenter region. If set to Off, meeting recordings can be stored in regional datacenters.
- **Transcription:** Allow users to turn on automatic transcription generation for a meeting.
- **Live captions:** Controls if users can view live captions during a meeting.
- **Copilot:** Controls the access Copilot has to the meeting transcript. The default is *On only with retained transcript*, which means that Copilot can access the transcript during and after the meeting. The other option is *On*, meaning that Copilot only accesses the transcript during the meeting.
- **Audio and Video:**
 - **Mode for IP audio:** Defines if IP audio is enabled.
 - **Mode for IP video:** Defines if IP video is enabled.
 - **Video conferencing:** The default is to allow video meetings. If you want to restrict meetings to audio, change this setting to off. Individual users have the choice to restrict their participation to audio when they join a meeting and might choose to do so if the network connection is poor, or they simply don't want other participants to see them in all their glory.
 - **Broadcast production with NDI and SDI hardware:** Allow the user to employ NDI technology where the video for each participant becomes a discrete video source processible by video production software to create an output.
 - **Media bit rate:** The default is 50000 (50 MB). Do not change this value unless you have good reason to do so.
 - **Network configuration lookup:** If on, Teams checks roaming policies in network topology.
 - **Participants can use video effects:** Allow users to select from no filters, background blur, curated background images, or custom images they upload.
 - **Live streaming:** Controls if users can stream Teams meetings.
 - **Allow streaming media input:** When on, organizers of Teams webinars and meetings can use an external hardware encoder to produce their events using the real-time messaging protocol (RTMP).
- **Content Protection (Teams Premium):**
 - **Watermark videos:** Insert the email address of each participant in their video feed.
 - **Watermark shared content:** Insert the email address of each participant in the video feed generated for shared content.

Updating Meeting Policies with PowerShell

In some cases, Microsoft introduces meeting policy settings to support new functionality that is managed through PowerShell. This is usually an interim situation while Microsoft updates the Teams admin center UI. The `Set-CsTeamsMeetingPolicy` cmdlet updates meeting policy settings. This example enables settings in the default policy to:

- Allow meeting chat for everyone except anonymous participants.
- Allow the download of meeting engagement reports.
- Sets the languages used to generate meeting invitations to US English and German (user language preferences cannot override this setting because it's applied on the server when [Teams generates the joining instructions for meetings](#)).

The Global policy applies to Teams users unless their accounts are assigned other meeting policies:

```
Set-CsTeamsMeetingPolicy -Identity Global -MeetingChatEnabledType EnabledExceptAnonymous  
-AllowEngagementReport "Enabled" -MeetingInviteLanguages "en-US,de-DE"
```

Meeting Customization Policies

Meeting customization policies control features that require users to have the [Teams Premium licenses](#). A customization policy allows an organization to define one or more lobby themes for meeting organizers to choose from when they set up a meeting. People in the lobby then see the selected image, which is often a corporate logo. The other feature controlled by a meeting customization policy is the ability to upload corporate images for people to use as backgrounds during meetings. Corporate images appear before Microsoft's default set of meeting backgrounds and the custom images uploaded by a user.

Custom Teams Meeting Invitations

Organizations can customize the emails generated for Teams meeting invitations. Open the Meetings section of the Teams admin center and navigate to *Meeting settings*. You can now customize four components used by Teams to create email invitations for meetings:

- **Logo URL** points to a network-accessible JPEG or PNG file that Teams inserts into meeting details. [Microsoft's documentation](#) recommends using an image that's no more than 188 pixels wide by 30 pixels tall. I have used considerably larger images, but it's best to stay somewhat close to the recommended size to avoid bloating Teams meeting invitations with unnecessary graphic content.
- **Privacy and Security URL** points to a web page containing information users need to know about Teams meetings. For instance, the page might explain why Teams displays reminders when an organizer records a meeting.
- **Help URL** points to a web page containing information about Teams meetings. For example, the page could explain that Teams meeting recordings are subject to an automatic expiration policy.
- The **Footer** is free-form text containing whatever words of wisdom seem appropriate.

After completing the meeting settings, you can test what the customized body of a Teams meeting invitation looks like by clicking the *Preview invite* button. The view presented is only an approximation of what users see. The actual format depends on the client in use, but it's close enough to understand what people might see.

If meeting organizers update the details of a meeting (like setting a new time), the meeting invitation sent by Teams does not include the organization logo.

Feedback Policy

Teams contains several methods to allow users to express their views on Teams. Users can submit feedback to Microsoft using the **Give feedback** option in the Help menu. Users can also make suggestions about new features they would like to see in Teams. Finally, Microsoft can prompt users to take periodic surveys to tell Microsoft how they're getting on with Teams. Some organizations dislike the idea of users providing direct feedback as they consider this to be a function of the organization after gathering opinions across the entire user base. In these circumstances, you can disable the ability of users to give feedback or participate in surveys by:

- Amending the default (global) feedback policy. This approach has the advantage that it covers every user, including new accounts. If you decide to allow some users to submit feedback, you can create and assign a feedback policy that allows these options.
- Assigning the Disabled feedback policy provided by Teams to user accounts.
- Creating and assigning a new custom feedback policy to disable the options. The advantage of this approach is that the organization has full control over feedback policy settings. The downside is that you must remember to assign the custom policy to new accounts after their addition.

The Teams admin center doesn't support management of feedback policies, so you must use PowerShell. To create a new feedback policy, run the `New-CsTeamsFeedbackPolicy` cmdlet:

```
New-CsTeamsFeedbackPolicy -Identity "Tenant Disabled Feedback" -UserInitiatedMode Disabled
-ReceiveSurveysMode Disabled -EnableFeatureSuggestions $False
```

The settings are:

- `UserInitiatedMode` controls the visibility of the **Give feedback** option in the Help menu.
- `ReceiveSurveysMode` controls if users see the surveys initiated by Microsoft.
- `EnableFeatureSuggestions` controls the visibility of the **Suggest a feature** option in the Help menu.

Unfortunately, bulk policy assignment (which we will cover soon) does not support feedback policies, so you must assign the new policy individually using the `Grant-CsTeamsFeedbackPolicy` cmdlet. These commands read in a set of user principal names stored in a CSV file, assign a policy to each user, and check that the target accounts have the expected feedback policy.

```
[array]$Users = Import-Csv c:\temp\Users.csv
# Assign the Disabled feedback policy to all users loaded from the CSV file
ForEach ($User in $Users) { Grant-CsTeamsFeedbackPolicy -Identity $User.UserPrincipalName -Policy
"Tenant Disabled Feedback" }
# Check that the assignment works
Get-CsOnlineUser -Filter {TeamsFeedbackPolicy -eq "Tenant Disabled Feedback"} | Format-Table
DisplayName, TeamsFeedbackPolicy
```

Feedback policies are unsupported in the GCC, GCC High, and DOD clouds.

Assigning Policies

Several methods exist to assign Teams policies to user accounts, including:

- **Individual assignment** by updating the policies for user accounts in the Teams admin center.
- **Bulk editing** by selecting a set of users in the Teams admin center and assigning the same policies to the selected accounts.
- **Running PowerShell cmdlets** like `Grant-CsTeamsMeetingPolicy` to update individual or multiple accounts. Companies often configure Teams policies for users as part of their account provisioning process. Microsoft has modernized the policy management cmdlets to allow their use in Azure Automation and make it possible to schedule runbooks (scripts) to periodically check the policies assigned to user accounts. [This article](#) covers how to use Azure Automation to assign a specific Teams messaging policy to selected accounts.
- Using a **bulk policy assignment** to assign a policy to up to 5,000 accounts. This is a good method to assign the same policy to many accounts at one time and works by defining a set of accounts to receive a policy and submitting a batch job to perform the assignments using the `New-CsBatchPolicyAssignmentOperation` cmdlet.
- **Group policy assignment.** This is an effective way to assign a set of policies to a large population of target accounts. The membership of a distribution list, security group, or Microsoft 365 group (including dynamic groups) defines the set of target accounts. The Teams admin center supports group policy assignment for the most popular Teams policies, like meetings and messaging. Group policy assignment for other policies, like the Teams event policy, is possible by running the `New-CsGroupPolicyAssignment` cmdlet. For instance, this command finds the group identifier for a target group and uses it to assign a Teams events policy to the set of users in the group:

```
$GroupId = (Get-MgGroup -Filter "displayName eq 'All tenant member user accounts'").Id
New-CsGroupPolicyAssignment -GroupId $GroupId -PolicyType TeamsEventsPolicy -PolicyName "Webinar
Organizers" -Rank 1
```

A Teams background job processes group policy assignments and it can take up to 24 hours before assignments become effective. The process takes precedence into account to make sure that Teams uses directly-assigned policies before group assignments, and the highest-ranked group assignment before other group assignments. It's possible that a user account might receive multiple assignments of a policy type through their membership of different groups. When this happens, Teams uses the rank or priority order of the assignment to know which policy to use. The example above sets a rank of 1 (most important) for the assignment, meaning that Teams will use the specified events policy before any other assigned via a group.

Given the range of options available to manage Teams policies, most companies should be able to find suitable methods to assign policies to individuals or sets of users.

[This PowerShell script](#) generates a HTML report of Teams policy assignments per user, including direct and group policy assignments.

Scripting Bulk Policy Assignment

Although it's easy to write PowerShell scripts to process policy assignments for users, using bulk assignment jobs is the most efficient way to assign policies to large groups of users. Here's an example of the bulk application of a policy (in this case, a meeting policy) to a set of users. First, we find a set of mailboxes based on a value in a custom attribute and extract the user principal name for each account. The data is stored in an array variable.

```
$Users = Get-ExoMailbox -RecipientTypeDetails UserMailbox -Filter {CustomAttribute14 -eq "Code22"}  
-ResultSize Unlimited | Select -ExpandProperty UserPrincipalName
```

Although a maximum of 5,000 accounts can be included in a single operation, it's wise to divide processing up across smaller batches and run a single batch at a time. This approach allows you to take corrective action if errors are encountered for some reason. Another way of managing the set of users for a bulk assignment is to use a CSV to collect the account information. If you do, make sure that the CSV file only contains user principal names. When you're ready to import the data, create an array and populate it with the user principal names from the CSV. For instance, this snippet creates a suitable variable and populates it with the imported data:

```
$TargetUsers = Import-Csv c:\temp\UsersToProcess.csv  
$Users = [System.Collections.Generic.List[Object]]::new()  
ForEach ($U in $TargetUsers) { $Users.Add($U.UserPrincipalName) }
```

Next, create a policy assignment operation linking the policy to apply and the set of users to process:

```
New-CsBatchPolicyAssignmentOperation -PolicyType TeamsMeetingPolicy -PolicyName  
RestrictedFunctionality -Identity $Users -OperationName "Teams Meeting Policy Assignment"  
2d5c6c07-bc19-4c6c-a359-2f6530b3a652
```

As you can see, Teams responds with an operation identifier (a GUID). This can be used to find the status of the operation:

```
Get-CsBatchPolicyAssignmentOperation -OperationId 2d5c6c07-bc19-4c6c-a359-2f6530b3a652 | Format-List  
  
OperationId : 2d5c6c07-bc19-4c6c-a359-2f6530b3a652  
OperationName : Teams Meeting Policy Assignment  
OverallStatus : NotStarted  
CreatedTime : 3 Jun 2020 17:13:46  
CreatedBy : 53f08764-07d4-418c-8403-a737a8fac7b3  
CompletedTime :  
CompletedCount : 0  
ErrorCount : 0  
PendingCount : 4
```

We can see that the background processor has not yet started to process the operation. It can take up to an hour before processing starts. We can determine which account submitted the operation by fetching its object identifier from the operation properties and running the `Get-MgUser` cmdlet to return the display name of the account:

```
Get-MgUser -UserId (Get-CsBatchPolicyAssignmentOperation -OperationId 2d5c6c07-bc19-4c6c-a359-2f6530b3a652).CreatedBy | Select DisplayName
```

```
DisplayName
-----
Global Tenant Administrator
```

Eventually, the operation will finish, and its status will change to *Completed*. If the *ErrorCount* is non-zero, we can check the state of each account processed with:

```
Get-CsBatchPolicyAssignmentOperation -OperationId 2d5c6c07-bc19-4c6c-a359-2f6530b3a652 | Select -ExpandProperty UserState
```

Id	Result	State
--	-----	-----
Ben.James@Office365itpros.com	Success	Completed
Imran.Khan@office365itpros.com	Success	Completed
John.Adams@office365itpros.com	Unknown error occurred.	Completed
Rene.Artois@office365itpros.com	Success	Completed

In this instance, a problem happened with the John Adams account. You'll need to check the account to see what might have caused the problem. It might just be a temporary glitch (or the account was already assigned the policy) and you can go ahead and make the change to the account manually through the Teams admin center. The "user not found" error is common and usually happens when a mistake is made with a property like a user principal name and the batch processor cannot find the account to update.

To discover who has been assigned a policy, you can use the `Get-CsOnlineUser` cmdlet. For example, this command reports the accounts assigned a Teams meeting policy called 'RestrictedFunctionality':

```
Get-CsOnlineUser -Filter {TeamsMeetingPolicy -eq 'RestrictedFunctionality'} | Select UserPrincipalName
```

To report users assigned a default policy, check for a null value in the meeting policy:

```
Get-CsOnlineUser -Filter {TeamsMeetingPolicy -eq $Null} | Select UserPrincipalName
```

Reporting Teams Policy Assignments: After you're finished assigning policies to Teams users, you might like to generate a report showing what policies apply to what accounts. Teams doesn't include a report of this nature, but it's easy to generate with PowerShell. [This article](#) explains how to write a script to create a Teams policy report output in both HTML and CSV formats.

Policy Packages

Teams policy packages are collections of policies assigned together to a set of user accounts defined by a group. Policy packages have their own section in the Teams admin center. Each package can include up to ten different Teams policies including meeting, message, app setup, voice routing, and calling. The association of the policy package with the group causes Teams to assign the individual policies specified in the package to the user accounts defined in the group.

Microsoft includes a set of predefined policy packages with Teams. Organizations cannot change the set of policy types in the predefined policy packages, but it is possible to choose individual policies for each type contained in the policy. Organizations can define custom policy packages containing their own selection of

policy types if they have Teams premium licenses for every account assigned policies through a policy packages.

User Settings

User settings cover the management of users, settings for guest access, and controls for external access (federation). User management deals with the assignment of Teams policies to user accounts.

External Access (Federated Chat)

External access defines how users communicate with people outside the tenant. The settings are:

- **Teams and Skype for Business users in external organizations:** This setting must be *Allow all external domains* (open federation – the default) or *Allow only specific external domains* (limited federation) before people can communicate with users in other organizations. See the later section covering how external access works.
- **Teams accounts not managed by an organization:** Turn on to allow users to chat with people who use Teams Personal. You can restrict the set of external users that people are allowed to chat with by creating user profiles. Essentially, a user profile is an entry in the Teams directory tied to their phone number. Profiles can be discoverable, meaning that it can be found by users within the organization. When someone attempts to connect to an user profile, Teams attempts to create a one-to-one federated chat using the telephone number to connect. If the external person doesn't have Teams on their device, Teams sends them an SMS with a link to download and install Teams to allow the connection to be made.
- **Skype users:** Turn On to allow Teams to communicate with Skype users.

By default, Teams allows people to use federated chat to communicate with Teams users in other Microsoft 365 tenants. The following settings are available to control this capability under **External Access** in the **Users** section of the Teams admin center:

- Allow all external domains. This is the default option, chosen because Microsoft wants to encourage organizations to communicate and collaborate.
- Block all external domains.
- Block only specific external domains.
- Allow only specific external domains.

We suggest that organizations restrict external access to specific domains to avoid potential spamming or social engineering compromise through techniques like the [GIFShell proof of concept attack](#).

Maintaining an extensive allow list of external domains in the federation allow list through the GUI can be an onerous task. It's possible to automate updates for the federation allow and block lists with PowerShell using the `Set-CsTenantFederationConfiguration` cmdlet. For example, this code updates the allow list:

```
$Domain = "office365itpros.com"
Set-CsTenantFederationConfiguration -AllowedDomainsAsAList @{$Add=$Domain} -ErrorAction
SilentlyContinue
```

The external access domain allow and block lists can accommodate 4,000 entries.

Building the External Access Allow List: By default, Teams supports federated chat with any other Microsoft 365 domain. Blocking external chat against spamming, malware, and social engineering attacks creates a challenge to maintain the domain allow list. It can be difficult to decide what domains to include. One source of data is the domains that people connect to in federated one-to-one chats. This information can be analyzed using Graph APIs to [analyze user chats to extract the domain names](#). Another source of information is the domains used by guest accounts present in the tenant. [This article](#) explains how to find the set of domains and use the domain data to populate the external access allow list.

Block Against Trial Tenants

A block against federated communications with trial Microsoft 365 tenants comes into effect at the end of July 2024. A trial tenant is defined as a tenant where only Teams trial licenses are present. The block is governed by the *ExternalAccessWithTrialTenants* settings in the tenant federation configuration policy. By default, the setting is *Blocked*.

```
Get-CsTenantFederationConfiguration | Format-List ExternalAccessWithTrialTenants
```

```
ExternalAccessWithTrialTenants: Blocked
```

You can update the configuration to set *ExternalAccessWithTrialTenants* to *Allowed* if necessary, but this is not recommended because it opens a potential exploitation route that attackers might attempt to use after setting up a trial tenant.

The allowed domains list explained above takes precedence over the *ExternalAccessWithTrialTenants* setting. If a trial tenant is on the allowed domains list, federated chats and meetings with users in that tenant are allowed.

Guest Access Settings

Guest access settings control what a guest user can do within Teams. The settings include enabling or disabling guest access for the tenant, allowing guests to use personal chat, and settings to control the interaction guests have with messages like the ability to edit or delete sent messages. Settings are available to control aspects of guest participation in meetings, such as allowing guests to use the Meet Now feature to create impromptu meetings. Microsoft enables guest access for Teams for new tenants.

Teams Settings

Teams settings are organization-wide settings to control how users interact with Teams for aspects not covered by messaging and meeting policies. These settings include:

- **Notification and Feeds:** Define if you want Teams to add suggested items in users' activity feeds.
- **Tagging:** Define who can manage tags, suggested tags that appear in all teams, and whether users can create custom tags.
- **Email integration:** Settings to control if people can send email to channels (see section later) using special email addresses generated by Teams for channels. If you enable email integration, you can also confine the ability of people to send email to channels to an allowed list of SMTP domains.
- **Files:** Settings to control how users can share files, including whether they can share files using third-party cloud storage solutions like DropBox, and Google Drive.
- **Organization:** Turn the organization tab on or off. If enabled, the tab allows Teams users (but not guests) to see details of the organizational hierarchy represented by the manager-employee links stored in Entra ID.
- The **Devices** settings control how Room Systems (like a Surface Hub) and IP phones work in meetings. The settings are:
 - Require a secondary form of authentication (the default is no access).
 - Set content PIN. The default is that a PIN is needed for outside scheduled meetings.
 - Surface hub accounts can send emails. Some devices such as Surface Hub use device accounts to interact with real users through email, IM, and calls. By default, this setting is True, which allows devices to send IM messages.
- **Search by Name** defines whether directory searches performed by Teams users are limited by Exchange address book policies (ABPs). An address book policy limits the visibility of a user to specific sections of the overall corporate address book, such as only the users in a certain department or country. Organizations often use policies to limit communication between different groups like

students and teachers or traders and financial advisors. The default for the directory search setting is *Off*, meaning that Teams imposes no restrictions on users. If set to *On*, the address book policy defined for mailboxes limits what users can see (if no policy exists, users can see and communicate with everyone in the directory). For example, they can only start a personal chat with another user who is visible to them according to the address book policy. In addition, if you use address book policies to limit the directory search for users, Teams is no longer able to suggest teams for them to join (and disables the /Join command). Limiting directory searches for Teams is a prerequisite for Information Barriers (discussed later).

- **Safety and Communications:** This setting controls if supervised chat is enabled for the organization. The most common use of supervised chat is in education settings where a teacher or responsible adult oversees chats between students.
- **Shared channels:** Owners of shared channels cannot add members from domains where a Direct Connect two-way trust is not in place. You can enable the option to have Teams display a prompt when it detects that a trust is unavailable together with a link to a web page (defined here) to give the channel owner information about how to get additional support.

Planning

The Planning section of the admin center covers:

- Teams advisor: This is a wizard-based guide to help organizations who do not currently use Teams roll out different areas of functionality. See [this page](#) for more information. Among the topics covered by the advisor are:
 - Chat, messaging, and apps.
 - Meetings and conferencing.
 - Skype for Business upgrade.
- Network planner: See the Calling and Devices chapter for more information about planning your network for Teams and the Microsoft Phone system (cloud voice).

Licensing Teams

The license necessary to access Teams is bundled in many Microsoft 365 offerings, with the notable exception being standalone subscriptions, like Exchange Online Plan 2. These users can't even join teams as guest users because Microsoft 365 considers them to be part of the same organization that hosts the teams and therefore aren't guests.

You can selectively enable or disable Teams on a per-user basis by editing a user's account in the Microsoft 365 admin center and switching their Teams license on or off. If you need to enable or disable Teams for many accounts, it's easier to do this with PowerShell (see the license management section in the PowerShell book). To ensure that the widest range of functionality is available to users, make sure that you enable Exchange Online and SharePoint Online for anyone using Teams. Users who do not have a license for SharePoint Online cannot use OneDrive for Business to share files with users in personal or group chats.

Teams Licenses for Guest Users

Microsoft licenses access for guest accounts to functionality like Teams through its [billing model for External identities](#). This is a monthly active user (MAU) model based on unique users with authentication activity in a calendar month. In other words, each guest account counts as one MAU if it authenticates and connects to a tenant to access resources like Teams, SharePoint Online, or Planner.

Guest access to standard Entra ID features is free and the first 50,000 MAUs per month are free for Entra ID premium features. Tenants pay for guest access to premium features above the 50,000 MAU allowance through an Azure subscription.

Access for On-Premises Users

If a tenant uses AAD Connect to synchronize accounts with an on-premises deployment, users can access Teams even if their mailboxes are on Exchange on-premises servers. These users can take part in conversations, group chats, and calls and set up new tabs. However, they cannot create or access meetings or even change their profile picture.

Creating Teams

Before anyone can create a new team, they must be able to create a new Microsoft 365 group. Some tenants allow any user to create a group while others control group creation to a limited set of authorized users. The settings to control who can create new groups (and teams) are in the Entra ID Groups policy. The Groups chapter includes a full discussion of how to manage the policy settings for Groups using PowerShell. If the policy restricts the ability of users to create new groups, it should also include a pointer to a group holding a list of people who can create new groups. If your account is on that list, you can go ahead and create a new team. If not, you will see an error informing you that "*Your IT department has disabled this Microsoft Teams feature for you*" together with a suggestion to contact the IT department for help.

The available methods to create new teams are:

- Teams client (desktop, web, or mobile).
- *New-Team* cmdlet in the Teams PowerShell module.
- Use the Teams Graph API (or the Microsoft Graph PowerShell SDK). This includes methods such as "teamifying" a SharePoint Online site (create a new team for an existing site using the SharePoint browser UI).

The advantage of these methods is that they explicitly mark a group as intended for use by Teams. In technical terms, this means that several properties of the group are set for Teams. These include:

- The group is hidden from Exchange clients like Outlook and OWA (*HiddenFromExchangeClientsEnabled* is \$True).
- The group is hidden from Exchange address lists like the GAL and OAB (*HiddenFromAddressListsEnabled* is \$True).
- New members receive a welcome message for Teams instead of Microsoft 365 Groups.
- Members are not subscribed to receive calendar updates for the group. This means that team members do not receive invitations to meetings scheduled in the group calendar (channel meetings). Some organizations prefer that team members receive invitations. If this is the case, you can update the *AlwaysSubscribeMembersToCalendarEvents* property for the group to \$True.

Another way to create a team is to create a Microsoft 365 group using an admin center, PowerShell cmdlets like *New-UnifiedGroup* or *New-MgGroup*, Graph APIs, or apps like Dynamics 365, and then team-enable the group. If you take this approach, consider updating the group settings listed above to make groups created outside Teams work like those created by Teams.

Automate Teams Creation

Many organizations restrict the creation of teams and require users to go through a process to seek approval for a new team and use methods like a Power Automate flow or PowerShell script to automate the collection of details for the new team, gaining approval, and creating the team if approved. Microsoft has a sample Power Apps application (called [request-a-team](#)) to automate the provisioning of new teams. You can [download its source code from GitHub](#). Whatever method you use, remember to:

- Update team properties like hidden from address lists, and hidden from Exchange clients, just like a team created by Teams would be.
- Add a description so that people will remember why the team exists.
- Set the privacy of the new team to Public or Private.
- Assign a classification or sensitivity label to the team (assigning the label will set the privacy).
- Ensure that the new team has at least one owner.
- Populate the initial membership.

Creating a Team in the Teams Client

To create a new team in the desktop or browser client, click **Teams** in the navigation bar and then select the plus sign (**create and join teams and channels**) at the top of the screen. You can now choose to create a new team or join one of the teams suggested by Teams. The default is to create a new team from scratch, but you can also choose more options to:

- Create a team from an existing group or team.
- Use a template created by Microsoft or the organization.

You can also team-enable an existing modern SharePoint Online site (one with a Microsoft 365 group) from the SharePoint browser interface.

The Teams mobile client only supports the creation of a new team from scratch. You can't create an org-wide team, use a template, or create a team from an existing team or group using the Teams mobile client.

Before creating a new team, make sure that a team is the best choice for your purpose. In many cases, it is better to create a channel in an existing team. Remember that a team can support up to 1,000 channels, and it is possible that a regular, private, or shared channel can act as the collaborative space that you need. Using a channel rather than a team conserves resources and lessens the potential for the accrual of "digital debris" (unused teams and SharePoint sites).

Creating a New Team from Scratch

Creating a team from scratch means that you have maximum control over its characteristics. The first step is to choose what kind of team to create. A team can be:

- **Private:** The team owners and tenant administrators control membership and decide who can join the team. This kind of team is not discoverable by users unless allowed by policy or the discoverability setting in the sensitivity label assigned to the private team.
- **Public:** Anyone in the organization can join the team. The SharePoint Online sites created for these teams are also public. This creates the possibility that sensitive information might be inadvertently exposed. A [container management sensitivity label can prevent the creation of public groups](#) or team members can assign sensitivity labels with encryption to documents to ensure that access to confidential information stored in SharePoint Online is restricted.
- **Org-wide:** Every licensed account in the organization automatically becomes a member of the team. Like other teams, org-wide teams can support up to 10,000 members. If your tenant exceeds the membership threshold or five org-wide teams already exist (including archived teams), you won't have the choice to create org-wide teams and should consider an alternative for org-wide communications (like Viva Engage). Only tenant global administrators can create org-wide teams.

The basic details for the new team are:

- **Team Name:** This is the display name for the team (and the underlying group) and it is what appears in the list of teams in the Teams client and the Exchange GAL (if you decide to reveal Teams to Exchange). It is always best when you give a team a meaningful name that conveys its purpose. If your

organization uses a group naming policy, Teams shows the effect of the policy by displaying the name of the team after it applies the policy when it creates the new team. The group naming policy does not affect tenant administrators, so teams created by administrators keep the display name as entered.

- **Description:** This is a free-form text description of why the team exists and what the members of the team use it to do. Users see the team description when they browse teams, so it is important to put some thought into the description to make it accurate, interesting, and easily digestible. Get right to the point and put the essential information like the purpose of the group at the start and make sure that the first 80 characters convey the essence of the group because this is the amount of text displayed in search interfaces. Put less essential information at the end of the description, such as who created the team, the contact name for the team, and so on.
- **The name of the first channel:** Give a name for the initial channel in the team. Ideally, the first channel in the team should reflect the major topic to be discussed in the team. You cannot use "General" (or its local language equivalent) as the channel name because this is a reserved word.

To indicate the level of confidentiality of the information contained in a team, it has a classification. This can be set by assigning a:

- **Sensitivity label:** if the tenant uses sensitivity labels for container management (see below), the team inherits the privacy level (public or private) and guest access (on or off) from the settings in the chosen label.
- **Classification:** Classifications are simple text description strings defined in the Entra ID Groups policy. Classifications do not affect team settings.

Teams clients do not check that a group, distribution list, or team of the same display name already exists in the tenant, so it is quite possible to create multiple teams with the same name. This is one of the good reasons why some tenants restrict team creation to a small set of people, who have the responsibility to check that the display name does not clash before they create a team.

After entering the properties, click **Next** to continue. Teams creates the group object in Entra ID and Microsoft 365 provisions the resources used by the team, such as the SharePoint team site.

An Effective Teams Naming Convention: The essence of an effective Teams naming convention is that it should result in team names that are simple and clear. With this in mind, here are some recommendations to consider:

- Use **shorter rather than longer names**. The Teams client GUI displays between 31 and 35 characters (depending on case). If a team name is longer, make sure that the most important part of the name is at the start.
- Use a **suitable team photo** to illustrate the purpose of the team. Remember that Teams displays thumbnail photos in team lists, so make sure that sufficient detail is visible in a thumbnail.
- If your organization uses the group naming policy, **don't use prefixes** because they take up too much space in the Teams client GUI.
- **Don't include dates** in team names. If you need to have time-limited discussions, host them in a channel with an appropriate name.
- **Don't include hyphens or dashes** in team names. These characters are included in the SharePoint site address and might contribute to reaching the 400 character maximum for full file paths.
- **Use sensitivity labels** to indicate the level of confidentiality of the information discussed in a team. There's no need to include words like "Internal" or "Confidential" in a team name if the team is labelled appropriately.

Sensitivity Labels and Teams

If the tenant enables sensitivity labels for container management, Teams retrieves settings from sensitivity labels when creating new teams or when editing the properties of existing teams. When a team has a sensitivity label, the team uses the name of the label as its classification and applies the settings in the label for privacy and guest access. If the team has any private or shared channels, the channels and the SharePoint sites belonging to those channels inherit the label assigned to the parent team.

If an administrator or group owner updates the sensitivity label assigned to a group or SharePoint site linked to a team, the updated label assignment synchronizes to Teams to apply the settings from the new label. The synchronization of label assignments from other workloads can take up to 24 hours.

Currently, the only way to assign a sensitivity label to a team is via a client. The Teams PowerShell module does not support sensitivity labels (cmdlets in the Groups and SharePoint modules can assign labels, which then synchronize with Teams) and you can't assign a sensitivity label to a team using the Graph API or when creating a team from a template.

Assigning a sensitivity label to a team does not affect the information stored in the team. See the Information Protection chapter for more information about sensitivity labels and container management.

Create a Team from an Existing Team or Group

If you don't want to create a team from scratch, you can choose to create a new team based on the settings of an existing team (a template) or you can team-enable a group.

Using an Existing Team as a Template

The idea behind creating a team using an existing team as a template is that if you are in the position where you need to create multiple teams with approximately the same structure, it's easier to create one team to use as a template and set the team up in a form that you want to replicate to other teams. You can only use a team as a template when you have access to that team (you're a member).

When you create a new team based on a template, you can replicate the membership (including guests), settings, channels, apps, and tabs from the template team. No content is copied across in terms of conversations or files, and some tabs will need to complete a setup process before they can be used. For instance, if the template team includes a tab pointing to Planner in a channel, the channel and the tab are copied to the new team, but because the plan doesn't exist for the channel, you must start Planner and create the plan.

Enabling Existing Groups for Teams

In many ways, team-enabling a group is an interesting decision because it switches the focus for conversations in the group away from email to channel conversations. There is no way to migrate existing conversations from a group into channels, so the switch is a one-time all-in operation. However, the files stored in the group document library remain available to the team.

Whether you create a team from scratch or team-enable an existing group, you end up in the same place with a team-enabled group. The difference between the two methods is that team-enabling an existing group automatically makes the team available to the current group members because Teams and Groups share the same membership.

Groups can only be team-enabled by their owners. To begin, a group owner goes through the normal process to create a new team and chooses more create options. Then they select **from group** under the Create team options. This option only appears when the user is an owner of one or more Outlook-based groups that are not yet team-enabled (groups used for Viva Engage communities are unsupported). Click the link to expose

the set of groups owned by the user that are not team-enabled. As the UI only shows only a small number of groups at a time, it might be necessary to scroll through the list to find the group that you want to upgrade. The set of groups includes some hidden from Exchange address lists (because Teams does not use address lists) but excludes groups with hidden membership. Select the group that you want to enable for Teams and click Choose team to begin the process to populate the team resources and properties for the

A group owner must decide to enable the group for Teams. There is no way for a user to search for a group that is not team-enabled and ask its owner to upgrade it. A group owner does not need permission to create new groups to be able to team-enable an existing group. After you team-enable a group, you should consider hiding it from Exchange clients to force users to use Teams for conversations (see below).

Creating Teams from Templates

Team templates are prepopulated structures created by Microsoft or the organization to make it easy to create teams to do a specific job. Each template consists of a set of channels, tabs, and apps automatically added to teams created using the template. Some of the out-of-the-box templates are for general use (like project management); others (like Organize a Store) are for a particular industry. Among the templates published by Microsoft are:

- Adopt Office 365.
- Manage a project.
- Manage an event.
- Onboard employees.
- Organize help desk.
- Coordinate incident response.

Read [this documentation](#) for more information about creating teams from templates.

As an example of what happens when you create a team using a template, if you use the Manage a Project template, Teams adds four channels and two apps to the new team. The channels are General, Announcements, Resources, and Planning while the apps are OneNote and Wiki. During the creation process, you can rename the channels to make them more appropriate for the new team and add a sensitivity label to reflect the importance of the information you expect the new team to contain. After creating the team, you still need to add team members, add other apps and channels (including private channels), post a welcome note, and take whatever other actions are necessary to build out the complete team.

Template management is in the Teams section of the Teams admin center. You can add, edit, or remove templates to meet the needs of the organization, including the ability to copy (duplicate) one of Microsoft's policies to create a customized version more suitable for your organization. Custom templates created by a tenant appear before the standard templates from Microsoft when shown to people creating new teams.

[PowerShell cmdlets to manage team templates](#) are also available.

Template Policies

Template policies control the set of templates visible to users when they create new teams. The default global policy makes all templates visible. It's a good idea to consider creating custom team templates to deliver a more refined view to users. For instance, you could create a template that shows only custom templates and omits all the standard templates created by Microsoft. Template policies are managed in the Teams section of the Teams admin center. The `*-CsTeamsTemplatePermissionPolicy` cmdlets are available to manage template policies.

Creating a new template policy is simple. Navigate to the Teams section in the Teams admin center and select Templates policies. Create the policy and give it a name and description. Then select the set of templates you

want to hide from the available set. Click the *Hide* button to make the choice effective and then save the policy. The next step is to assign the policy to users individually or by using a bulk policy assignment job (the policy type is *TeamsTemplatePermissionPolicy*). Give the policy a couple of hours to become effective and then test it by asking one of the users assigned to the policy to create a new team. They should then see the set of templates dictated by the policy.

Sensitivity Label Control over Discoverability and Shared Channels

In February 2024, Microsoft introduced a new mechanism to control the discoverability of private teams. Discoverability means that Teams will list or suppress private teams in the gallery viewed after selecting the *Join a team* option. It does not mean that users can join private teams without permission. If a private team is discoverable, users can request to join that team, but an owner must approve the request before they can join.

The new mechanism enables granular visibility for private teams through two components:

- The *Discover private teams* setting in the Teams policy assigned to the user account. If enabled, the user can see private teams in the join a team gallery.
- Teams discoverability settings in sensitivity labels used for container management.

Sensitivity labels are only available to tenants with Office 365 E3 (or above) licenses. As explained in the Information protection chapter, container management labels contain settings to control the behavior of the containers (teams, sites, and groups) to which they are applied. The Teams discoverability setting for a label takes precedence over the Teams policy assigned to a user account, meaning that it is possible to allow general visibility for private teams but restrict access to private teams assigned with specific sensitivity labels. For instance, let's assume that the settings for the Confidential Access sensitivity label block access to private teams. A user assigned a Teams policy that makes private teams visible can see any private team except those assigned the Confidential Access label. See [this article](#) for more information.

Sensitivity labels can also control the types of teams that can be invited to participate in shared channels belonging to labeled teams. The choices are:

- **Internal teams only:** Only teams from the same tenant can be invited.
- **Same label only:** Only teams assigned the same sensitivity label can be invited.
- **Private teams only:** Only teams with private membership can be invited. When the label is assigned to a team, Teams checks shared channels for public teams and remove any that are found. If a team owner subsequently changes the privacy for a team in the shared channel from private to public, Teams removes the team from the shared channel.

If the setting is *internal teams only* or *same label only*, it controls what teams can join shared channels in the future. It has no retrospective effect on affect teams that currently participate in shared channels belonging to labeled teams.

Over time, it is likely that we will see additional controls for Teams managed through sensitivity labels.

Adding Team Members

After Teams creates the new team, you can add members (Figure 12-3) and specify whether the new member is an owner or just a normal member. You can add individual users or use a distribution list, mail-enabled security group, or group (or another team) as a source, in which case Teams expands the membership of the selected group and adds each user individually to the team. Teams excludes unsupported recipient types found in these groups (such as a mail-enabled public folder) and will not try to add them as members. If you use any form of a group to add members to a team, remember that any later changes to the membership of the source group will not replicate to update the membership of the team.

As described later, if the tenant supports guest accounts, you can add external people as guest members. If team settings block guest membership, Teams won't show you guest accounts that already exist in the tenant directory or allow you to input the email address of an external user to create a new guest account. Finally, if your tenant uses information barrier policies to stop different sets of users from communicating with each other, you won't be able to add someone to a team if their presence causes a policy violation. To automate processing, any of the supported member types can be added to (or removed from) a team with PowerShell.

Add members to Office 365 Adoption

Start typing a name, distribution list, or security group to add to your team. You can also add people outside your organisation as guests by typing their email addresses. People outside your org will get an email letting them know they've been added. [Learn about adding guests](#)

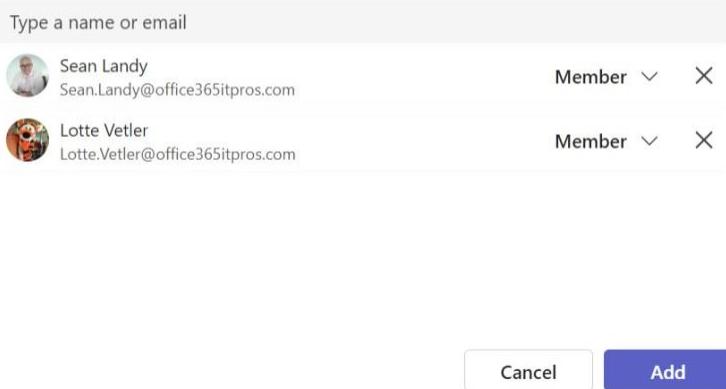


Figure 12-3: Adding new team members

Updating Team Rosters

Internally, Teams refers to the membership of a team as its "roster." If you add someone to a team through a Teams client, Teams refreshes the roster immediately in that client. Other Microsoft 365 applications can update group membership and cause Entra ID to synchronize the updated group membership to Teams. For example:

- A Teams client updates team membership. Teams synchronizes the Entra ID updates.
- A PowerShell script, Graph API, or another administrative interface (like the Microsoft 365 admin center) updates group membership.
- A client like OWA updates group membership. Outlook clients also update group membership in the Exchange directory.

Behind the scenes, Teams uses a background process called *Roster sync* to synchronize changes made in Entra ID and update its rosters. When a user connects to a team with the desktop client, the client checks to see if any changes are waiting in Entra ID. If some are, the Roster sync process downloads the changes and updates the local cache.

The internal SLA for synchronization between Teams and Entra ID is 24 hours, and at worst it can take this long before a change made to group membership by another workload is effective across Teams. Usually, changes are available much sooner than the SLA limit.

Teams with Duplicate Names: As noted above, Teams will let you create a team with a display name that duplicates another team. This will confuse users who belong to those teams as they will never be quite sure which team they should use. From a technical perspective, Teams is quite happy to have duplicate display names because behind the scenes the teams have different aliases and names. If you get into this unhappy circumstance, you can change the display name of one of the affected teams by editing the team

properties (Edit team) or by running the `Set-UnifiedGroup` cmdlet to update the `DisplayName` property for the underlying group. For example:

```
Set-UnifiedGroup -Identity BudgetPlanning -DisplayName "Budget Planning Group"
```

Renaming the team fixes the immediate issue of the duplicate display name. It will not rename the SharePoint team site. If you want to rename the SharePoint site, do so in the SharePoint Admin Center or use the `Start-SPOSiteRename` cmdlet.

Creating an Org-Wide Team

If your tenant has fewer than 10,000 accounts (the limits are smaller for GCC and GCC/High tenants), you can create an org-wide team. A tenant can have up to five org-wide teams. Org-wide teams are intended for tenant-wide communications without the need for an administrator or team owner to manually add all the employees to the team membership, including the need to check for new employees and add them periodically with PowerShell. The advantage of using PowerShell to manage the membership of an org-wide team is that you have more flexibility in managing the membership; the downside is that you must check and update the membership with new users and remove those who leave the organization periodically. Using an org-wide team avoids this work.

Larger tenants can consider using:

- **Dynamic Teams** to support discussions for different sections of the organization. For example, you might have a team for each department or each country.
- **Viva Engage** for company-wide communications and collaboration. Viva Engage can easily scale up to handle very large organizations with hundreds of thousands of users.

To create an org-wide team, choose **Create team** as usual, then **more team options**, and then select **Org-wide** from the list of options. The choice to create an org-wide team is only exposed to tenant (global) administrators and when you create an org-wide team, Teams adds all the global admins as team owners. It then adds all "active users" as members. You know the membership is managed by Teams because the Manage team screen has a banner saying, "*Team members will be automatically added and removed to reflect your Active Directory*".

Automatic membership should exclude accounts without valid Teams licenses as well as guest users. However, sometimes accounts that should not be included in an org-wide team turn up in the automatically generated membership. Among accounts that should be checked against the team membership are:

- Service accounts (if they are assigned a license).
- Mailboxes used for purposes such as DLP incident reports.
- Accounts that don't have a Teams license (or licenses where the Teams service plan is disabled).

Although Microsoft has fixed the bugs at the root of automatic membership, it is still good practice to check the membership after creating an org-wide team to remove anything that doesn't belong. Once you remove someone from an org-wide team, the service remembers the deletion and won't try to add that account back to the membership. Likewise, if you find that an account that should be in the membership has been omitted for some reason, you can add them manually. As with any team with a large membership, after you create an org-wide team, consider imposing some order on discussions from the start by updating team settings to restrict channel creation, the ability to post to the General channel, and to use @team mentions (because these generate notifications to everyone).

On an ongoing basis, employees leave and join the company and people lose or gain Teams licenses. When someone leaves the company and their account is removed, their membership in the team is also removed. To handle new joiners and people who gain or lose Teams licenses, a background process running on Teams

clients scans the accounts in the tenant periodically (expect new users to appear within a few minutes) and adds or removes the user as needed.

Unlike normal teams, members can't choose to leave an org-wide team. This limitation is the same as exists for dynamic teams, but unlike dynamic teams, an org-wide team doesn't use a membership rule to calculate its membership. Instead, the background process manages membership and the Microsoft 365 group for the team has an "assigned" membership, so you don't need to buy Entra ID P1 licenses for all the members.

Adding New Employees to Org-Wide Teams

Soon after you create an account for a new employee, if the account has a license for Teams, the account is added to the membership of org-wide teams. If your company provisions Microsoft 365 accounts for new employees in advance of their joining date as part of an onboarding process, you might not want this to happen because you don't want other employees to know that someone is joining the company. In this case, you can either:

- Wait for the employee to join the company and create their account at that point.
- Create the account for the new employee but assign dummy information for the display name and primary SMTP address. For example, you could assign "New Employee" as the display name so that other employees see that "New Employee:" has joined. The reason why to assign a dummy SMTP address is that users can click on "New Employee" to see more information from their people card. The SMTP address usually contains the first and last name of a person, so you don't want to expose that information on the people card.

You then update the mailbox display name, name, and SMTP address after the new employee comes on board. If you use a dummy email address, you also need to update the account's User Principal Name to be the user's real sign-in address. These updates are easily done using PowerShell. For example:

```
Set-Mailbox -Identity NewEmployeexxx20 -DisplayName "Jake Adams" -WindowsEmailAddress "Jake.Adams@Office365itpros.com" -Alias "Jake.Adams" -Name "Jake Adams"
```

```
Update-MgUser -UserId (Get-Mailbox -Identity Jake.Adams).ExternalDirectoryObjectID -UserPrincipalName Jake.Adams@office365itpros.com
```

You don't need to worry about the dummy email address assigned to the account because it will never have been used. Any messages delivered to the mailbox will be waiting for the new employee.

If this arrangement doesn't work, consider using all-employee teams whose membership is updated manually. It is easy to script additions and removals of employees from membership as part of the HR onboarding or leaving processes. Another workaround is to create accounts for new users in a disabled state and only enable the accounts when people join the organization. Teams ignores disabled accounts when it builds the membership of org-wide teams.

Updating an Existing Team to be an Org-wide Team

Any existing team with private or public access can be converted by a tenant administrator to be an org-wide team to gain the benefit of automatic membership management. To make a team into an org-wide team, use the **Edit team** feature to change the privacy setting to be org-wide. When you save the setting, Teams updates the membership with all valid accounts. Any users not included in the automatic membership remain in place, including guest users. You can also change an org-wide team to be a private or public team using the same approach, and in this case, the existing membership stays in place, but the automatic background refresh of membership is disabled.

Dynamic Teams

You cannot create a team with dynamic membership using a Teams client. Instead, you first create a new dynamic Microsoft 365 group through the Entra admin center or PowerShell, including the membership rules used by Entra ID to calculate the group membership. When you're happy that the group membership is correct, go ahead and create a new team from the group as described earlier. Teams respects the membership calculated by Entra ID and if you examine the membership (using **Manage team**), you see the same membership there as you see in the Entra admin center. However, you can't update the membership from Teams.

Team owners are static and not computed automatically. You can add team owners to the dynamic group through the Entra admin center, or with PowerShell. You can change a member in the dynamic set to be an owner. However, if you demote an owner to become a member and they are not in the set computed by the query, they lose their membership of the team.

You can also use a dynamic group as the source to add members to another team. In this case, just like a regular distribution list or group, Teams reads the present membership and adds them to the team. And just like when you use other types of groups to populate membership for a team, this is a one-time operation and anyone who joins the original team thereafter does not automatically join the other team.

Hiding Teams from Exchange Online

Teams uses the Microsoft 365 Groups membership service. And because each team has all the resources of a Microsoft 365 group, it has a group mailbox that can function as an Outlook group with email-based conversations. Users therefore could use email or Teams for their conversations. To remove any potential for confusion, Microsoft hides the existence of groups created by Teams from Exchange-based clients (OWA, Outlook desktop, and Outlook mobile).

Following the creation of a new team, Exchange Online sets the *HiddenFromExchangeClientsEnabled* and *HiddenFromAddressListsEnabled* properties of the underlying Microsoft 365 group to *\$True*. The new group is perfect for Teams but remains invisible to Exchange clients and does not appear in address lists like the GAL. In addition, because the focus of communication for the group is Teams communications, the group's subscriber list is not populated with tenant users (guest members are added). Any email sent to the group is delivered to the group inbox, but copies are not distributed to local tenant members (as explained in the Groups chapter, group owners can create an auto-reply for team-enabled groups to inform email senders that the group doesn't use email). Email from external senders is blocked.

Unfortunately, the flags to hide teams from Exchange Online are not set when an administrator creates a new team-enabled group using an administrative interface like the Teams admin center, Microsoft 365 admin center, Entra admin center, SharePoint admin center, or APIs like *New-UnifiedGroup* and the Microsoft Graph API. Administrators have full control over group settings and can update the settings as they wish. The net result is that team-enabled groups can be visible to Exchange Online clients. In addition, older team-enabled groups might not have *HiddenFromExchangeClientsEnabled* set to *\$True* because Microsoft did not update groups retrospectively following the introduction of the setting.

To check if any team-enabled groups are visible to Exchange, fetch the set of team-enabled groups and filter out the hidden groups. For example:

```
[array]$Groups = Get-UnifiedGroup -Filter {ResourceProvisioningOptions -eq "Team"}  
-ResultSize Unlimited  
[array]$Groups = $Groups | Where-Object {$_.HiddenFromExchangeClientsEnabled -eq $False}  
$Groups | Format-Table DisplayName
```

To hide a team-enabled group from Exchange clients, update the properties with the `Set-UnifiedGroup` cmdlet. For example:

```
Set-UnifiedGroup -Identity Team1 -HiddenFromExchangeClientsEnabled:$True  
-HiddenFromAddressListsEnabled:$True
```

Setting `HiddenFromExchangeClientsEnabled` to `$True` should also set `HiddenFromAddressListsEnabled` to `$True`, but it's good to be specific. You can [download a script to find and set the flags for team-enabled groups from our GitHub repository](#).

Exchange clients periodically refresh their list of groups from the server, so it might take between 15 minutes and an hour before a hidden group disappears from a client. When you hide a group from Exchange, you also remove the group from users' Favorites lists for Outlook clients. Another side effect is that because Teams has no user-accessible directory, once a group disappears from address lists, users won't be able to browse groups in the GAL and so won't know of the existence of public teams that they might want to join (or private teams, for that matter). Also, remember that most Outlook desktop clients depend on the OAB and that it takes some time for Exchange to publish the removal of groups in OAB updates that must then be downloaded and applied by clients.

Using a Team-Enabled Group as a Distribution List

Before rushing to hide the groups used by Teams from Exchange clients, remember that Teams uses the Groups service to manage team members. A group is a mail-enabled object, meaning that people can send emails to the group. A group also functions as a distribution list and it can be useful to use the group for that purpose, even when you conduct most discussions inside Teams. For example, you can't send an encrypted message to Teams, but you can send a protected email to the group and the members will receive and be able to read the content in the message (if they subscribe to the group).

It's easier to decide to hide a team when its communications are exclusively internal. Making the call for a team with guest members is harder. When you have a team with many guest members and want to send something important and time-critical to those members, you could post a message in Teams, but each guest then needs to switch to your tenant to read the message. An email to the group might be quicker and more effective if you need fast action.

Even when a team is hidden from Exchange clients, you can send messages to the group by using its SMTP address fetched through the Microsoft 365 admin center or PowerShell. For example:

```
Get-UnifiedGroup -Identity MyOffice365Group | Select PrimarySmtpAddress
```

Administrators can find this address relatively easily, but users might not be so lucky.

If you create a team and decide that you want to keep its ability to act as a distribution list, you can reveal it to Exchange by setting the property to `$False`:

```
Set-UnifiedGroup -Identity MyTeam -HiddenFromExchangeClientsEnabled:$False
```

Exchange Online delivers messages sent to a group to the Inbox folder of the group mailbox. Members of the local tenant do not receive copies of messages because they are not part of the group's subscriber list. This is by design because Teams uses a different type of conversation. For this reason, when you create a new team, Groups sets the `AutoSubscribeNewMembers` property for the group to `False` and does not populate the subscriber list.

Normally, no issue arises because the group's subscriber list is empty. That is, unless you want to be able to use the team to distribute email to all or some of the members by using the team in the same way as a distribution list. To do this, you must add the members who you want to receive emails (or calendar requests)

sent to the team to the group subscriber list. You can only do this through PowerShell. For example, this code adds two users (who must already be members of the group) to the subscriber list.

```
Add-UnifiedGroupLinks -Identity SeniorLeaders -LinkType Subscribers -Links  
Jack.Healy@Office365itpros.com, Marc.Vigneau@Office365itpros.com
```

Deleting (and Restoring) Channels and Teams

By default, any member can remove a channel or restore a deleted channel, but you can restrict this ability to team owners by updating team settings and unchecking the “allow members to delete and restore channels” setting under **Member Permissions**. Not only will this prevent accidents (unless a team owner makes a mistake), but it also stops disaffected employees who might be on the way out of the company doing something silly on the way to the exit (they might not know that the channel can be recovered). Like channel creation, Teams generates an audit record whenever someone removes a channel and writes a notification into the General channel. This information tells you who removed the channel, which might be cold comfort when you consider how much information might be lost in a deleted channel.

Removing a Channel

You cannot delete the General channel for a team, but you can remove any of the other channels using the desktop, browser, or mobile client. When someone deletes a channel, Teams puts the channel into a soft-deleted state and starts a 30-day countdown, after which the messages and metadata for the channel become irrecoverable. There’s no way to accelerate the permanent removal of a deleted channel.

During the 30-day grace period, you can recover the channel by selecting **Manage Team** and then **Channels**. Any deleted channels are listed under the set of active channels. To recover a deleted channel, select it and then click **Restore**. Teams then restores the channel to its original configuration to make its conversations available to users. One point to note is that the restored channel does not regain its previous status in the list of channels visible to the user, so users must mark the channel if they want it to show in their activity feed.

If the 30-day retention period for a deleted channel expires, you can still recover messages from a deleted channel if the team is subject to a retention hold. To do this, run a content search to find the copies of the items held for compliance purposes in the group mailbox and export the found items to a PST, ZIP file, or individual messages. Although you cannot reassemble the recovered items into the threads they had in the channel, you will be able to email them to a channel or cut and paste content from the recovered items into Teams.

Teams does not remove the folder and files belonging to a deleted channel from the SharePoint document library, including the OneNote sections associated with the deleted channel. If you want to remove the folder and files, you must do so through SharePoint. One good reason why Teams does not remove the SharePoint content is that some or all the content in the folder associated with the channel might come under the scope of a retention policy applied to the site or that individual documents might be assigned retention labels that prevent their removal.

It’s also possible that other channel tabs might be associated with content like a plan or form that will remain after the channel deletion. For this reason, it’s a good idea to note what tabs exist for a channel and investigate what content is accessed via the tabs to build up a full picture of what’s associated with the channel so that you can decide what to remove and what should be left before you go ahead with a channel deletion.

Remember that a team can have a maximum of 200 channels. If a team is at the limit and you remove some channels, the 30-day period must lapse before a Teams background process removes the channels permanently. When this process completes, new channels can be created for the team.

Removing a Team

A team owner (using the Teams client) or a tenant administrator (using an administrative interface, like PowerShell) can remove a team. When this happens, Entra ID removes the underlying group and all its resources including its SharePoint team site. For this reason, the owner must confirm that the deletion of the team should go ahead before Entra ID executes the command. This is important because once Entra ID removes the group object all the team data become inaccessible.

Generally, if you want to remove a team, do this from a Teams client as this action makes the team unavailable to all members at once. After removing the team, Teams synchronizes the deletion of the group object to Entra ID. In turn, the deletion command ripples across workloads through the normal directory synchronization process to instruct applications to remove any resources they manage for the group. It can take up to 30 minutes before all the resources belonging to a team are completely removed.

In most cases, unless you need to remove a team, it is better to leave it in place as a disused team. To do this, remove all members from the team except a single owner and update its display name to include a sign that the group is not in active use. This approach keeps the team in a state where you can revive it if needed by simply assigning new owners and members to its membership.

If you remove a team accidentally, you can recover its group (and the team) using the Microsoft 365 admin center or PowerShell, providing you do so within the 30-day retention period for deleted groups. When Entra ID recovers a team belonging to a soft-deleted group, the recovery process puts all content back in place into channels and personal chats and restores apps. Any email addresses belonging to channels in the deleted team are reactivated. Although the object for a recovered team is in the directory soon after a recovery begins, it often takes up to 24 hours before all the resources for a team are reconnected. At this point, Teams makes the recovered team available to users.

Although you can team-enable an existing group, no method exists to remove a team from a group, which you might want to do to “reset” a team by removing all channels, including the default channel, removing any tabs and apps, and reducing the membership to a single owner. The only way to reset a team is to remove the group (and all its resources) and recreate it from scratch.

Custom Emojis

The messaging policy assigned to Teams users contains two settings to control custom emojis. One (*CreateCustomEmojis*) allows users to upload PNG or GIF files to create custom emojis. The other allows users to delete custom emojis (*DeleteCustomEmojis*). Administrators can always remove custom emojis. The settings are managed through the Teams admin center or PowerShell. For example, here’s how to find which messaging policies allow users to create custom emojis.

```
Get-CsTeamsMessagingPolicy | Format-Table identity, *emojis*
```

Identity	CreateCustomEmojis	DeleteCustomEmojis
Global	False	False
Tag:Advanced	True	False
Tag:Advanced Users	True	False

A tenant can support up to 5,000 custom emojis. To create a new emoji, open the emojis and reactions menu (available by choosing the emoji icon in chats and channel conversations). Choose the custom emoji category to the far right side of the categories shown at the bottom of the menu and click the plus sign. You can now upload the source file for the emoji. Teams will reduce the file to the necessary size and show a preview of how the emoji will look in different situations.

Once someone creates a new emoji, it becomes available to everyone. Guest accounts cannot create emojis in host tenants. However, they can see the custom emojis created by others.

Obviously, administrators and team owners should keep a close eye on custom emojis to ensure that their names or graphic content are not offensive. Custom emojis are not available in organizations with educational licenses.

Channel Moderation

You might want to reserve a channel for specific posts such as group announcements. The General channel has a setting to limit new posts to group owners. Moderation serves much the same purpose for channels other than General by controlling who can post new topics and replies to the channel.

Moderation is supported for both public and private teams. To enable moderation, select the channel you want to control and then **Manage channel** from the [...] menu. You can then turn moderation on or off for the channel (the default is Off). Even if moderation is disabled, you still have the option to restrict the creation of new topics (posts) to any member of the team or everyone except guests. After enabling moderation for a channel, the next step is to decide who the moderators should be (Figure 12-4). By default, all team owners are moderators, but you can select a different set of owners and members to act as moderators. Click **Manage** to change the set of moderators. Up to 100 moderators can be defined for a channel.

After moderation is enabled, members who aren't moderators cannot create new conversations in the channel and will see an informational banner saying, "only channel moderators can post in this channel." In channels where moderation is enabled, it's a good idea to create an "Anything Goes" topic where people can discuss anything they like, including appealing to the channel moderators to create a new topic to discuss something specific.

The screenshot shows the 'Channel details' section of a Microsoft Teams channel named '2025 Edition (11th)'. The channel was launched on July 1, 2024. The 'Moderation' section is expanded, showing the following configuration:

- Channel moderation:** Set to 'On'.
- Who are the moderators?**: 'Team owners' is selected, and there is a 'Manage' button.
- Who can start a new post?**: 'Only moderators' is selected.
- Team member permissions** (checkboxes):
 - Allow members to reply to channel messages
 - Allow members to pin channel messages
 - Allow bots to submit channel messages
 - Allow connectors to submit channel messages

Figure 12-4: Setting up moderation for a channel

Settings also control if members can reply to posts and if automated processes (workflows) can submit messages to the channel. For example, you could use this setting in situations where the channel hosts automated notifications about builds performed by Visual Studio.

You can't update moderation settings for a channel with a Teams PowerShell cmdlet, but you can [with the Graph API](#).

Managing Settings for a Team

Team owners can manage team settings through the ellipsis [...] menu found beside the team name. Select **Manage Team** from the menu to access the available settings:

- **Members:** List existing team members (including guests), change roles (from Member to Owner and vice versa), remove members from the team, or add new members. When you add or remove members to a team, Teams updates the group membership.
- **Pending Requests:** Process any waiting requests to join the team. This tab is only visible for private teams.
- **Channels:** Manage channels for the team. As mentioned earlier, if a channel is important and should be brought to the attention of team members, a team owner can check the auto-show box to force the inclusion of the channel in each member's *Your teams* list.
- **Analytics:** Gain insight into the level of activity for the team over the last seven, 30, or 90 days for all channels or individual channels.
- **Settings:** Settings to control the team picture; assign permissions to users and guests; allow team members to use @mentions to reference other members, teams, and channels; and use stickers and memes (including the uploading of new memes). You can also upload a graphic file (of up to 4 MB) to add a team picture. A file measuring 640 x 420 pixels works well. Under **Member permissions**, you control the actions users can take within a team, such as whether they can add or remove channels, tabs, or apps; restore deleted channels; and whether owners and members can delete messages. If your tenant deploys a group expiration policy, you'll see the expiry date for the team and be able to renew it here. Settings also include the ability to manage **Tags**, a way to address subsets of members (see the Teams chapter).
- **Tags.** Shows the set of tags available for use to address members in channel conversations. Users allowed to create tags can create them here.
- **Analytics:** View usage information for the team and individual channels. See the later section about reporting usage of teams.
- **Apps:** Add or remove an app for the team. Apps include first-party apps like Forms, Planner, OneNote, SharePoint, and Stream as well as third-party apps like the Hipmunk bot installed in the team.

Figure 12-5 shows the set of channels in a team. The ellipsis menu includes the option to **Delete the team**, an action that removes the underlying group and any other resources belonging to the group. To edit team properties, select the **Settings** option under Manage team. Here you can amend:

- The team name (display name). When you rename a team, you change the display name for the group. The change, therefore, affects applications like Groups and Planner. Because of the need to synchronize directories and clients, the name change might take some time before it is fully effective.
- Team description.
- Privacy (change the team from Public or Private or vice versa).
- Sensitivity (or classification).

These properties apply to all workloads using the group. Updating team settings is the equivalent of running the *Set-UnifiedGroup* cmdlet to change group properties. For example:

```
Set-UnifiedGroup -Identity HydraProjectTeam -DisplayName "The New Hydra Project Team" -Notes "A very nice group of people that is team-enabled to get stuff done" -AccessType Public -Classification Confidential
```

Name	Show for me	Recommend channel	Description	Type	Last activity	
General	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The Ultimate and Best Guide to Office...		28/2/2024	...
2024 Edition (10th)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Planned Publication date 1 July 2023		1/6/2024	...
2025 Edition (11th)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	The 11th or 2025 Edition, launched 1 J...		1/6/2024	...
Office 365 for IT P...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Feed from the Office 365 for IT Pros B...		3/6/2024	...
2020 Edition	<input type="checkbox"/>	<input checked="" type="checkbox"/>			4/6/2020	...
Stream Videos	<input type="checkbox"/>	<input type="checkbox"/>			24/6/2022	...
2022 Edition	<input type="checkbox"/>	<input type="checkbox"/>	All about the 2022 (8th) edition of Off...		24/6/2022	...
2023 Edition (9th)	<input type="checkbox"/>	<input type="checkbox"/>			5/6/2023	...

Figure 12-5: Managing the set of channels in a team

As explained in the Information Protection chapter, if you use sensitivity labels to control group settings for privacy and classification, those settings come from the label assigned to the group. The only way to update the settings is to change the sensitivity label to one which imports the settings you want to use.

System Messages for Membership Changes

Teams posts system messages about updates to team settings, including those made with PowerShell, in the information pane. If you add or delete members for a team, system messages tell team members about the change. If someone uses a Graph API call (including the Teams clients and the *Add-TeamUser* cmdlet) to add or remove a member, the system message includes the display names of the member and the person (owner or administrator) who took the action. Changes made through the other administrative interfaces, such as the *Add-UnifiedGroupLinks* and *Remove-UnifiedGroupLinks* cmdlets (Exchange Online module) or *Add-MgGroupMember* and *Remove-MgGroupMemberDirectoryObjectByRef* cmdlets (Microsoft Graph PowerShell SDK), don't include the name of the person who took the action. It takes some time before Teams posts the system messages to inform members about changes. Changes that occur through other workloads, like Exchange Online or SharePoint Online, update Entra ID first. Subsequently, a background process called Microsoft Teams Aad Sync, synchronizes the changes to Teams. If you want membership changes to be effective immediately, you should manage team membership through the Teams admin center or Teams client rather than using other administrative interfaces.

Guest Access for Teams

The mechanics of guest user access for Teams function like those for Microsoft 365 Groups. Team owners add guests to teams, joining invitations go to the email address identifying the guests, who then redeem the invitation to complete the process and join the team. As part of the Azure B2B collaboration process, Teams creates guest accounts to allow guests to authenticate their access to resources. The Microsoft Invitations service generates the invitations and Teams manages the redemption process, including the verification of the guest account. You can invite anyone to be a guest if they have a valid email address.

Users can accept invitations to join other organizations as a guest from any client. The desktop and browser clients support other features through the Accounts and Orgs section of Teams settings, including the ability to:

- Decline an invitation received to join a team in another organization.
- Leave an organization by removing their guest account. This option takes the user to the Entra ID [Organizations page](#) to choose the tenant to leave.
- Hide or show organizations where the user has a guest account from the drop-down list displayed by Teams when the user selects a target organization for switching. If you hide an organization, Teams no longer notifies you when something happens (like an @ mention) in that tenant.

After a guest joins a team in a tenant, they don't have to accept invitations to join other teams through the links contained in the emailed notifications. Instead, the Teams apps detect that the guest is now part of other teams and perform an in-app redemption to add those teams to the list available to the guest.

A user of the free Teams version can be a guest in a tenant that uses the enterprise version and can switch between free and enterprise tenants. The same is true for users belonging to enterprise tenants, who can switch to guest accounts in free tenants.

Enabling Guest Access for Teams

Because Teams consumes multiple Microsoft cloud services, different settings in the services combine to control guest access. In order of priority, these are:

1. **Entra ID.** The first hurdle is to make sure that Entra ID allows group owners and members to invite guests. In the **External Identities** section of the Entra admin center, the **External collaboration settings** control external access to Entra ID. Under Guest invite settings, the default setting is "*member users and users assigned to specific admin roles can invite guest users including guests with member permissions.*" If the setting is more restrictive, for instance, the control is set to "*only users assigned to specific admin roles can invite guest users,*" any attempt by users who don't hold an administrative role such as Groups administrator fails.
2. **Groups.** In the Settings-section of the Microsoft 365 Admin Center, select Org Settings, then Microsoft 365 Groups, and make sure that *Let group members outside the organization access group content* and *Let group owners add people outside the organization to groups* are both On. When set, you can invite guests to join Teams. If you have specific teams that discuss sensitive information, you can block the ability of the owner to add guests to those teams by either editing the properties of the teams or by assigning a sensitivity label to the teams which prohibit guest membership. For more information, see the discussion about how to block guests for specific groups in the Groups chapter.
3. **Teams.** Go to the Teams admin center and then the **Guest access** setting under **Users** to make sure that the **Guest access** slider is set to *On* (the default for this setting). Other settings in this policy control the functionality available to guests, such as if they can edit their sent messages. Guest users don't need a license to access Teams. You can also enable guest access to Teams with PowerShell by running the [`Set-CsTeamsClientConfiguration`](#) cmdlet and setting the *AllowGuestUser* setting to *\$True*.

4. **SharePoint.** In the SharePoint Admin Center, under External Sharing, set *Let users share SharePoint Online and OneDrive for Business content with people outside the organization* to On. This enables guest access to the Files in SharePoint document libraries used by Teams and to files in users' OneDrive sites shared in personal chats.

With all settings turned on, the full spectrum for guest access is supported for all teams in the tenant.

Teams shared channels do not use guest accounts. Instead, users connect to shared channels in other tenants using B2B Direct Connect. See the Identities chapter for more information on this topic.

Adding Guests to Teams

With all the correct settings in place, team owners can add guests. It is important to understand that the group and its associated team share a common membership list, including guests. Therefore, if you add a guest to the group, the guest gains access to the team and vice versa. Sometimes a small delay happens between adding or removing a guest from the membership and that action showing up when viewing membership, but background synchronization processes make sure that any addition or removal of guests applies across both Teams and Groups.

To add a guest member, select **Manage team** and then **Members**, or use **Add members** from the ellipsis menu. You then input the email address of the new member (Figure 12-6). In this case, the email address entered for the guest was Jack.Smith@contoso.com. When a guest appears in a team, its display name has a *(Guest)* suffix. This is a language-specific string added by Teams to mark a member as external. The string is translated when displayed by Teams clients and notifications – for example, if a guest user runs Teams in Spanish and you receive an email notification for something they post, you'll see *(Invitado)* after their name. You cannot change the guest suffix because that is a visual reminder to other members that a guest is an external person, but administrators can edit the display name of the Entra ID guest account to add additional information (such as the person's company) if necessary.

Add members to Microsoft Graph Gurus

Start typing a name, distribution list, or security group to add to your team. You can also add people outside your organisation as guests by typing their email addresses. People outside your org will get an email letting them know they've been added. Learn about adding guests



Figure 12-6: Adding guests to team membership

When the information for the guest member is complete, press **Add**. Teams checks whether a guest account for this address already exists in the tenant directory and adds it to the membership if found. If not, Entra ID creates a new guest account. Teams then adds the account to the team membership and generates an invitation for the user to redeem. The invitation has all the information necessary for the recipient to know about the team they are joining, including a GUID to find the right tenant, another GUID for the team, and a

token request to redeem the invitation to join the team. The recipient redeems the invitation by clicking the **Open Microsoft Teams** link in the message, which then invokes the necessary flow to confirm the user's details, update the guest account for the user with credentials to allow them to connect to the tenant, and access the team. Entra ID logs the redemption in a "redeem external user invite" audit record.

To give a visual clue to tenant users that they should be careful about the information shared externally, once you add a guest to a team, Teams displays the number of guests in the team in the top right-hand corner of the conversations pane.

Updating Guest Information: Do not worry if you forget to update the display name for a guest when you add them as you can always update it afterward. You can edit the contact information for the guest through the Microsoft 365 admin center, update the guest account properties in the Entra admin center, or run the *Update-MgUser* cmdlet. For example, this code updates the display name for the guest account created for John.Smith@contoso.com bypassing the user principal name as the object identifier. It also updates the user's job title and city as Teams displays these properties when you view a team. Finally, we update the telephone and mobile numbers for the user so that they appear when someone looks at their contact card.

```
Update-MgUser -User John.Smith_contoso.com#EXT#office365itpros.onmicrosoft.com  
-DisplayName "John Smith (Contoso)" -JobTitle "Account Manager" -City "NY" -BusinessPhones "+1  
617 551 6531" -MobilePhone "+1 650 561 4136"
```

It's also a good idea to upload photos for guest accounts. You can either upload an actual photo (the nice approach) or use a default photo to mark the guest as an external person. In either case, uploading a photo for a guest is done by editing their account in the Entra admin center or by running the *Set-MgUserPhotoContent* cmdlet. See the Groups chapter for more information. Teams must synchronize with Entra ID before the updated account information shows up in the Teams clients.

Every guest has an Entra ID user account in the host tenant. An administrator can amend settings for the guest user account (like their photo), but because guests don't have mailboxes in the tenant, they can't set an out of office notification or any other feature which depends on a mailbox.

Multi-Factor Authentication for Guests

Like the other Microsoft 365 applications, Teams supports multi-factor authentication (MFA). If your tenant implements an Azure conditional access policy to require MFA, you can include guest members in the scope of the policy to force them to use MFA to connect to Teams, even if their home tenant does not require MFA for connection to services. The logic here is that a tenant always controls its resources and can therefore dictate the level of authentication required to access those resources.

To ensure that a conditional access policy applies to guest users, choose *All Guests and External Users* as the target group for the policy to apply to.

Blocking Guests from Specific Domains

If you do not want team owners to add guests from specific domains, you can create a block list using the Entra B2B Collaboration policy. The same policy can also create an allow list to restrict guest user access to specific domains, but a tenant can only support either an allow or a block list. When a policy is in place, team owners cannot add guests from blocked domains. However, any guests from blocked domains who are already members of teams continue as before and that guest can be added to other teams because Teams only uses the deny list when adding new guest accounts. It could be the case that the account was added by another application (to share a SharePoint document, for instance) that has nothing to do with Teams.

If you want to revoke membership for guests belonging to blocked domains, you must use PowerShell to search the membership lists for all Microsoft 365 Groups and remove any guest members found that belong

to those domains. An example of how to remove a user whom you wish to block is in the Groups chapter. If you want to ensure that no guest users are added to specific teams, disable the ability for team owners to add guests to those teams with a sensitivity label or by updating the policy setting for the group.

Switching Between Tenants

When a user with a guest account wants to access teams in your domain, they must "switch" Teams client by signing into your tenant using their guest account. Switching to work as a guest into another tenant means that an account has a limited view of the Teams environment within that tenant when compared to what they can do in their home tenant. Guests can only see teams to which they belong and cannot browse to join other public teams; they cannot see organizational information about other members, nor can they create new teams or add apps to channels. Because guests cannot access the directory, they cannot update the picture for their account, or any other setting related to their account such as the display name. In addition, they cannot browse the directory to find people to chat with. Instead, guests enter the email address of the person they are looking for and Teams checks the directory and creates a chat if that person exists.

On the other hand, guests can join in private and public conversations, take part in video and audio chats and access files from the team SharePoint site (or the sites used by private channels, if their account is added to the membership of private channels). Another point to note is that guests can only access applications available to the team if they have the right credentials and the application supports guest user access. It is as if they signed into your tenant with more restricted access than a normal tenant user has, which is exactly what you want.

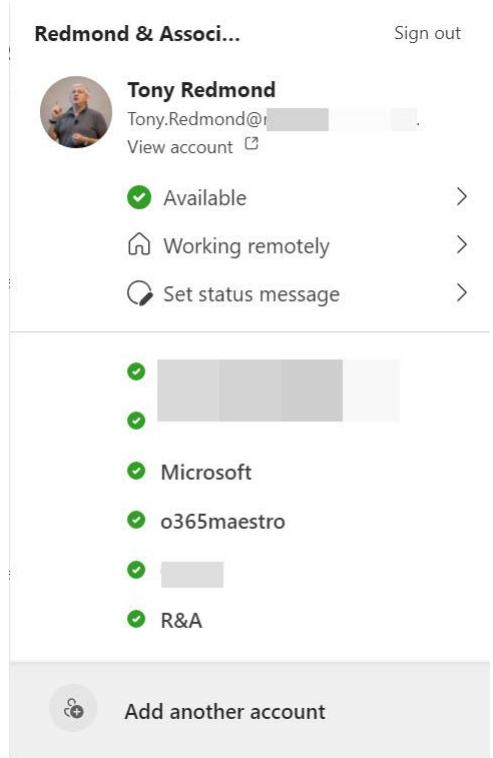


Figure 12-7: Using the account manager to switch to a tenant

Assuming you have an account in at least one other tenant where Teams is active, switching to an account in a different tenant is simple. In the desktop and browser clients, click the name of the tenant you're currently connected to in the title bar to reveal the set of known tenants in your Teams profile. A tenant is listed only if your account is added to at least one team in that tenant. If your access expires for a tenant, you'll be asked to reauthenticate before you can connect. For mobile clients, click the hamburger menu in the top left-hand corner and select the target tenant from the list shown at the bottom of the screen. In Figure 12-7, the

account manager (top right of the main Teams window in the desktop client) shows that six host tenants (and the home tenant) are available for switching. When you select a different tenant, Teams switches to the target tenant and displays the teams that the user belongs to in that tenant.

When you have guest accounts in one or more tenants, Teams monitors the activity in those tenants and posts notifications when you're mentioned in chats or channel conversations. The notifications appear to the right of the account manager.

Personal Account

Users can add a personal account to their Teams profile. A personal account is a Microsoft Services account with a valid email address. When someone uses Teams with a personal account, they switch away from Teams enterprise to Teams consumer. Teams consumer supports very different functionality to Teams enterprise and two separate clients (windows) are active after the user signs into Teams consumer. The user can move from one client to the other as they like.

Removing Guests

You remove guests from a team in the same way as you remove a tenant user. Select **Manage team** from the menu and then **Remove** for the user in the member list. Alternatively, you can run the *Remove-TeamUser* cmdlet to remove the user from the group. For example, this command removes the guest Joan.Smith@contoso.com from the Industry News team:

```
$TeamId = (Get-UnifiedGroup -Identity "Industry News").ExternalDirectoryObjectId  
Remove-TeamUser -GroupId $TeamId -User "Joan.Smith@contoso.com"
```

Removing an external member from a team does not remove the guest account from Entra ID. If you want to remove an external user from all teams in a tenant, you can remove their guest account using the Entra admin center, the Microsoft 365 admin center, or by running the *Remove-MgUser* cmdlet. Removing the account removes membership from all teams and groups and removes any sharing permission the user has for SharePoint and OneDrive for Business files in the tenant.

Email Integration for Teams Channels

The Teams architecture chapter discusses the various methods available to bridge the gap between email and Teams. The *Email Integration* setting for the tenant (managed through the Teams settings section of the Teams admin center) controls if channels can receive SMTP addresses to allow them to accept emails. This is a useful way for people to introduce a new topic into a channel using information contained in emails. To retrieve the email address of a channel, use the desktop or web client to click the ellipsis menu for the channel, select **Get email address**, and then **Copy** (Figure 12-8) to copy the address to the clipboard. If an email address does not already exist for the channel, Teams creates one.

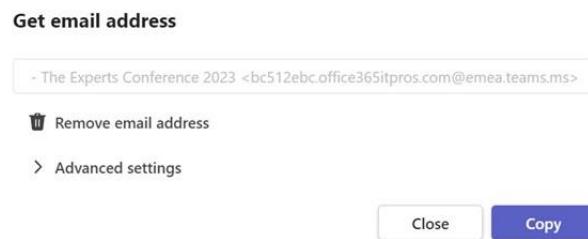


Figure 12-8: Retrieving the email address for a channel

Alternatively, an administrator can provision an email address for a channel using the `New-MgTeamChannelEmail` cmdlet. This code finds the target channel in a team and calls the cmdlet to provision the channel with an email address:

```
$Team = Get-MgTeam -filter "DisplayName eq 'Privacy Advocates'"
$Channel = Get-MgTeamChannel -filter "DisplayName eq 'Human Rights'" -Team $Team.Id
New-MgTeamChannelEmail -ChannelId $Channel.Id -TeamId $Team.Id

Email
-----
d44f4c45.Office365itpros.com@emea.teams.ms
```

Teams signals a 409 (conflict) errors if the channel already has an email address.

Once created, people can use the address to send a message to the channel. Any team member can retrieve the email address for a channel, but guest members can't force Teams to create an email address for a channel that doesn't already have one.

Originally, the default was to allow anyone inside or outside the tenant to use the email address to send a message to the channel. The current default (introduced with the Teams 2.1 client) restricts access to members of the team. If necessary, a team owner can use the **Advanced settings** option to restrict the acceptance of messages to allow anyone to send messages to the channel or restrict inbound messages to certain domains.

At the organization level, tenant administrators can block all channels from receiving email or define a **list of domains allowed** to send email to channels. Any user from these domains can send an email to a channel in the tenant, including private and shared channels. If you create an accepted domains list, make sure to include all the domains you wish to allow communicate with Teams via email. Note that you cannot specify a wildcard domain like *.onmicrosoft.com.

You can also use PowerShell to update the set of accepted domains for the tenant. In this example, we pass the set of accepted domains as a string with each domain separated by a semi-colon (don't leave any spaces). The `Set-CsTeamsClientConfiguration` updates the configuration, which we can then check with `Get-CsTeamsClientConfiguration`.

```
[string]$SenderDomains = "Microsoft.com;Office365itpros.com;contoso.com"
Set-CsTeamsClientConfiguration -RestrictedSenderList $SenderDomains -AllowEmailIntoChannel $True
Get-CsTeamsClientConfiguration | Select AllowEmailIntoChannel, RestrictedSenderList
```

It can take a couple of hours before the updated list of accepted domains becomes active. When delivery restrictions are in place, Teams rejects emails sent to a channel from senders not on the allowed list, and the sender receives a message from Teams. The text of the notification is something like this:

Delivery has failed to these recipients or groups:

1e2d0eb3.office365itpros.com@emea.teams.ms

The administrator has restricted permissions to send emails to this channel.

Team members don't receive copies of emails delivered to a channel. If you want people to receive a copy of a message sent to a channel, add their email addresses to the message.

Managing Channel Email Addresses

When Teams creates an email address for a channel, it also creates a mailbox in a special tenant dedicated to Teams email processing and assigns the email address to the mailbox. The channel's email address is in the form `<unique-identifier>.tenant-domain@region.teams.ms`. Tenants cannot change the format of the address or the domain it uses to make it more human-friendly.

For example, the email address `b400aa20.tenant-smtpaddress@emea.teams.ms` belongs to a tenant in the EMEA region. The SMTP domain included in the email address generated for the channel uses the domain defined in the email address policy for the tenant. If a separate email address policy exists for Microsoft 365 groups, Teams uses that domain.

After creating a mailbox to handle inbound email for the channel, Teams creates a connector (see below) to link the mailbox to the channel so that any email arriving in the mailbox flows through to the channel.

Dedicated infrastructure exists to host Teams mailboxes in every Microsoft data center region supported by Teams. It's worth noting here that because Teams uses a connector to bring messages into a channel, any information barrier policies used by the organization don't apply. This means that someone otherwise blocked from communicating with team members can send emails to them via the channel.

Any team member (except guests) can use the **Remove email address** option to nullify the email address for a channel. Allowing users to remove the email address used for inbound communications is in line with the general rule that everyone shares equal access to team resources, but it is easy to see how this could lead to problems if people rely on the address to communicate with the channel. It is easy to reconnect email access for a channel by using the **Get email address** option again, but Teams does not restore the old address to the channel and generates a new address instead.

Teams captures audit records when team members generate or remove channel email addresses. Here's an example of [how to interrogate the audit log to find the relevant records](#). Teams doesn't expose email addresses in the properties reported for a channel in the `Get-TeamChannel` PowerShell cmdlet. You can't generate a report of Teams channels with email addresses using pure PowerShell, but you can with [a combination of PowerShell and the Microsoft Graph](#).

Posting to a Channel from Exchange Online

To make it easier for people to post emails to a channel, you can create an Exchange Online mail contact with the channel's email address and give the mail contact a suitable display name. The mail contact will appear in the Exchange GAL and users can add it to messages as easily as any other email address, including [using the mail contact in a distribution list](#). If someone changes the email address for the channel, you'll have to update the mail contact because no synchronization exists for these objects between Exchange and Teams.

Messages sent to the email address of the Microsoft 365 group used by a team go to the group mailbox. Members who subscribe to the group receive copies, but Exchange will not deliver a copy of the message to a channel in the team unless you add the channel's email address as an external member of the team. For example, let's assume that you want any email sent to the Corporate Business Development group to show up in Teams and you create a channel called Email Communications for this purpose. You can then get the email address for the channel and add it to the group as a new guest member with OWA. Exchange Online delivers a copy of any messages sent to the group thereafter to the channel. Guest user accounts do not appear in the Exchange GAL.

Use BCC to Stop Mail Storms: The email address for a Teams channel functions in the same way as any other email address in that you can use it as a message recipient. However, there's a very good reason for always using BCC when sending emails to Teams. The purpose of a Teams email address is to allow users to start new discussions in a channel with content that already exists in emails. You do not want the channel to take part in a lively back-and-forth email conversation because every interaction shows up as a new thread in the channel and can confuse team members. Use BCC to address email for a channel and then develop the conversation forward in the channel.

Message Hygiene for Inbound Email to Teams

Because the mailboxes used by Teams are part of the Microsoft 365 infrastructure, inbound messages go through Exchange Online Protection (EOP). Although EOP will stop the delivery of malware to Teams, the special nature of the configuration used by Teams means that inbound mail does not go through the same processing as the email stream for a regular customer tenant. For example, if you license Office 365 E5 and configure the Microsoft Defender for Office 365 policy to enable Safe Attachments and Dynamic Delivery, you expect that EOP processes all attachments in this manner. However, this will not happen for messages routed through Teams. On the other hand, if you configure Microsoft Defender for SharePoint, when Teams captures the message files in the SharePoint document library (see below), Microsoft Defender processes any attachments at that point.

Teams will not deliver a message to a channel if the message has more than 20 file attachments or more than 50 inline images. Exchange Online sends a non-delivery-notification to the sender whenever Teams rejects a message.

SharePoint Captures Email Sent to Teams Channels

When a channel receives an email, the text of the message appears as a new topic in the channel. If the text exceeds the limit for a contribution to a chat (25 KB, or roughly 20,000 characters including spaces), you see some text but need to download the “original email” to view the full content. You cannot reply to an inbound message because Teams has no other access to email except its ability to receive inbound messages. Any attempt to reply to an inbound email generates the response that your reply will only be visible in Teams.

When Teams receives a message via email, it strips any attachment and stores the file in the channel folder created in the SharePoint Online document library for the team (a separate folder exists for each channel in the team). Originally, Teams held copies of received messages in a single *Email Messages* folder. To improve performance, Teams creates a separate folder per month named after the month. For instance, the folder used for February 2021 is **EmailMessages_2_2021**.

In addition to attachments, Teams captures a copy of the message as an *.eml* file and keeps the file in the same location. Keeping copies of messages and attachments received by Teams in SharePoint means that Microsoft Search can index the information to make it available for eDiscovery. Users can download a copy of the original message from email conversations posted to the channel.

Because copies of messages sent to channels end up in SharePoint Online, each delivery of a message to a channel creates an *Uploaded File* audit record. You’ll see that the user noted in the audit record is *app@sharepoint*, a background process that performs many management operations for SharePoint. This process copies the message from Teams to SharePoint.

Teams and Compliance

Teams stores chat and channel messages in a data store hosted by Azure Cosmos DB. The information in the Teams data store is not directly accessible to the data governance framework. It is obvious that many interesting conversations occur in Teams and that the information discussed in these conversations might be of interest to eDiscovery investigations. The same fear that eDiscovery investigations might not have access to all relevant information exists when employees use third-party chat networks like Slack.

Despite the lack of access to the native Teams data stores, Teams has other mechanisms to support many of the data governance technologies available in Microsoft 365, including:

- **eDiscovery:** The Microsoft 365 substrate captures and indexes compliance records so that content searches can find, preview, and export these items. The substrate captures compliance records for Teams chats and conversations, meetings, adaptive card content, and call data records.
- **Retention:** Teams supports the application of retention policies against messages sent to Teams channels and private/group chats.
- **Communication Compliance:** Teams supports the capture of messages matched against classifiers identifying offensive, threatening, or other problematic interactions. Administrators can remove messages that violate policies to make them inaccessible to anyone but the sender. Microsoft automatically creates a communication compliance policy called *User-reported messages* for investigators to process chat messages flagged using the Report a concern option.
- **Data Loss Prevention:** Teams supports the checking of personal chats and channel messages to detect the presence of sensitive information types.
- **High-value audit events:** If your tenant has the necessary licenses (Office 365 E5 is one example), Teams generates audit events for meetings to capture details of the meetings and their participants. See [this article](#) for more information.

Retention policies govern the preservation or removal of data as required by the organization. By default, Teams does not remove any conversation or other information belonging to a channel or chat. This data remains in the Teams data stores or the underlying application (for example, Planner) unless a user or team owner takes action to remove the data. For instance, a user might delete a document from the SharePoint Online site belonging to a team or a task from Planner.

If you want to ensure the retention of Teams data for a defined period or removed after a certain period, you must deploy retention policies to cover Teams messages (chat and channel conversations) and any other repository used by Teams, such as SharePoint Online. We'll discuss how to use retention policies to manage Teams data later. A more general discussion of retention policies to cover other Microsoft 365 data is in the Compliance chapter.

Capturing Teams Compliance Data

To ensure that Teams conversations are available for eDiscovery, the Microsoft 365 substrate captures copies of the messages sent in personal chats and channel conversations as items in Exchange Online mailboxes, including messages emailed to channels. These mail items are compliance records. They are imperfect copies of the complete Teams message data as they contain the information needed for eDiscovery and other compliance functionality, such as messages detected by trainable classifiers used by communication compliance policies. The substrate stores the compliance records in the **TeamsMessagesData** folder in the non-IPM part of user and group mailboxes. You can see how many compliance records exist in these mailboxes with PowerShell (see [this article](#)). Because the compliance messages exist in Exchange Online mailboxes, Microsoft Search indexes their content and metadata to make the items available for eDiscovery.

As people communicate in chats and channel conversations, the Microsoft 365 substrate captures each message as a separate compliance record. A complete conversation between multiple people might involve thirty or more contributions, each of which exists as a separate compliance record. The compliance records are mail items, so they have a sender (the author), a recipient (the group mailbox for channel conversations or user mailboxes for personal chats), and a timestamp for when Teams created the item. Like other mail items, you can examine the properties and content of Teams compliance items using [the MFCMAPI program](#). If the author or a team owner edits a message, the substrate captures compliance records for the original message and every edited version of the message.

The Microsoft 365 substrate captures compliance records as follows:

- **Personal and group chats:** The substrate creates compliance records in the *TeamsMessagesData* folder of the mailboxes of the participating users. For example, if John and Pat have a chat, the substrate creates compliance records for the chat in both their mailboxes. If a group chat involves ten people, compliance records for every message in the chat exist in all ten mailboxes. Compliance records for chats in private meetings are also in user mailboxes.
- **Regular channel conversations:** The substrate captures compliance for messages posted to channels in the group mailbox belonging to the team. Compliance records for conversations in all channels in a team are intermingled.
- **Private channel conversations:** The substrate captures compliance records for these messages in the user mailboxes of the channel members.
- **Shared channel conversations:** The substrate captures compliance records for these messages in a special cloud-only mailbox created for the shared channel. This mailbox is inaccessible to regular email clients and is also known as a *SubstrateGroup* mailbox.
- **Meetings and Calls.** The substrate generates compliance records as the calling infrastructure creates records of meetings and calls. Meetings include scheduled private meetings and ad-hoc meetings associated with a channel. Group chats that include more than two people are also in this category. Calls cover one-to-one calls. The substrate captures compliance records when users from your tenant participate in meeting chats hosted by another tenant.
- **Meeting artifacts:** These artifacts include meeting attendance reports, transcripts, whiteboards shared during meetings, and recordings. As described below, Teams captures meeting and webinar information in Microsoft Lists stored in the meeting organizer's OneDrive for Business account. This data is available for eDiscovery. Transcripts generated from Teams meeting recordings are in the OneDrive for Business account of the person (usually the organizer) who initiates the recording. OneDrive hides this data from users. A background process indexes the spoken words from the transcripts against meeting recordings to allow concurrent playback of video and text. The text (spoken words) is available to SharePoint Search but is not yet available for eDiscovery. See the Managing Video chapter for more information about Teams meeting recordings.
- **Adaptive card data:** First-party and third-party apps integrated with Teams can use adaptive cards as part of their user interface. Another category is cards representing data from network sources created in channels using workflows. The substrate captures compliance items for adaptive cards. If an app creates a card in a personal or group chat, the substrate creates compliance records in the mailboxes of all those involved in the chat. Compliance records for cards created in channel conversations are in the group mailbox of the team which owns the channel.

Compliance records are available very soon after users or apps create messages in Teams (usually a matter of seconds, never more than a few minutes). The substrate does not capture records for draft messages. These messages remain in the local client cache until the user eventually sends them, at which point the substrate creates a compliance record.

Warning: The compliance records created for voice memos generated in personal chats by Teams mobile clients do not contain any metadata or other information necessary for inclusion in content indexes. No attempt is made to transcribe the voice message into a form that can be indexed, so these memos cannot be found by content searches. Because some Microsoft 365 workloads do not support eDiscovery, other challenges for Teams compliance capture include:

- Planner tasks.
- Whiteboards shared in meetings.
- Data belonging to third-party apps stored outside Microsoft 365.
- Loop components in Teams chat. Compliance records exist, but they don't contain any of the content for the loop component.

Capture of Webinar Event Data

The Microsoft 365 substrate captures attendance information for Teams meetings as items in the hidden `93c8660e-1330-4e40-8fda-fd27f9eafe10AttendanceReportV3Collection` folder in the non-IPM part of the meeting organizer's mailbox. The data in these items is sufficient to display the attendance report for a regular meeting.

Special processing occurs to make information about meetings configured as webinars available for eDiscovery. For a webinar, Teams creates three lists in the meeting organizer's OneDrive for Business account. These lists are:

- **Event:** Stores event information such as its start and end time and webinar description and title. The `ThreadId` for the webinar is stored in this list. The webinar title and description can be edited in the list but the information created by Teams for the meeting cannot.
- **Questionnaire:** Stores the attendance records for individual webinar attendees. The information about attendee details (like name and email address) can be edited in the list but information relating to the Teams meeting (like its URI) cannot.
- **Speakers:** Stores details of the speakers such as their names and bios. This information can be edited in the list.

The lists used to hold webinar data are not usually visible to users unless they navigate to the lists section of their OneDrive account (Site Settings, then Site Libraries and Lists). They can then retrieve the URL to a list and use the URL to access the data in a browser.

Information held in webinar lists (including any updates) is available for searching through SharePoint Search or Microsoft 365 eDiscovery. See [this article](#) for more information.

If your organization has Office 365 E5 or Microsoft 365 E5 compliance licenses, Teams generates audit events for meetings (`MeetingDetail`) and participants (`MeetingParticipantDetail`). See the section on advanced auditing in the Report and Auditing chapter.

Compliance and Communication Compliance Policies

Teams supports communication compliance policies. When a user or team comes within the scope of a policy, copies of their messages which violate communications policies are captured in a special mailbox and kept there until reviewed. The messages generated for review are like those captured for compliance purposes, but they go through a different process. During the review process, messages identified as violations can be blocked so that recipients can no longer see these messages. The sender can still see the message, but it is highlighted as being blocked due to a policy violation. See the Compliance chapter for more information about communication compliance policies.

Compliance Records for Private Channels

Two challenges exist for compliance records collected for private channels:

- *Compliance records for private channel messages are in member mailboxes:* Private channels don't have a group mailbox. For this reason, Exchange Online stores the compliance records captured for conversations in the private channel in the personal mailboxes of channel members like the way that it stores records for group chats. From a content search perspective, it means that the substrate captures more copies of compliance records (up to 250 copies of each message posted to a private channel). Another way of looking at this is that you'll find a record if you add a single member of a private channel to a content search. The compliance records in private mailboxes contain a mixture of records for private chats, group chats, and private channel conversations. The items for private channel messages have different MAPI property values to chat messages. For instance, property

0x0DE001F is *MicrosoftTeams* for chat messages but *MicrosoftTeamsChannelMessages* for private channel messages.

Because compliance records for private channel conversations are in user mailboxes, retention policies must apply special processing to find and deal with compliance records created for private channels. For this reason, retention policies to process private channel messages are separate from other retention policies. By contrast, the substrate stores compliance records captured for Teams shared channels in cloud-only mailboxes (like those used for hybrid and guest users), meaning that regular retention processing for Teams channel messages covers these items.

- *eDiscovery searches might not include some SharePoint sites:* Private and shared channels use special hidden SharePoint sites to store their documents. If you include teams in content searches, the search only includes documents in the standard SharePoint sites used by the teams. To ensure searches process documents stored in the special sites used by private and shared channels, you must add the URLs for the channel sites to the content search locations.

This code returns the URLs for sites belonging to Teams private channels. If you exclude the filter against the set of sites returned by the *Get-SPOSite* cmdlet, the set includes both private and shared channels.

```
[array]$Sites = Get-SPOSite -Template "TeamChannel#1" -Limit All | Where-Object {$_._TeamsChannelType -eq "PrivateChannel"}

ForEach ($Site in $Sites) {
    $SPOSite = Get-SPOSite -Identity $Site.url -Detailed
    $Group = Get-UnifiedGroup -Identity $SPOSite.RelatedGroupID.Guid
    Write-Host "Team" $Group.DisplayName "owns private channel site" $Site.URL}
```

Earlier iterations of private channels used the *TeamChannel#0* template. Microsoft switched the template in mid-2021. However, it's possible that you might find some sites with the old template.

Teams Control Messages

Along with compliance records generated when users send messages, Teams captures control messages for events such as:

- Adding or removing a chat participant.
- Renaming a chat.
- Renaming a team or updating the team description.
- Renaming a channel or updating the channel description (regular, shared, and private channels).
- Adding or deleting a channel.
- Updating a member to grant or remove the owner role.
- Start or stop sharing a channel with a team.

Retention policies applies to Teams chat or channel conversations also process control messages.

Teams Compliance Record Structure

Like other mail items stored in an Exchange Online mailbox, a Teams compliance record is composed of a set of MAPI properties that can be viewed using a MAPI editor like [MFCMAPI](#). The properties include:

- *SkypeInternalIds:* a list of GUIDs for each of the participants (other than the sender) in the conversation. Teams uses GUIDs internally to avoid problems with user display and principal names, both of which can change over time due to marriage, divorce, or other circumstances. Teams resolves the GUIDs for display and stores the display names in the *PR_DISPLAY_TO* property.
- *ParentMessageId:* The reply identifier for the message thread (also in the *LinkId* property).
- *CreatedDateTime:* Date and time of the message.
- *PR_BODY:* Text of the message (also captured in HTML format in *PR_HTML*).

- *PR_SUBJECT*: The subject of the message (also contains the channel name).
- *PR_SENDER_NAME*: The display name of the sender. The GUID for the sender is found in the *FromSkypeInternalId* property.

Compliance records don't currently capture the channel name for channel conversations, which makes it more difficult to track down the original message within its host channel.

Compliance records captured for meetings hosted by other tenants contain slightly different information. To resolve the GUIDs used to record participants in the compliance records, remove the "&:orgid:" prefix from the value and run the *Get-MgUser* cmdlet. For example:

```
Get-MgUser -UserId c7745bc8-6f5c-4d45-82c7-fee55f384985  
  
DisplayName UserPrincipalName  
-----  
Ståle Hansen stale.hansen_cloudway.no#EXT#@office365itpros.onmicrosoft.com
```

What Teams Compliance Records Capture

It is important to understand that the compliance records captured by the Microsoft 365 substrate in user and group mailboxes are only copies of Teams messages. They are not the real messages (which remain stored in Azure Cosmos DB), nor are compliance records perfect replicas of those messages. Instead, the copies captured by the substrate are mail items that Microsoft Search indexes to make discoverable. If investigators find some issues in an eDiscovery case, they can access the real content in Teams to understand the full context of messages (the investigators will need access to the teams where the content exists to allow this to happen).

When the substrate captures copies of Teams messages, some transformation happens to create the compliance records. Not everything found in a Teams message ends up in the mail item. Because the copies created in Exchange Online are incomplete versions of the original data in Teams, you can't compare the copies generated by this process to email journaling. Elements copied to the mail item include:

- Links to any embedded emojis, stickers, inline images, and GIFs.
- Tables.
- Embedded deeplinks to other Teams messages.
- Sharing links to files in SharePoint Online document libraries.
- For channel messages, the compliance item records the subject of the message (if available) as is the name of the team holding the message. For personal chats, the compliance item captures the names of the people involved in the conversation.
- Code snippets in the body of messages. People can use code snippets to disguise conversations that they want to hide. Compliance records capture code snippets in Teams messages as .DAT attachments. The attachments store the HTML-formatted text for the code snippet.

Compliance records do not capture:

- **User reactions** (for example, a like, heart, or smile) to messages. In an eDiscovery context, reactions can be important signs that certain individuals have seen a conversation in the same way that changing the read status of an email from "unread" tells you that someone opened the message. Microsoft Purview Premium eDiscovery supports the inclusion of reactions in its results, but the standard eDiscovery does not. However, Teams captures "*ReactedToMessage*" audit events when people use reactions to respond to chats or channel conversations, and the [information in these events](#) can help investigators know when reactions appear in message threads.
- **Videos** for the one-minute long audio messages sent from mobile clients or chat. A lot can be communicated in one minute of video.

Compliance records created for adaptive cards are in the form of mail items with one or more attachments. The attachments hold the adaptive card content. In addition, compliance records captured for *praise* messages only have the text of the praise and don't include the graphic, and compliance messages for messages with quoted text include the text but not the formatting marking the text as a quote.

Versions of Compliance Records

If a retention policy is in place for Teams, the substrate captures changes made by a user to a message in the *Versions* sub-folder of Recoverable Items in the target mailbox. Thus, a content search might uncover several different versions of the same message, with the last version stored in the *TeamsMessagesData* folder being the content of the last update applied to the message (the earlier versions are in Recoverable Items).

Compliance Records for Hybrid and Guest Users

Not every person who interacts with Teams has an Exchange Online mailbox in which the Microsoft 365 substrate can create and store compliance records. To get around the problem, the substrate creates special cloud-only Exchange Online mailboxes to store compliance records for:

- Hybrid users with Exchange on-premises mailboxes.
- Federated connections, such as external access to chat with Teams users in other domains or Skype consumer users.
- Guest accounts.

The substrate provisions a cloud-only mailbox (otherwise known as a "phantom" or "shard" mailbox) the first time it needs to create a compliance record for an external user. Cloud-based mailboxes are in the same data center region as the host tenant. The substrate uses the same approach to store compliance records for apps like Planner. Users cannot sign into these mailboxes, nor are they used for sending or receiving emails. They exist purely for storage purposes.

For example, if a Teams user starts a federated (external access) chat with a Skype consumer user, the substrate creates a mailbox called *Skypeld@teams.microsoft.com* (where *Skypeld* is the user's Skype identifier) to store the compliance records.

On-premises users must be part of a hybrid organization that synchronizes their accounts with Entra ID using AAD Connect. The mail user accounts created for hybrid mailboxes must have both Teams licenses and Exchange Online P1 licenses. If a hybrid mailbox moves from on-premises to Exchange Online, the transfer process moves the compliance records from the phantom mailbox into the user's new cloud mailbox.

Although Teams supports retention policies, those policies do not apply to cloud-only (or "phantom") mailboxes. Likewise, you cannot apply retention holds to these mailboxes.

Teams Compliance Outside the Tenant

When people collaborate in Teams, they can work with external users from outside their tenant. In this scenario, the rule is that the home tenant has all the compliance data. In other words, if an external user posts a message to a channel in your tenant, the substrate captures the compliance record in your tenant and no trace exists of their contribution within their home tenant. The reverse is also true: a tenant administrator has no oversight into what users from their tenant do inside other tenants.

Usually, this isn't an issue unless compliance administrators need to access information about what users do in other tenants. For example, an investigation needs to know if someone discussed a confidential issue with people they should not have. A search can scan the Microsoft 365 repositories in the user's home tenant, but any communications with the relevant individual in a channel (regular or private as a guest, or in a shared channel using their home account) remains invisible to eDiscovery performed in the home tenant. To find

evidence, an arrangement must be made with the administrators of the tenant where the conversation occurred.

Administrators usually want to know when people are accessing data outside the tenant. To see signs of cross-tenant activity, you can check the sign-in logs. This code uses the Microsoft Graph PowerShell SDK to find the sign-in log entries not related to your tenant. A filter extracts the records for shared channels. The beta version of the cmdlet is required because it supports filtering against the *ResourceTenantId* property.

```
Connect-MgGraph -Scopes "AuditLog.Read.All, Directory.Read.All" -NoWelcome
$TenantId = (Get-MgOrganization).Id
Get-MgBetaAuditLogSignIn -Filter "ResourceTenantId ne '$TenantID'" -All | Where-Object
{$_._CrossTenantAccessType -eq "b2bDirectConnect" -and $_.AppDisplayName -eq "Microsoft Teams"} |
Format-List CreatedDateTime, UserDisplayName, ResourceDisplayName, AppDisplayName, ResourceTenantId

CreatedDateTime      : 20/03/2022 00:04:51
UserDisplayName     : Tony Redmond
ResourceDisplayName : Office 365 SharePoint Online
AppDisplayName      : Microsoft Teams
ResourceTenantId   : 22e90715-3da6-4a78-9ec6-b3282389492b
```

You can download a script to [find and analyze sign-in records from GitHub](#). A similar approach is possible to find records for guest access (the filter used is *CrossTenantAccessType -eq "b2bCollaboration"*). See the PowerShell book for more information about using the Microsoft Graph PowerShell SDK.

The [Get-MSIDCrossTenantAccessActivity](#) function from the [MS Identity tools PowerShell module](#) is a good way of monitoring inbound and outbound cross-tenant connections for an organization.

Call Records

Compliance records captured for meetings and calls depend on the Call Record Processing service. In telephony terms, the compliance records captured for calls and meetings are known as call detail records or CDRs. The substrate creates CDRs in the mailboxes of all call participants in the same hidden folder used to store the compliance records for messages. It can take up to eight hours before CDRs are available for searching. This usually is not a problem because eDiscovery searches normally happen after an event occurs.

CDRs do not include audio or video events in meetings. If you want this, record the meeting, and Teams will store the audio and video feeds for the meeting in an MP4 file in OneDrive for Business. CDRs capture textual details of a meeting or call such as:

- The start and end time of the meeting or call, and its overall duration.
- Notes of when each participant joined and left the meeting. Participants can join through VOIP or PSTN, and as anonymous, federated, and guest users. Teams assigns an identifier for anonymous joiners in the form *teamsvisitor:13c3a4132a584b918b9c6528b6dabef9*. It isn't possible to translate these identifiers into email addresses or other more identifiable addresses.
- Calls to voicemail.
- Missed or unanswered calls.
- Call transfers (which are represented as two separate calls).

An example of a CDR is:

```
Start Time (UTC): 6/20/2020 3:54:56 PM
End Time (UTC): 6/20/2020 5:05:28 PM
Duration: 01:10:31.9773921

[6/20/2020 4:21:17 PM (UTC)] teamsvisitor:d1cce625a5ee4a29911a7a954a89f1ee joined.
[6/20/2020 4:23:29 PM (UTC)] teamsvisitor:d1cce625a5ee4a29911a7a954a89f1ee left.
[6/20/2020 3:59:38 PM (UTC)] John.Hubbard@office365itpros.com joined.
[6/20/2020 5:05:27 PM (UTC)] John.Hubbard@office365itpros.com left.
```

Because CDRs are captured as email items, the person who starts a call or schedules a meeting is recorded as the sender, and participants are recorded as message recipients. The first part of the item's subject captures the kind of call or meeting while the remainder is a unique identifier for the event in the Teams media stack. For example:

- Meeting (ScheduledMeeting).
- Meeting (RecurringMeeting).
- Call (Completed).

Microsoft plans to capture more details for calls such as screen and app sharing in the future.

Storage of Teams Compliance Records

For both group and personal mailboxes, the substrate stores compliance records captured for Teams conversations in a special hidden folder called *TeamsMessagesData* in the non-IPM (system) part of user and group mailboxes. Because the folder holds compliance data that users should not be able to interfere with, clients like OWA and Outlook desktop do not expose the folder in their GUI. If you need to examine compliance records, you can open the folder in a personal mailbox (but not a group mailbox) to examine individual items with a program like MFCMAPI. Exchange Online doesn't charge the storage used by Teams compliance records against user mailbox quotas.

Depending on load, the delay before a compliance record appears in the mailbox varies from a few seconds to a few minutes. Once captured in a mailbox, Exchange Online automatically indexes the compliance records to make them discoverable by content searches. To see how many Teams compliance records are in a user, or group mailbox, run the *Get-ExoMailboxFolderStatistics* cmdlet to report the items held in the *TeamsMessagesData* folder:

Get-ExoMailboxFolderStatistics -Identity "Office 365 Adoption" -FolderScope NonIPMRoot -IncludeOldestAndNewestItems Where-Object {\$_.FolderType -eq "TeamsMessagesData"} Format-Table Name, ItemsInFolder, NewestItemReceivedDate, OldestItemReceivedDate			
Name	ItemsInFolder	NewestItemReceivedDate	OldestItemReceivedDate
TeamsMessagesData	4227	02/02/2022 16:10:41	11/03/2017 15:41:34

The reason why we use the *IncludeOldestAndNewestItems* switch with the command is to force Exchange Online to return information about the oldest and newest items found in the folder. This is interesting information if you want to know if retention policies are removing items as their retention period expires.

In addition to compliance records captured for chats and conversations, Teams captures copies of email messages sent to a channel in a sub-folder called "Email Messages" of the channel folder in the SharePoint document library belonging to the underlying group. The messages are individual indexed files discoverable by content searches. Any files uploaded to the SharePoint document libraries used by Teams or to users' OneDrive for Business sites come under the usual compliance controls deployed to those workloads.

Searching Teams Compliance Records

Content searches for Teams messages do not process Teams data stored in its Azure-based data services. Instead, searches depend on the Teams compliance records held in Exchange as those records are the data indexed and available for search. You do not have to do anything special to include compliance records in content searches because these items are searched whenever you include the mailboxes (group or user) or sites used by Teams in content searches. The sole exception is for users who have their mailboxes on on-premises Exchange servers (compliance records created for these users are stored in cloud mailboxes and available for eDiscovery). The content of these mailboxes is unavailable to content searches, so they cannot be included. In addition, you cannot apply a hold to content stored in on-premises mailboxes.

The screenshot shows a Microsoft Purview search interface. The search results list several messages, with one message selected. The selected message is shown in a preview pane. The preview pane displays the following details:

- From:** Tony Redmond <Tony.Redmond@...
- To:** Marc.Vigneau <Marc.Vigneau@office365itpros.com>; Ben Owens (DCPG) <Ben.Owens@office365itpros.com>; James Abrahams <James.A.Abrahams@office365itpros.com>
- Send Date (UTC):** 05/11/2023 18:06:30
- Download Original Item**

Version 101!

Office 365 for IT Pros November 2023 Update Available

The Office 365 for IT Pros eBook team is delighted to announce the release of the 101st monthly update (November 2023). Subscribers can download the updated files from [Umroad.com](https://umroad.com). The update covers many chapters and includes topics like the release of the new Teams client, which we learned on October 31 will become the only Teams client on March 31, 2024. Lots of ongoing change inside the Microsoft 365 ecosystem... Which is why a book like Office 365 for IT Pros is the only way to stay current!

<https://office365itpros.com/2023/11/01/office-365-for-it-pros-101/>

Figure 12-9: Teams compliance records in a preview sample generated by a content search

Figure 12-9 shows how Teams compliance records appear in the preview of items found by a content search. In this case, the compliance record captures details of a message posted to a group chat. We know this by examining the item properties, where we can find:

- **From:** The display name and email address of the user who posted the message.
- **To:** The display names and email addresses of the chat participants. If the message was a channel conversation, the name and email address of the team is shown. The email address belongs to the Microsoft 365 group used by the team rather than the channel holding the message.
- **Send date:** The date and time in UTC format when the sender posted the item.

As noted above, Teams compliance records for channel and personal conversations use the message item type of IM rather than the normal "Email" used for mailbox items. Note that messages created in channels by workflows also use the IM message type. Compliance records for meetings have the "Meeting" message type while personal calls use the "Call" message type.

No Team or Channel Names Displayed for Compliance Items: In the past, content searches displayed the names of the team and channel in the Subject field of items returned by searches. This information was useful in terms of finding the exact location of an item, but it's no longer displayed. The team name and email address are now the only clues as to the team where an item is found.

Refine Searches for Specific Teams Items

The parameters for the content search shown in Figure 12-9 scans Exchange Online mailboxes to find any Teams compliance record matching the keyword. However, if it asked to search mailboxes without further qualification, the search will also find other non-Teams messages. To restrict search results to Teams content, we add the IM message kind condition to the search. This will find chat and channel conversations. Other search refinements are:

- Message kind set to *MicrosoftTeams* to find chat and channel conversations and call detail records.
- Keyword: *Itemclass:IPM.AppointmentSnapshot.SkypeTeams.Meeting* to find call detail records for meetings.
- Keyword: *Itemclass:IPM.AppointmentSnapshot.SkypeTeams.Call* to find call detail records for calls.

- Keyword: *Itemclass:IPM.AppointmentSnapshot.SkypeTeams.Meeting OR Itemclass:IPM.AppointmentSnapshot.SkypeTeams.Call* to find all call detail records.

Note: when you create a content search, make sure to set the “add app content for on-premises” checkbox to allow the search to include compliance records generated by hybrid and guest users.

Searching Other Microsoft 365 Workloads for Teams Content

Remember that Teams content exists in many other places than channel conversations and chats. To do a complete search, you might need to include:

- OneDrive for Business accounts to find files shared in personal and group chats.
- SharePoint Online sites for files shared in channel conversations.

Some information used by Teams will remain unavailable to content searches until applications support indexing. Whiteboards shared during meetings are a good example of information unavailable to content searches.

Reassembling Conversations

The way that the Microsoft 365 substrate captures individual compliance records for each message posted to a chat or channel conversation makes it more difficult to reconstruct a full conversation from start to finish. Normally, when eDiscovery investigators review information, they want to see the full context to understand who said what to whom and how a conversation developed. A full message thread gives context by recording the different interactions of participants in a conversation. Email can do this too by including the text of prior replies in a message.

The Microsoft 365 Advanced eDiscovery and Communication Compliance services are both able to reconstruct a Teams conversation from discovered messages and present the conversation in the same manner as it appears in a Teams client. This isn’t possible with Core eDiscovery or simple content searches as these operations return individual compliance records instead of complete conversations. However, it is possible to use a manual process to construct a complete conversation from the compliance records captured by Teams. To do this, you must:

- Search for and find the compliance records for all contributions to the conversation. You won’t find all the compliance records belonging to a conversation unless you use its reply chain identifier as a search keyword. For example, you could search for 1529919175913 to find all items in the conversation with that reply chain identifier.
- Because items from all channels are in the same mailbox, be careful not to mix items from different channels together.
- Arrange the items in date order using the timestamp. Some commercial products combine compliance records to form threads when they present search results.

You can export the information found in Teams by a content search to PST files or as individual items, and then give the PST or items to external investigators for their review. See the eDiscovery chapter for more information about how to build and run content searches and export items found by the searches.

If a Teams meeting is recorded and a transcript is produced, Microsoft Search can look for information in the transcript. Content searches can also find videos based on transcript text, but the content search UI doesn’t display the transcript. The items found by searches are the recordings (MP4 files) rather than their transcripts. However, when you export search results, the transcript is in the exported data. If you download a video found by a search, the compliance portal creates a file without an extension. You can rename the file to give it an MP4 extension and it will then play as normal (this issue might be corrected when you read this).

Searching Hybrid and Guest for Teams Compliance Records

If a guest user sends a message to a tenant user in a chat, the substrate captures two copies of the message: one in the cloud-only mailbox created for the guest, the other in the tenant user's mailbox. Searches executed through the Microsoft 365 Compliance Center automatically include Teams messages sent by hybrid and guest users using the copies kept in user or group mailboxes but do not scan the phantom mailboxes belonging to these users.

Two ways exist to search compliance items stored in guest mailboxes. You can:

1. Amend search settings to set the checkbox to include "*Add app content for on-premises users*." The checkbox covers the cloud-based mailboxes created for hybrid, federated, and guest users. This is the default setting for new content searches.
2. Use PowerShell to update the search criteria to include phantom mailboxes.

Content searches find Teams compliance records in cloud-based mailboxes when two parameters are set to `$True`:

- **AllowNotFoundExchangeLocationsEnabled** controls if the search covers Exchange Online mailboxes that cannot be verified. These are the cloud-only mailboxes used by hybrid and guest accounts.
- **IncludeUserAppContent** controls if app content is searched. App content means the cloud-based mailboxes used by guest and hybrid users.

You can set these parameters for a new content search with the `New-ComplianceSearch` cmdlet or apply them to an existing search with the `Set-ComplianceSearch` cmdlet.

For example, these commands create a search including cloud-only mailboxes and then start the search.

```
New-ComplianceSearch -Name "Teams Chat Scan" -Description "Search for Teams Chat Information about Finance" -IncludeUserAppContent $True -AllowNotFoundExchangeLocationsEnabled $True -ExchangeLocation All -ContentMatchQuery "Finance AND Kind:MicrosoftTeams"
```

```
Start-ComplianceSearch -Identity "Teams Chat Scan"
```

After Purview runs the content search, you can use the preview search GUI in the Microsoft 365 Purview portal to review a sample of search results. If necessary, you can refine the search keywords and qualifiers to improve the accuracy of the search, and eventually export the results for further investigation.

Teams and Retention Policies

Teams messages are persistent and remain in the Azure Cosmos DB data store until removed by user action or through Microsoft Purview retention processing. Channel messages belong to the channel and don't disappear following the removal of the authors from Microsoft 365 (if Teams can't resolve the user who posted a message because their account no longer exists, it displays the message as posted by an "unknown user"). Chat participants collectively own the messages in the chat. A participant can delete their link to a chat message, but the message will remain available to the other participants.

Purview retention policies use a synchronization process to remove messages from Teams. An organization can create retention policies to process Teams chats and/or channel conversations, including the call data records (CDR) created for Teams calls. Teams retention policies can only process Teams data. Other retention policies to process items such as documents and email cannot include Teams. The reason is that the Teams retention policies operate against the compliance records stored in the `TeamsMessagesData` folder in user and group mailboxes instead of the actual Teams data stored in Cosmos DB.

A background retention assistant job processes Teams retention policies (the same assistant also processes retention policies for SharePoint Online and OneDrive for Business). The assistant applies the settings in Teams retention policies to know when compliance records expire. At this point, the assistant removes the compliance records from the mailboxes and the Microsoft 365 substrate synchronizes the deletions back to the Teams chat service, which then removes the relevant messages from its store. Later, Teams clients connect to the Teams service and synchronize their local cache to complete the removal cycle.

If an in-place hold or litigation hold applies to some group or personal mailboxes which include compliance records, those items come under the scope of the hold. The substrate captures any attempt to remove or edit a compliance record by keeping the copies of the removed or edited item in the `\Purges` or `\DiscoveryHolds` sub-folders under Recoverable Items in the mailbox. However, Teams removes the items from its message store in Azure Cosmos DB.

When you create a retention policy for Teams, you can choose to keep messages for a selected retention period (a minimum of one day) or to remove items after the retention period elapses. What you cannot do is give users the ability to mark specific messages to force retention policies to remove those items sooner or keep them longer. SharePoint and Exchange support this kind of flexibility through retention labels or mailbox personal tags.

Auditing Teams

In addition to capturing compliance records for individual and channel conversations, Teams generates audit records for many user and administrative operations. The most common audit record is to record each time a user, including guests, signs in. Teams captures an audit record for a user sign-in for every hour in a session. This is because the access token expires after an hour. After Entra ID renews the access token, the user signs in again. The user does not notice the sign-in happening as token renewal and reconnection happens in the background. The audit record tells you when the user signed into Teams and some information about what client they used, but it does not capture details of which team or channel they accessed.

Among the administrative activities that Teams captures audit records for are:

- Team creation and deletion.
- Channel creation and deletion.
- Users added or removed from teams.
- Settings changed for the organization, team, or channel.
- Tab addition and deletion (for a channel).
- Connector addition, deletion, and updates.

For example, audit events are captured for the creation and removal of teams and the creation of channels within teams. For instance, when you use a Teams client to create a new team, the audit log receives an *"add group"* event when Entra ID creates the new group followed by some *"update group"* events when it populates the properties of the new group. Finally, you see a *"TeamCreated"* event for the new team. Audit events are also recorded for any alteration of team settings. However, a *"TeamCreated"* audit event is not captured when you enable an existing group for Teams.

The audit records for the creation of teams and channels capture the names given to the new teams and channels and who created the object. However, the records for tab creation only tell you that someone created a tab. No information is captured about the content the tab links to. For example, if you create a tab to link to a YouTube video, the audit record tells you that the tab type is *"extension"* but not that it links to a video or what the video is (apart from third-party apps like YouTube, the extension tab type covers Microsoft applications like Planner and Stream too). No information is recorded about the content either when someone updates a tab. The lack of data is sometimes explained by the need to protect user privacy, and sometimes

because tenants and Microsoft need to define what information Teams should capture (and why) for audit purposes.

Teams periodically uploads its audit data to the audit log. You can interrogate audit records using the audit log search in the Microsoft Purview compliance portal, by running the *Search-UnifiedAuditLog* cmdlet, or with third-party security products. Techniques for using these tools are explained in the Report and Auditing chapter.

Teams and the Groups Expiration Policy

Removing teams when they are no longer in active use is part of compliance planning. If your tenant uses the Entra ID group expiration policy and a team-enabled group comes within the scope of the expiration policy, an extra section called **Team Expiration** is visible to team owners under the Settings tab in the Manage team option. Here owners can discover when the team expires.

When a team is within a month of its expiry date, Teams highlights its potential expiration with a notification posted to the activity feed of the team owners. In addition, a warning triangle appears beside the team name in the navigation pane (but only to team owners). Hovering over the warning triangle reveals the expiry date and the choice to **Renew team** appears in the ellipsis menu. Because the Groups expiration policy auto-renews groups if they are active (and posting topics and replies in team channels is suitable evidence of activity), you shouldn't see warnings unless the assessment against the policy settings considers the team to be inactive. This can happen for teams used to host workflows where the number of human-originated posts is low. If you see a warning, go to the Manage team options for the team and renew it there.

If a team reaches its expiry date and is not renewed by an owner or administrator, Entra ID soft-deletes the group and all associated resources, including the team, and removes the ability of users to access those resources. An administrator can restore the team at any time within 30 days of its being soft-deleted. Once the 30-day period elapses, Entra ID permanently removes the group and all its associated resources, and the group becomes irrecoverable. Teams administrators can renew teams and restore deleted teams using the options in the Manage Teams section of the Teams admin center. Alternatively, deleted teams (groups) are recoverable using the Entra admin center or [PowerShell](#).

Archiving Teams

Entra ID removes expired teams from the tenant. Archiving a team is another way of dealing with teams that are no longer active. When you archive a team, you make the elements controlled by Teams (like channel conversations and the wiki) read-only. Users can access messages in an archived team, but they cannot post new messages, edit messages, or remove messages from a channel. In addition, members can access files in the document library belonging to the team, but they cannot upload new documents or remove files from the library, and the link to open the document library in the SharePoint browser interface is not available. When users open an archived team, they see notices to tell them that they can no longer post to the team. Teams also displays an icon (a closed drawer) alongside the names of archived teams in the team list. The idea is that the team remains available to its membership to allow users to continue accessing information while not being able to add to that information. You can update the membership of an archived team to add or remove members, including guests, or promote members to be owners.

Three methods are available to archive a team:

- In the desktop or browser client, select Teams, then the **Your teams and channels** option from the [...] menu. The list of teams is divided into active teams and archived teams. This option is available to all team members, including guest accounts. However, only team owners, tenant administrators, and Teams service administrators see the option to **Archive team** in the ellipsis menu for the team (Figure

- 12-10). To restore an archived team and make it read-write again, select it in the list of archived teams and then choose **Restore team** from the ellipsis menu.
- In the Teams admin center, find the team in the **Manage teams** section and then select the **Archive** option. Only those assigned a Teams administration role can archive a team using this method.
 - Use the Teams PowerShell module to archive a team. For example, to see the set of archived teams:

```
Get-Team -Archived $True
```

To archive a team, run the *Set-TeamArchivedState* cmdlet and pass the identifier to the team to archive. The *SetSpoSiteReadOnlyForMembers* setting controls if the SharePoint site belonging to the team is set to read-only.

```
Set-TeamArchivedState -GroupId $GroupId -Archived $True -SetSpoSiteReadOnlyForMembers $True
```

To reverse the process, set the Archived switch to False. You can only update the *SetSpoSiteReadOnlyForMembers* setting if it was set when archiving the team:

```
Set-TeamArchivedState -GroupId $GroupId -Archived $False -SetSpoSiteReadOnlyForMembers $False
```

Before archiving a team, it's important to check the status of any private or shared channels in the team. Administrators or team owners don't have access to the content of these channels unless they are channel members. A private or shared channel can be very active without the knowledge of the team owner, and if the team is archived at this point, team members (including external and guest members) won't be able to post new content. The Teams desktop client doesn't display any details about private and shared channels in a team. This information is available in the Teams admin center and can be retrieved by querying the team channel configuration with PowerShell using the *Get-TeamChannel* cmdlet.

After archiving a team, Teams moves it into the set of hidden teams displayed at the bottom of the teams list. Removing a team from the active set effectively makes the archived team invisible to users unless they go looking for it by opening the hidden set or by using the Manage teams option to find the team in the archived section. If you restore an archived team, Teams makes it writeable again but leaves the restored team in the set of hidden teams.

When archiving a team, you can choose to make its SharePoint site read-only for team members (this also sets the wiki to be read-only). Team owners can continue to upload and update content, but team members who access the site after the team is archived have restricted options because Teams adjusts the site permissions for team members to remove their write access. For example, members cannot upload files to the library, rename or remove files, update document details, assign retention or sensitivity labels, and so on. They can still synchronize the library and download files. The sites belonging to private and shared channels also become read-only (even for channel owners), and in these instances, SharePoint displays a banner to inform channel members of the site's read-only state.

Setting read-only access to the conversations and files belonging to a team is an effective way of putting it into an archive status, but a big selling point for Teams is its ability to be an integration point for other third-party applications. To make archive status fully effective, every application connected to Teams must understand when a team is archived. SharePoint does this, but the other connected apps don't, which means that team members can continue to have read-write access to other apps like Planner, OneNote, and apps added to the team as tabs, and bots. This makes sense for third-party apps as they might be shared across multiple teams.

Archiving a team does not stop it from expiring if it is within the scope of the group expiration policy. The team still exists, albeit in a read-only state; expiration kicks in once the renewal time of the underlying group is reached and if the group is not renewed, Entra ID soft-deletes the archived team.

The screenshot shows the 'Your teams' section of the Microsoft Teams admin center. A context menu is open over a team named 'Information Quality an...'. The menu items are: Manage team, Add member, Add channel, Get link to team, Leave team, **Archive team** (with a red arrow pointing to it), Manage tags, and Delete team.

Name	Description	Membership	People	Type
Project Hidden Secret	A project full of hidden secrets	Owner	8	
Technology News and ...	All about new technology	Member	10	
Test Team with 1000 c...	Team with 1,000 channels	Member	4	
Sales Team	Members of the Sales Department	Owner	6	
Industry News	All the news about the IT industry	Owner	9	
Ultimate Guide to Offi...	The Ultimate and Best Guide to Office 3...	Owner	1	
Information Quality an...	Ultra Fans	Owner	1	
Practical365 Writers	People who write for Practical 365	Owner	6	
Holiday Plans	All about holidays	Owner	2	

Figure 12-10: The option to archive a team

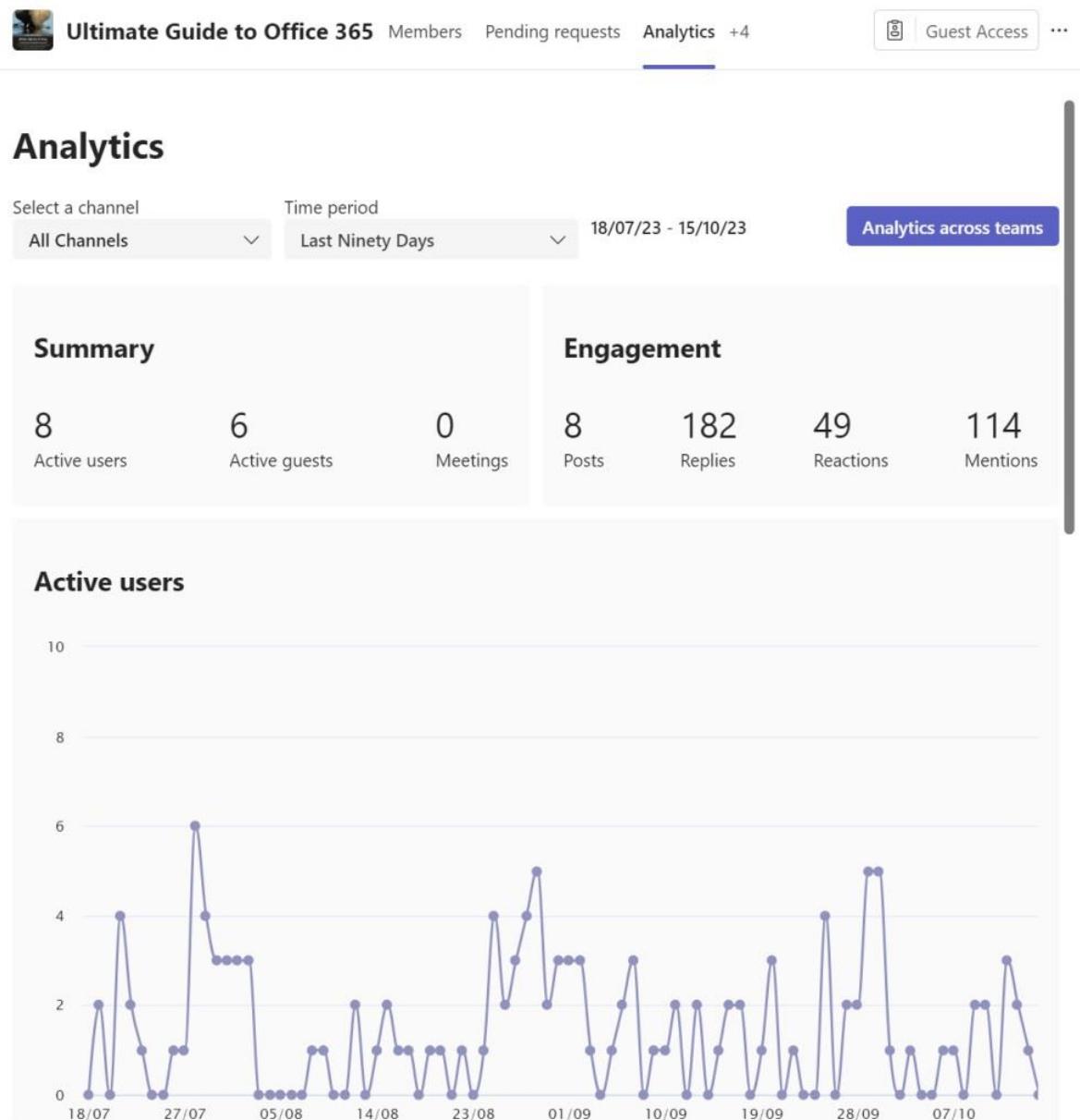
The mechanism used to archive teams is reasonable. Its biggest advantage is that members continue to enjoy access to channel conversations. A different approach is outlined in the PowerShell book showing how to archive teams by removing everyone but a single owner from group membership. The advantage of this approach is that access to all team resources is removed from previous members, which is what you might want to achieve.

Reporting Teams Usage

Microsoft 365 includes several methods to gain an insight into the activity levels of Teams:

- The standard usage reports available in the Microsoft 365 admin center include a Teams usage report. The data can be viewed in 7-day, 30-day, 90-day, or 180-day snapshots. [A Graph usage API generates the Teams usage data](#) and can be incorporated into apps. Data is available for the overall tenant, per-team, and per-user level (in a sortable table) and is exportable to a CSV file.
- The **Analytics and Reports** section of the Teams admin center includes a set of usage reports. The Teams admin center doesn't support sorting of the report detail, but you can export the information to a CSV file to analyze and report the data as you wish. Reports are available for the last 7, 30, 90, or 180 days, except the PSTN data, which is available for up to 28 days. The same data is available for device usage and user activity in the Microsoft 365 admin center. The range of reports has grown over time and includes:
 - Teams user activity (number of channel messages, chat messages, 1:1 calls, video and audio minutes, date of last activity, and meeting statistics).
 - Teams device usage (Windows, Mac, iOS, Android, and browsers).

- Teams usage (active users, guest members, active channels, number of messages, team privacy setting).
- Teams Live Event usage (event, start time, organizer, presenter, producer, and views).
- PSTN blocked users.
- PSTN minutes.
- PSTN usage.
- Audio conferencing dial-out usage.
- Advanced virtual appointment activity.
- Information protection license report. This has nothing to do with Microsoft 365 Information Protection and instead deals with if users have the [necessary license for apps to receive subscriptions](#) to the endpoints tracking changes to messages and chats.
- Teams premium feature usage.
- Apps usage (number of active users per app, number of teams where the apps are used).



- Figure 12-11: Analytics for an individual team (all channels) Analytics for individual teams are available through the Manage team option in the Teams desktop and browser clients (Figure 12-11). The data reveals activity for the selected team over a 7, 30, or 90-day period. The information is available to any

member of a team, including guests, and is intended to give an overall view of the activity within a team together with some other information such as the breakdown of membership into active and inactive members and tenant users and guests. You can view data for all channels or select the data for an individual channel (including private channels). The data available for a channel covers the number of topics and replies posted. Team analytics track active users over time, the split between tenant users and guests and members and owners, the number of apps installed in the team, and meeting activity. The data doesn't include messages posted to channels by workflows (like an RSS feed) or those that come in through email. Analytics for an individual channel is also available through the Manage channel menu. Teams doesn't include a facility to export analytics data from a client. The report also lists the top five inactive channels in the team. Typically, the channels listed have had no activity in over a month, but this depends on the number of channels in the team.

- The [Microsoft 365 usage analytics content pack](#) for Power BI includes a Teams usage report. Like the usage data for all workloads available in the content pack, the Teams data can be up to a month or so behind, depending on when Microsoft 365 last refreshed the data. The content pack exists to track usage over a sustained period and that is how to use it.

Many aspects of user interaction with Teams is collected and collated by background processes and stored in the Microsoft Graph, where it is accessible [through a usage API](#). The information available through these options is at least two days old. The analytics and reports available in the Teams client and the admin centers present data in different ways, so you might observe some minor inconsistencies when comparing the data viewed in one interface against another. Remember that third-party reporting alternatives usually offer more powerful and flexible analysis and reporting functionality than is available in Microsoft 365.

Advanced Collaboration Analytics

Advanced collaboration analytics are available for users with Teams Premium licenses to allow administrators to understand more about how users collaborate with external domains. The analytics are presented in the collaboration activity tab on the Teams dashboard and through reports such as the external domain activity report.

Analytics can be displayed for different periods (7, 30, or 60 days) and include:

- Inactive teams report lists teams where no collaboration activities have been detected.
- Inactive external domains activity reveals domains in the external access allow list where federated communications has not happened.
- Teams with the most external user and guest activity.
- Users with the most external user and guest collaboration.
- Guests with the most external user and guest collaboration.

In addition, the collaboration dashboard includes cards for teams by user type (teams with only internal users, teams with guests, etc.) and channel by user type. Like other reports generated from Microsoft 365 usage data, cards respect the tenant usage data privacy control and will not display information if the privacy control is set.

Extending Teams

Out-of-the-box, you can extend Teams by adding tabs, apps, bots, and workflows to channels. Bots fit into conversations to allow users to interact via chat with software assistants, usually to answer questions about specific topics. Workflows set up links between channels and network data sources so that information flows from the data source and appears in the channel like user contributions.

Microsoft has a [developer program for Teams](#) focusing on different aspects of integration like creating new integrated apps for Teams. MVP Tom Morgan publishes [Building and Development Apps and Bots for](#)

[Microsoft Teams](#). It's a good starting point for app developers who want to build apps using the Teams platform. Given the attractiveness of the platform and the hundreds of millions of active Teams users, it is no surprise that the number of Teams apps increases over time. As of mid-June 2024, nearly 2,500 apps are available in the Teams app store, and the number of apps increases by approximately 80 per month.

The [Microsoft 365 app certification program](#) helps customers to understand what apps they might like to run in Teams by publishing developer-provided information about the apps. Three levels are available:

- **Publisher verification:** The app developer has a Microsoft developer network identity. The app supports modern authentication and is capable of multi-tenant activity. This is the entry-level participation in certification.
- **Publisher attestation:** The app developer completes a questionnaire covering security, data handling, and compliance.
- **Microsoft 365 certification:** Instead of the app developer reporting details of their app, third-party assessors audit the assertions to validate that the app meets Microsoft standards for security and compliance. The process occurs annually, and details gathered during the audit are available online. The audit information is available through the Microsoft 365 certification link for the app. Adobe Sign is an example of a Microsoft 365 certified app.

Regrettably, many apps (including some created by Microsoft) are uncertified and few app developers go through the full Microsoft 365 certification process. This might be a question of resources or a lack of perceived value in achieving certification. However, the audit information gathered by the attestation procedure is valuable and worthwhile knowledge for customers interested in the data accessed by apps.

Managing Teams Apps

Not every organization is willing to allow users free rein over the apps they can install and use with Teams. To exert control over the apps available to users, three mechanisms are available in the **Teams Apps** section of the Teams admin center:

- **Manage apps:** Define which apps are available in the tenant. By default, any app published in the Teams app store is available to a tenant. Some apps might be inappropriate or not very useful for an organization, so tenant administrators can block individual apps here. Blocked apps can't be installed by users and won't be displayed in the app navigation bar if included in an app setup policy. To decide whether to allow an app, you can check its properties:
 - *Publisher:* The organization responsible for creating and maintaining the app.
 - *Version:* The current version of the software.
 - *Categories:* For example, Productivity or Business Management. The publisher chooses these categories as general guidance for the type of solution an app is.
 - *Certification:* The highest level of certification is [Microsoft 365 certified app](#), which means that Microsoft has reviewed and approved the app against a set of security, compliance, and data handling standards.
 - *Licenses:* ISVs can generate Teams apps that support per-user licensing (monthly or annually) or in-app purchases. The Plans and Pricing tab for the app tells administrators what licensing is available. Some apps offer free versions that users can upgrade to a premium version with a license.
 - *Capabilities:* Where in Teams the app can be used. If *Team*, the app can be installed into a team channel. Other categories include *Personal*, meaning that a user can install the app for their personal use, and *Group chats*, meaning that the app can be installed to be shared by participants in a group chat.
 - *App Id:* Each app gets a unique identifier (GUID) during the publication process to make the app available in the Teams app store. The identifier is the same for all tenants.

To block an app, select it from the app inventory and move the App status slider from *On* to *Off*.

If an app is scoped for installation into a team (normally as a channel tab), the administrator can install it into selected teams.

- **App Setup policies:** Controls the set of apps displayed in the Teams app navigation bar. Setup policies also control if users can pin apps or upload custom apps. See the section below.
- **App Permission policies:** Apps come from multiple sources and not every app is suitable for every user. App permission policies allow tenants to control the set of allowed apps that individual users can install in Teams.

The Manage apps page also includes **org-wide app settings** for apps. These settings are tenant settings to:

- **Third-party apps:** If *On*, third-party apps can be installed by users. Turning this setting to *Off* prevents users from installing third-party apps and limits them to apps provided by Microsoft.
- **New third-party apps published to the store:** If *On*, any new third-party apps published to the Teams app store are visible in the tenant's Teams app store and are available to users if the app permission policy assigned to their account allows third-party apps. If *Off*, new third-party apps do not appear in the app store.
- **Auto-install approved apps.** If set, Teams automatically installs apps for users when they sign-in on a different platform (for instance, on macOS after using Windows).
- **Interaction with custom apps:** Custom apps are those developed for your organization. If this control is *On*, users can install and access custom apps. If *Off*, they cannot (this setting also disables [outgoing webhooks](#)). This setting is *Off* by default for GCC tenants.
- **Show tailored apps.** This setting controls the automatic pinning of apps for frontline workers (those with Office 365 or Microsoft 365 F licenses). If set, Teams pins selected apps when a user signs in.
- **Redirect requests to external link.** If a user discovers that an app they want is unavailable because it's blocked by policy, they can request administrators to amend the app settings so that it is available. Tenants can use this option to redirect user requests to a link to a site to log the requests.

Microsoft creates default app setup and app permission policies (both called Global (Org-wide default)). These policies are assigned automatically to Teams users and stay in place unless an administrator updates the policy assignment for an account. You can amend the default policies or create new policies to assign to individual users or sets of users to match organizational requirements.

Customizable Apps

Depending on the manifest settings published by an app's developers, the settings of an app can be customized for an organization. For instance, you can replace the app's icons with versions that include corporate branding. When an app is customizable, it is marked as such in the Teams admin center and an administrator can update the following settings:

- **Short name:** a 30-character app name.
- **Short description:** an 80-character description of what the app does. You can also add a full description. I've used descriptions of over a thousand words.
- **Full description.** A longer-form description covering the use and intention of the app.
- **Privacy policy URL:** You can use this link to point to an appropriate page on the organization's website where users can find information about the company's privacy policy.
- **Website URL:** This is usually the URL for the main landing page of your company's website.
- **Terms of use URL:** Typically points to a web page where users find information about the terms of use for the application. Normally provided by the app developer.

- **Color and outline icons:** The color image must be smaller than 1,000 KB and must be a PNG file and should be 192 x 192 pixels. The outline icon is 32 x 32 pixels. The color app shows up in the Teams app store. Teams uses the outline app to display in the app navigation bar.
- **Accent color:** A hex code defining the background upon which Teams displays the app's color icon. Here's a [website](#) to help find the code for the background color.

Some experimentation might be needed to identify the best icons and colors.

Applications and Permissions

Administrators (or users, if an app requires access to that user's information) must grant consent to applications based on the Graph API to use the required permissions before they can access data such as teams, channels, and messages. Although some apps do not need to access tenant data, many third-party and LOB apps interact with data from Teams or other workloads which they access using the Microsoft Graph APIs. Before they can access any tenant data, a tenant administrator must grant an app the consent for the permissions the app uses to access the data. Consent is managed through the Permissions tab of app properties, divided into two sections:

- **Org-wide permissions:** Allow access to org-wide data, such as all sites, users, or teams in the tenant.
- **Teams Resource-specific-consent (RSC) permissions:** These are permissions granted to access [certain types of Teams data](#) (like channel settings or the tabs available in a team) scoped only to the team in which an app is installed. The user consent necessary to allow access for the Microsoft video filters and Snapchat Lenses app to video feeds in meetings is an example of RSC. Another is where it is used to allow a bot to receive chat and channel conversations without being @mentioned. Some [Entra ID configuration](#) is necessary to allow users to grant consent to applications and allow RSC to work. Trello, Zoho CRM, and Template Chooser are examples of apps that support RSC. Not all Graph-based applications support resource-specific consent permissions. The ability to use resource-specific consent permissions is enabled by default at the tenant level. As [explained here](#), administrators can configure RSC for a tenant using PowerShell, including the [Chat-specific RSC](#) to limit app access to only the resources available to a specific chat or channel conversation.

When an administrator grants consent to the permissions requested by an app, they do so on behalf of the tenant. This has the advantage that individual team owners won't be asked to grant consent when they install an app into their team. Often, team owners don't have the necessary administrative rights to grant the necessary permission, which causes a delay in making the app available to users. It's also the case that team owners might be unaware of the danger of granting consent, especially org-wide permissions, to an app published by a company they don't know.

Figure 12-12 shows the set of permissions requested by an app. This app wants consent for a set of permissions more extensive than the norm. To consent, click **Grant admin consent** when signed in with an administrator account. Teams then updates the app's service principal in Entra ID. App consent can be withdrawn at any time by editing the app details through the [Enterprise applications blade](#) in the Entra admin center.

Upon receiving consent, each time the app is used, it authenticates with Entra ID and receives an access token including the permissions granted to the app to allow the app to access data. See [this article](#) for more information about app permissions.

The screenshot shows the 'Grant admin consent' page for a Teams app. At the top, there's a warning message: 'Review and grant admin consent for the permissions required to use this app.' and a 'Grant admin consent' button. Below this, the 'Application permissions' section lists two items: 'RoleManagement.ReadWrite.Directory' (Read and write all directory RBAC settings) and 'Directory.Read.All' (Read directory data). The 'Delegated permissions' section also lists two items: 'RoleManagement.Read.Directory' (Read directory RBAC settings) and 'Directory.ReadWrite.All' (Read and write directory data). At the bottom, a section titled 'What this app can do in Teams' states: 'This app will receive consent for the following permissions upon installation so it can accomplish tasks in Teams. Learn more about app capabilities'. It then lists two permissions: 'Receive messages and data that I provide to it.' and 'Access my profile information such as my name, email address, company name, and preferred language.'

Figure 12-12: Listing the Graph permissions requested for consent by a Teams app

App Templates

To illustrate the capabilities of the platform, Microsoft has created a set of production-ready apps for Teams. This is both a learning tool and a way to accelerate app development for Teams. The idea is that organizations can browse [the available set](#) to find an app that's similar in concept (or an exact match) for what they want to do and then download the code base and deployment scripts for the chosen app from GitHub before tailoring the code to meet their requirements. The GitHub repository for each app template also includes documentation. Among the available templates are:

- Ask Away: A bot to conduct question and answer sessions within Teams.
- Building Access: Administration of access to buildings.
- Company Communicator: Create and send messages to multiple teams or large numbers of users over chat.
- Employee Ideas: Allow employees to submit ideas.
- Expert Finder: A bot to find someone in the organization based on their skill set (depends on the user account properties registered in Entra ID).

Teams App Setup Policies

The Teams app navigation bar contains a set of pinned apps and an ellipsis [...] menu to allow quick access to other apps. The app setup policy assigned to a user account controls the apps the user sees in the navigation bar. Management of [app setup policies](#) is through the **Teams Apps** section of the Teams admin center. An app setup policy describes the set of apps to show in the app navigation rail (left-hand side in desktop and

browser clients, bottom of the mobile client) and the order in which the apps appear. An app setup policy also controls if the users assigned the policy can pin apps or upload custom apps.

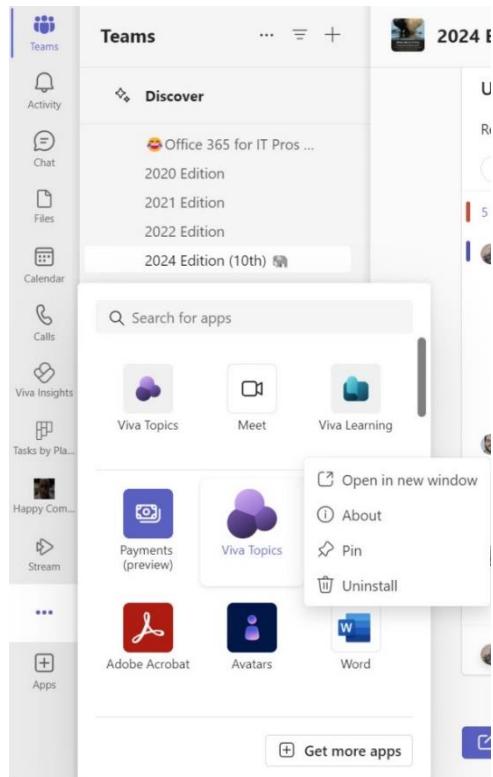


Figure 12-13: Selecting an app to pin to the app bar in the left rail of the Teams client

A typical app setup policy includes all or some of the default Teams apps (like Chat and Teams) together with other apps from the Teams app store or the organization's app catalog. The idea is that you can build sets of apps appropriate for different kinds of users and assign them via policy. The default Teams app setup policy (called Global) is used unless another policy is assigned. Teams also installs an out-of-the-box policy for front-line workers in each tenant.

In Figure 12-13, we see that the set of core Teams apps are rearranged so that Teams is at the top of the list in the app bar. Several non-core apps like Stream are pinned to the bottom of the list. The user can select additional apps to pin to the app navigation rail from the Apps menu. If the user unpins a core app like Calls, they can search for the app and repin it.

The *Allow user pinning* setting in an app setup policy controls if users can add (pin) or remove (unpin) apps to the app bar. By default, the setting is On. Update the policy setting to Off if you don't want users to be able to select apps for the app bar. Clients won't implement the new settings until they refresh their copies of policies, which can take an hour or so. Guest users don't have app setup policies and are limited to the apps they can access (Teams, Chat, Activity, and Files).

If an administrator changes the app setup policy assigned to an account, Teams notifies the user that their settings have been updated and that some of their pinned apps might have been moved.

Analyzing App Usage

The Apps usage report in the Reports section of the Teams admin center helps administrators to understand the effectiveness of Teams app setup policies. For instance, if you see that an app displayed in the navigation pane isn't being used, it's a prompt to either make people aware of the app or to consider replacing the app in the pane. Likewise, if you see an app in heavy use that isn't shown in the navigation pane, perhaps it's time to include it there. The most effective way of analyzing app usage is to download the data to Excel and review

it there. The apps with the heaviest usage are likely to be Teams (channels and conversations), Activity (the feed), Files (SharePoint Online), and other standard Microsoft apps found in all Teams installations.

Assigning App Setup Policies

App setup policies can be assigned individually to accounts in the Teams admin center or via PowerShell. It's usually more convenient to use PowerShell to assign a new policy to multiple accounts. In this example, the set of users for the marketing department is selected and an app policy designed for that department is assigned to each account.

```
$Users = (Get-CSOnlineUser -Filter {Department -eq 'Marketing'})  
ForEach ($U in $Users) {  
    Write-Host "Assigning Teams App Setup Policy for the Marketing department to" $U.DisplayName  
    Grant-CsTeamsAppSetupPolicy -PolicyName "Marketing" -Identity $U.UserPrincipalName  
}
```

Managing Access to Apps

App permission policies are the original method to control the set of apps available to users. An app permission policy grants access to a set of apps to the users to whom the policy is assigned. A user doesn't have to use the apps specified in the policy, but it does mean that the user can install the app without administrator intervention. An app permission policy can't override a blocked app defined in the org-wide app settings. Management of app permission policies is through the Teams apps section of the Teams admin center.

If you want to allow access to different sets of apps, you can customize the apps defined in the global app permission policy or create a new app permission policy and assign it to selected accounts. An app permission policy covers three types of apps:

- Microsoft apps.
- Third-party apps. Some of these apps support the purchase of applicable licenses through the Teams admin center.
- Custom or tenant apps (apps published and owned by the organization).

For each category, you can decide to:

- **Allow all apps.** Users can install and use any app of the type published in the Teams app store.
- **Allow specific apps and block all others:** The administrator selects the apps that users can install and use. Teams doesn't allow users to install blocked apps in the Teams app store.
- **Block specific apps and allow all others:** The administrator blocks selected apps available in the Teams app store and makes them unavailable to users.
- **Block all apps:** Users cannot install apps of this type.

When you restrict the set of apps with an app permission policy, Teams filters the set of apps clients display to users who are assigned that policy. Due to caching, it can take up to a day before Teams clients respond to a change in the set of apps allowed to users or a change in the policy assigned to an account.

Assigning App Permission Policies with PowerShell

The *Get-CsTeamsAppPermissionPolicy* cmdlet lists the Teams app permission policies available in the tenant. Use the *Grant-CsTeamsAppPermissionPolicy* to assign a policy to a user. For example:

```
Grant-CsTeamsAppPermissionPolicy -PolicyName "Unrestricted App Access" -Identity  
Kim.Akers@office365itpros.com
```

To assign an app permission policy to the members of a team, we need to retrieve the members of the team and then assign the policy. Here's how to do it using the *Get-Team* and *Get-TeamUser* cmdlets from the Teams PowerShell module followed by a call to *Grant-CsTeamsAppPermissionPolicy* to assign the policy to the individual members:

```
$HRGroup = Get-Team -DisplayName "Human Resources Group"
$TeamUsers = Get-TeamUser -GroupId $HRGroup.GroupId -Role Member
$TeamUsers | ForEach-Object { Grant-CsTeamsAppPermissionPolicy -PolicyName "HR App Policy" -Identity $_.User }
```

Application Centric Management

Microsoft introduced Application Centric Management (ACM) in mid-2024 as a replacement for app permission policies. Tenants can move from app permission policies to ACM using a wizard in the Teams admin center. Switching to ACM is a one-time, non-reversible migration.

Under ACM, each app has an access definition holding a list of users and groups and the permission granted to use an app. The permission can be:

- **Everyone:** The app is available to anyone in the organization, including guests.
- **Specific users or groups:** The app is available only to selected users (including guests) and groups. The groups can be Microsoft 365 groups, security groups, dynamic groups, and distribution lists.
- **No one:** The app is blocked to everyone in the organization.

To modify the permission for an app, go to the app's Users and Groups tab and edit the availability of the app there.

User Requests for Apps

Users can request administrators to allow them to install blocked apps. Administrators don't receive notifications of these requests. Instead, administrators must check the apps listing in the Teams admin center for apps with open requests.

After receiving a request, the administrator can unblock the application and add it to the relevant app permission policy (or use app-centric management) to allow the user to install the app. Users receive a notification that the app is approved for use and can go ahead to install the app.

If a user installs an app in a chat, the app becomes available for use in any other chat without the need to reinstall the app from scratch.

Teams App Store

The Teams app store is the place where users go to discover the set of apps available to them. Apps blocked by the tenant (in Manage apps) are not shown. Users reach the app store by opening the app selection panel from the app (left-hand) rail and then selecting the [...] option. The More apps link leads to the app store where the user can browse the set of available apps, which might be limited by their geographic region (a decision made by the app developer). Depending on the app type, it might be installable in various places. The target varies with app type. For instance, a connector usually installs into a channel while other apps might show up in a channel tab. See [this link](#) for more information.

Organizations can [customize the Teams app store](#) by adding their logo and corporate colors.

Teams and Bots

Another way of extending the usefulness of a team is to connect it to one or more bots. A bot is a virtual software assistant. In the context of Teams, a bot is an application that accepts questions about specific topics

from team members and responds, all within a conversation like those conducted with humans. The Microsoft [Bot Framework](#) assists developers to build their bots for use with Teams. A sample [Teams application written in C#](#) is available too. After creating a bot, to enable it for a team, go to the Teams Apps Store and click **Bots**. You can then browse the set of available bots and decide which bot to install into a channel within a team.

If you do not want users to interact with bots, you can disable access to bots on a user-specific basis by configuring and assigning an app permission policy.

Office Connectors and Teams

Office connectors create a link between an external data source and an Office application. In Teams, the destination is a channel within a team. Connectors work by fetching data from a network source and posting the information as cards in new conversations within the target channel. The cards do not hold the full content of an item fetched from a source like an RSS feed. Instead, they hold enough text to let users decide whether they want to discuss the content – or click an embedded link to explore the full content. Only users with an Exchange Online license can create a connector for a channel.

In July 2024, Microsoft announced the retirement of Office Connectors in Teams. The retirement process begins on August 15, 2024, when no one can create new connectors. Existing connectors will stop working on October 1, 2024. Microsoft's suggestion is to replace connectors with Power Automate workflows. A wide range of workflow templates are available for common scenarios, like bringing an RSS feed into a channel. The programmatic manipulation of the adaptive cards used to post items to a channel via a webhook workflow is similar but different to the way that the same operation proceeds with a connector. See [this article](#) for an example of posting Microsoft 365 service health information to Teams using PowerShell to create and post the adaptive cards.

Teams Approvals

The Teams Approvals app delivers easy-to-use and simple workflow processing. The app has links to Power Automate, but Teams hides the details of the Power Automate connection from users. Users can:

- Use the basic approval form to seek approval from reviewers for a variety of requests from time off to trips.
- Use a variation of the [basic form connected to an eSignature package](#) like Adobe Sign or DocuSign to seek approval for a document. In this case, Teams gathers information about the document for approval and the reviewers and passes the details to the eSignature provider for processing. As the document goes through the approval process, the eSignature provider sends status information back to Teams for the user to track.
- Use approval templates created by the organization. An approval template deals with a specific form of approval, such as a form to request authority to discount a customer order. Administrators create custom approval templates from scratch or use sample templates as a base. Approval templates have a scope defining who can use them. The scope can be org-wide, confined to a named set of people, or a team (in which case, any team member can create approval requests using the template). Figure 12-14 shows the creation of a Teams approval request based on a custom template.

An approver can view and approve requests generated by the Teams Approvals app in the Power Automate admin center.

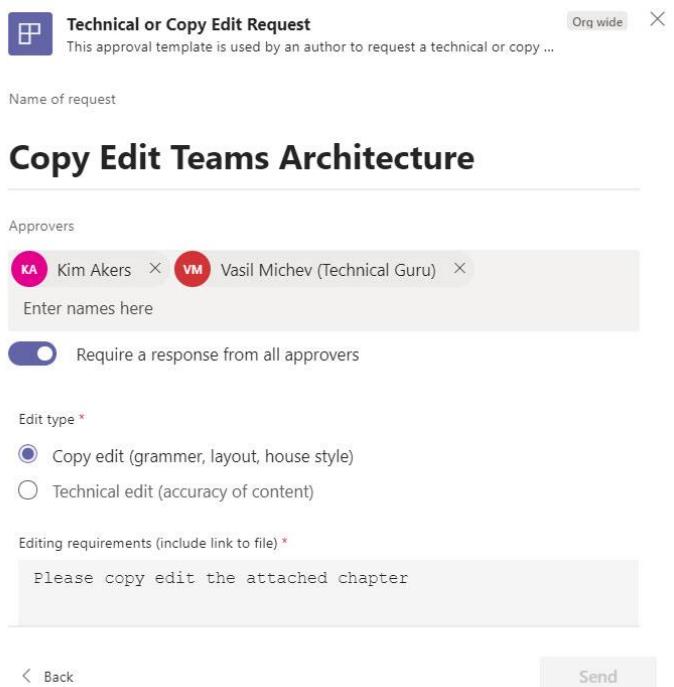


Figure 12-14: Creating a Teams approval request using a custom template

Debugging Teams Clients

If something goes wrong and you experience a problem with the Teams desktop client, the approach to restart the client usually follows these steps:

1. For desktop and mobile clients, sign out of Teams and then sign in again. This removes any lurking problems with authentication and credentials and solves many connectivity and cache synchronization issues. For browser clients, use a private session to connect to Teams. If this works, clear any browser cookies associated with Teams and office.com and try with a normal session again.
2. If the desktop client is still failing, stop all the Teams processes. On Windows, use Task Manager to find the processes and end them. Restart the client to see if the problem disappears.
3. If that doesn't work and the desktop client continues to have problems, clear the Teams cache. On Windows workstations, to speed up performance, Teams caches copies of server data in the `%UserProfile%\%appdata%\Microsoft\Teams` folder. Occasionally, the cached data is out of sync with the server or holds some corrupted data. Both conditions cause problems for the client. Before removing the cache, stop the Teams client (all processes). Then remove the complete Teams folder. When you restart Teams, the client rebuilds the cache so that its content is fresh. Although it's not recommended to blow away the Teams cache as the first step in troubleshooting, it can solve problems where other steps fail.
4. If you cannot resolve the problem, you should file a service request and give the diagnostics and client logs (see below) to Microsoft to help them understand where the root cause might lie.

If you find that you can't switch to another tenant, you may have expired credentials. To solve the problem, sign out of Teams and sign back in again. After you sign in, if you then try to switch to another tenant, Teams will prompt for credentials to allow the client to connect to that tenant.

Teams Client and Diagnostic Logs

As summarized in Table 12-1, Teams can generate several diagnostic logs.

Type	Clients	Contains
Debug	Browser, Windows, macOS	A text file read from the bottom up to capture client activity such as login, connection, call, and conversation events. Also includes information about the environment such as the client version. Teams uses continuous web logs (CWL) to save log data on a continuous basis to avoid the potential of losing valuable information due to memory buffer constraints. When Teams detects that it's running on low-end hardware (for example, Intel i3 generation 9 or older), it disables CWL and generates logs by flushing the memory buffer.
Desktop	Windows, macOS	Also known as the bootstrapper log. This text file notes details of communications between Teams and the underlying platform.
Media	Windows, macOS	Contains information about audio, video, and screen sharing in Teams meetings.
Teams meeting add-in	Windows	Contains information about the Teams meeting add-in used by clients like Outlook to schedule online Teams events. The file is found at %localappdata%\Temp\Microsoft\Teams\meeting-addin.

Table 12-1: Teams diagnostic logs

To generate the debug log, use the CTRL-Shift-Alt-1 key combination on Windows, and Command- Option-Shift-1 on a Mac. On all platforms, Teams creates the diagnostics log in the Downloads folder on the workstation and creates a name by combining *MSTeams Diagnostics Log* with the current timestamp.

Use the following commands to get the desktop log:

- Windows: click the system tray and find the Teams icon. Click the icon and select **Get Logs** from the right-click menu.
- macOS: Choose **Get Logs** from the Help pull-down menu.

By default, Teams turns off media logging. When needed, enable media logging through the General section of the Settings app and restart Teams. The locations of the various files created by media logging are noted in [this support article](#).

Utilities such as [Fiddler](#) and [Charles Proxy](#) are useful tools to collect a browser trace recording the communications between a Teams client and the back-end services. Make sure that you install the root certificate for the utility in the Trusted Root Certificate Store of your computer and enable HTTPS decryption before collecting anything. You can also use the [native functionality built into browsers like Edge](#) to capture logs (replace the references in the article to the Azure portal with Teams).

If asked to provide diagnostic information to Microsoft support, the easiest method to collect diagnostic information is to click the Teams icon in the system tray and select the **Collect support files** option. This command captures information used by Microsoft (like the debug log) and stores the data in a folder in Downloads. The folder is called *MSTeams Diagnostics Log* together with the date and time of its creation.

Migration to Teams

Microsoft has no migration tools to import existing content into Teams in such a way that the migrated information is usable within Teams. Instead, if you want to import content into Teams, you must do so manually. For example, you can email content to a channel from any application that supports SMTP, or you

can move documents into the folders in the SharePoint document libraries belonging to Teams. Several ISV products are available from companies such as AvePoint, Quest, and ShareGate to import documents from SharePoint on-premises servers, file servers, and other sources, or you can use Microsoft's free [SharePoint Migration Tool](#).

If you want to move content from another chat platform like HipChat or Slack to Teams, you can export data from these platforms. The difficulty then arises in how to import that data into Teams in the form of conversations and associated documents. The availability of [a Graph API to import third-party messages into Teams](#) has encouraged ISVs to investigate the area of Teams migration, so it's worth doing an internet search to discover what migration products are currently available.

All trans-platform migrations involve some form of data manipulation to ensure that the data imported into the target platform is usable. The migration code must parse the information taken from the source platform and update it to fit the data requirements of Teams. For instance, when the items forming a conversation go into a channel, the items must be in the correct order. The migration must apply permissions to attachments, and so on. Usernames are probably different, so some process of fixing these is necessary as otherwise, permissions might not work.

Chapter 13: Managing Teams Calling and Devices

Ben Lee

Previous chapters covered the structure and management of Teams. Here, we expand on that by looking at how to use Teams to make good quality calls and explore the devices available, from phones to full-blown meeting room systems that enhance the calling experience.

Teams Calling Fundamentals

Many organizations worldwide rely on Teams as their communications platform. While it is hard to get definitive figures from Microsoft about global usage, they claim 80 million monthly users use Teams for calling. Then, in the FY24 Q4 earnings call, Microsoft announced that 20 million users use Teams for PSTN (Public Switched Telephone Network) calling, up from 12 million in 2022. While the exact definitions of active users can be debated, there is no doubt that with numbers of this scale, Microsoft can rightfully claim a leading position in the enterprise calling space.

The technology behind Teams calling has a long history, and significant effort has been spent making what was once a very complex technology as simple and straightforward to deploy and use as possible. However, administrators still need to configure things correctly to ensure optimal performance. This chapter covers everything you should know to have a healthy Teams voice deployment, starting with some groundwork.

Calling Types

Let's start with defining some of the different types of calling that you might be using Teams for:

- **Teams Calls** is where users call from one Teams endpoint to another. It could be between two internal users, or an internal user and an external user. The important thing is that Teams is used on either end of the call. Media for a Teams call will either pass directly between the Teams clients or relay through components of the Teams service.
- **Teams Meetings** are when more than two people are on a call together. All communications occur between the Teams endpoint and the Teams meeting service. Teams automatically converts any call with more than two participants into a meeting. Meetings can also support PSTN dial-in, letting users participate via a standard phone number. While different types of Teams meetings are available (Standard, Webinar, and Town Hall), there is no difference between an ad-hoc meeting and a scheduled one.
- **Teams Phone** is a call between a Teams endpoint and a phone number. This could be a local number, an international number, a premium rate number, a mobile phone number, or even a call that terminates in another tenant. The important part is that the call passes over the PSTN network for at least one leg. The PSTN network is the global interconnection of phone carriers providing worldwide telephony services. There are four technologies for integrating a PSTN carrier: Calling Plans, Direct Routing, Operator Connect, and Teams Phone Mobile.

The licensing requirements for the different types of Teams calling can be complex, especially for Teams Phone, but they are broken down in the next section.

Licensing Teams Calling

Teams Calls and Teams Meetings, along with the default collaboration features, are included as part of the standard Teams licensing, but additional licenses can be needed for Teams Phone and other PSTN uses.

While the variety of licenses can seem complex or costly, it is essential to consider the overall impact of consolidating your telephony workload to Teams. In 2023, Forrester Consulting conducted a [Total Economic Impact™ \(TEI\)](#) study for Microsoft, providing a helpful framework that organizations can use to evaluate the complete ROI of migrating to Teams Phone.

Audio Conferencing

The Audio Conferencing license lets users dial-in and dial-out of meetings (subject to the appropriate configuration) using a PSTN number. Dial-in can be a quick and easy way for external users to join a meeting without any technology requirements or allow users without a suitable internet connection to participate in meetings. Remember that a dial-in user can only join the audio portion of the meeting.

By default, when a user is enabled for Audio Conferencing they have access to a set of Microsoft-provided shared numbers in over 180 Countries. You can also add more numbers to the service if you have numbers to bring from a legacy platform. Using toll-free numbers with the dial-in service is also possible, but the Communications Credits license is also needed to cover the cost of the inbound calls.

The Audio Conferencing license is standard in the Office 365 E5 plan but needs to be added for users with an Office 365 E3. Since 2022, Microsoft has been running various promotions where certain regions, such as the USA, can access a free version of this license. Alternatively, a pay-per-minute version is available for companies with a volume licensing agreement.

Teams Phone Standard

Teams Phone Standard is the basic license required for an account to have a PSTN number. This license covers the ability to make and receive PSTN calls via your Teams but does not provide the numbers or minutes themselves. You still need services from a carrier through one of several different delivery methods we discuss in more detail in the Teams Phone section.

Teams Phone Standard service plan is included in the Office 365 and Microsoft 365 E5 SKUs or is available as an add-on for the other Office 365 or Microsoft 365 plans.

Calling Plan Licenses

Calling Plan licenses let you use Microsoft as your PSTN provider in supported locations alongside the Teams Phone Standard license. Microsoft has relationships with carriers covering different portions of the world where they can directly integrate numbers and calling services with Teams. You can allocate numbers for your tenant from a Microsoft-managed pool or port your existing numbers to the service.

Calling plans are subject to geographical restrictions where Microsoft has regulatory approval to provide telephony services (currently in over thirty-one countries). A [complete list](#) of the available telephony services is available from Microsoft, listed by country.

Each Calling Plan license includes access to numbers, but they come in different varieties depending on the amount of included calling minutes (and supported destinations). Typically, plans include per-user domestic calling minutes (3,000 in the US and 1,200 in EU countries) and 600 tenant-wide international calling minutes.

The minutes in plans combine across all users with the same type of Calling Plan and in the same geography. For example, if you have two Calling Plans subscriptions for USA users, you have 6,000 domestic calling minutes each month. The number of minutes remains the same even if you add more Calling Plan users in, for example, the UK. Unused calling minutes do not carry over to the next month.

Calling Plans have two primary categories of licenses that pool like this:

- **Domestic Calling Plan** allows calls to the country/region where users are assigned. These are also available in either small, medium, or large variations.
- **Domestic and International Calling Plan** allows calls to a user's home country/region and to international numbers in 196 countries/regions.

A third kind of Calling Plan license operates on a Pay-As-You-Go model. This plan is available in either one of two zones, or for independent countries:

- **Zone1** covers: US, Puerto Rico, Canada, and the United Kingdom.
- **Zone 2** covers: Austria, Belgium, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Singapore, Slovakia, Slovenia, South Africa, Spain, Sweden, and Switzerland.
- **Independent:** Mexico.

PAYG Coverage: While Zone 1 Pay-As-You-Go calling plans cover the US and Puerto Rico they are not available for purchase in those regions. If you purchase calling plans via an agreement outside of these regions, you can allocate the plans to users homed there.

These plans have a low monthly service cost with unlimited incoming minutes, but all outbound calls must be paid for either using the Communications Credits pool or are billed directly in arrears. The PAYG model can be very attractive as a starting point for a company migrating to Teams Phone where they are uncertain how much usage there may be.

Communications Credits

Communications Credits are used as a pot of money that is then used to pay for telephony-related functionality that isn't covered elsewhere. Funds added apply across the tenant, but only the users assigned the license can access it. The Communication Credits are used to:

- Add toll-free numbers to Audio Conferencing meetings, auto attendants, and call queues. Toll-free calls are billed per minute.
- Cover costs for dial-out in a meeting when not covered by another license type.
- Dial-out from a Teams meeting to your mobile.
- Pay for any call-back features not covered by another license type.
- Cover international calls when a user is assigned a Domestic Calling Plans license.
- Covering telephony calls for a user where their pot of Calling Plan minutes has been used.
- Cover Pay-As-You-Go Calling Plan calls.

Communications Credits are available in the same countries where Audio Conferencing is available. You can buy and assign the license once you have either an Audio Conferencing license or a Phone System license in your tenant. The amount of funds you want to allocate varies greatly depending on expected usage so you should keep a close eye on it for the first few months. The funding can be auto-recharged to avoid any service disruption.

Communications Credits: Communications Credits are consumed at the published rates only when services are used. Any funds not used within 12 months of the purchase date expire and are lost. You can monitor Communication Credits under **Billing** then **Your products** in the Microsoft 365 admin center. It can take some time to set up Communications Credits, so it is recommended that a small amount be added to the tenant to be ready for any requirements at short notice.

Number Types

Numbers in Teams are split into two main categories depending on their intended use:

- **User Numbers** are allocated to users for use with Teams Phone and are used to route calls in and out. User Numbers only apply if you are consuming Teams Phone via Calling Plans or Operator Connect.
- **Service Numbers** are used in several different places, such as dial-in conferencing numbers or for VoiceApps (telephony-enabled workflows) with Attendants and Call Queues.

If you are using Direct Routing, you will not see any numbers for your trunks listed in the numbers section of the Teams admin center, as Teams does not have visibility downstream from your voice gateways. Also, in normal circumstances, numbers can be changed between these types, so you aren't limited to the initial selection.

E.164: All number management in Teams uses E.164 format, where numbers start with a + symbol, followed by country, area, and local access codes i.e.+44191374111 represents a UK number in the Newcastle region. Teams automatically converts user-entered numbers from their local country format into E.164 for you (you can modify this as needed and is covered in the Calling Configuration section)

User Numbers

If you sign up with a carrier via Operator Connect, the operator usually publishes your number allocation directly to your tenant.

If you want numbers provided by Microsoft, you must first have Calling Plan licenses available in your tenant. If you use Pay-As-You-Go Calling Plans, you are entitled to 1 number per license, or if you are using standard Calling Plans that have a minute bundle included, then the following formula applies:

$<\text{Number of Calling Plan Licenses}> \times 1.1 + 10$

In other words, if you have 50 Calling Plans, you can order 65 numbers.

Ordering new user numbers from Microsoft is done through the Voice section of the Teams admin center, where you specify the type (user) and quantity of numbers you need. If you have not added a location for your users, you must provide a location during the ordering process. The location describes where you are in case of an emergency and defines the area code you get for your numbers.

After finding a suitable block of numbers, you have 10 minutes to claim the numbers before the system releases them back to the available pool.

Because numbers are drawn randomly from a pool of what is available to Microsoft, it is unlikely that you will find consecutive numbers. However, the importance of number ranges is diminishing for most organizations as dialing is now done via contact cards rather than from memory. However, if you need specific ranges or have other number-related requirements, you can create a ticket with Microsoft, who will see what they can access via their carrier.

Number Porting: If you need to port existing numbers to Microsoft, this is usually possible but does vary by carrier and location. [Microsoft provides](#) details about the porting process for each country, along with any specific notes.

Service Numbers

Service Numbers differ from user numbers as they are designed to handle larger call volumes so may be provisioned on different back-end infrastructure. There are two types of Service Numbers: toll numbers and toll-free, depending on who pays for the incoming call. Service numbers can be provided through an Operator Connect carrier or accessed via Microsoft from their pool or through porting (see previous section's note).

Phone system licenses are required for toll numbers, and toll-free numbers also require Communications Credits to cover the incoming call cost. Calling Plans are not needed to take Service Numbers from Microsoft.

Service Numbers from Microsoft are available in approximately 80 countries. To add new service numbers, go to the Teams admin center, navigate to **Voice** then **Phone numbers** and click **Add**. From there you define the country, type, and region to find suitable numbers.

The amount of Microsoft service numbers a tenant can request is also based on the total number of Phone System and Audio Conferencing licenses purchased. Microsoft has a [table](#) of the allocation bands, but these are the most common allocations:

- If there are 1-25 licenses, 5 service numbers can be requested.
- If there are 100-149 licenses, 30 service numbers can be requested.
- If there are 500-749 licenses, 90 service numbers can be requested.
- If there are 1000-1,249 licenses, 125 service numbers can be requested.
- If there are 7,000-9,999 licenses, 500 service numbers can be requested.
- If there are 50,000+ licenses, 1500 service numbers can be requested.

Teams Administrator Roles

Like the rest of the M365 product stack, Teams supports different access roles to meet best practices around restricting administrative access to the platform.

Because the Teams Calling workloads are relatively specialized, there are several different admin roles available that cover them:

- **Teams Service Administrator:** can manage everything Teams-related without needing Global Admin rights, including all Teams Calling configuration.
- **Teams Communications Administrator:** can manage calling and meeting features within Teams.
- **Teams Telephony Admin:** can manage/report on calling settings for users and across the tenant.
- **Teams Communications Support Engineer:** can troubleshoot communications issues with access to advanced tools.
- **Teams Communications Support Specialist:** can troubleshoot communications issues within Teams using basic tools but cannot see user-identifying information such as SIP addresses or phone numbers.
- **Teams Device Administrator:** can manage Teams devices from the Teams admin center.

The roles can be combined if additional permissions are needed. For example, if you are working with an AV partner who is deploying devices for you at sites, they could have the Device Administrator role for managing the rollout and the Support Specialist role to allow them to troubleshoot any calling issues without being able to alter any tenant calling configuration.

Administrative units can also further restrict access, but currently, this is only supported for the Device Administrator role. An everyday use case for this would be to limit site managers' access to specific geographies; Microsoft shows how to do this in the [documentation](#).

Resource accounts: The Teams Service Administrator role used to be able to create resource accounts for use with Voice Apps, but this permission will be removed in late 2024. Teams administrators may need additional rights to continue creating Voice Apps after this change has been completed.

Global Reader: The Global Reader built-in RBAC role cannot access some Teams functionality. Most relevant here is the inability to view some phone-related reporting and lack of access to manage Teams phones. A more complete list of these restrictions is available [online](#).

Networking Preparation

Almost everything you do inside Teams sends traffic backward and forwards from your endpoint to the Microsoft service. In non-calling workloads, we usually aren't too concerned about the path traffic takes or how fast the connection is (unless things become terrible). However, any calling workload described above is very sensitive to bad network conditions as the voice and video are processed in near real-time. If we end up on a network connection where, for example, there is very high latency, calls will have a lot of gaps or garbled voice/video. Therefore, despite discussing networking best practices in previous chapters of this book, they are so essential for Teams Phone & for Teams devices that we will explore them in depth here with a specific focus on these workloads. Without the basic foundation of a reliable network, your environment will not be able to support good-quality calls, and the deployment will not succeed.

Traffic Optimization

There are two basic design principles that we should apply when working with network optimization for Teams, summarized as follows:

1. Ensure you move traffic onto the Microsoft network as quickly as possible:
 - a. Use local internet breakout.
 - b. Use local or regional DNS resolution. Microsoft 365 and Teams use GEO DNS for name resolution, meaning that you need to resolve the Teams services using local DNS to get the IP addresses of services closest to you.
 - c. Avoid sending traffic over internal or multiple WAN links unless they are very low latency.
2. Interfere with the network traffic as little as possible:
 - a. Open all the correct IP and port ranges required by Teams communications (see below).
 - b. Disable any deep packet inspection on the traffic.
 - c. Disable any WAN optimization technologies.
 - d. Avoid using VPNs with Teams traffic.

Following these basic principles helps to move traffic from the client and over to Microsoft as quickly and cleanly as possible, where it becomes their problem.

Media Relays: Teams meetings and calls route to local media relay services that are independent of the region that hosts your tenant. For example, if your tenant is in Europe and a team of four people in the US meet, the media flows through US media relay services to ensure the best possible quality for the call.

Microsoft documents [the range of IP addresses, ports, and FQDNs used by Teams](#) and other Microsoft 365 workloads accessed when consuming services. Microsoft categorizes traffic three ways:

- **Optimize:** this traffic is extra sensitive to network performance, latency, and availability. The IP addresses listed are guaranteed to come from Microsoft-hosted IP ranges. This category covers the endpoints used to process Teams media.
- **Allow:** is not as sensitive to network performance and latency but still provides connectivity to Microsoft 365 services and features. This category includes the main teams.microsoft.com URL.
- **Default:** should be handled as regular internet traffic, no optimization required. Non-Microsoft data centers could host these IP address ranges. The traffic could be icons inside SharePoint or other supporting types of data.

The Optimize and Allow ranges should be allowed to bypass any advanced network security features as they are effectively extensions of your own data center locations. To help alleviate any security concerns, all calling traffic that Teams puts out over the network is encrypted so can pass over the internet without additional protections.

You may get random connectivity issues, call drops, or poor audio, video, and desktop sharing quality if traffic is not optimized correctly.

ExpressRoute: Is ExpressRoute needed for Teams? The short answer is no, you still connect to the same IP addresses and services regardless of using ExpressRoute or the internet. ExpressRoute is used when you need an end-end SLA on the connection, or guaranteed bandwidth to Microsoft.

If you have constraints on existing internet connectivity, adding a new ExpressRoute connection may be an option. However, if you have lots of branch sites, providing them with local internet breakout may be a better overall solution, as a centralized ExpressRoute connection makes the overall traffic path longer. For a more detailed explanation of the considerations, read Microsoft's [article](#).

The Microsoft 365 Network Connectivity report, found under Health in the Microsoft 365 admin center, can help give an overview of how your tenant and networks are performing. This report can validate site performance as part of the planning process and monitor performance as part of the operational process. However, better tools are available for deeper dives into call troubleshooting; see the Troubleshooting and Monitoring Calls section.

This report highlights network performance for different technologies, including Exchange Online, SharePoint Online, and Teams. It forms part of the overall Adoption Score. The performance shown is based on the same network metrics (packet loss, jitter, and latency) highlighted by the Call Analytics and Call Quality Dashboard, which is also explained in the later Troubleshooting and Monitoring Calls section.

The location information shown here is a mix of company offices, home offices, and places where users connect to Office 365 on the move. Locations can be added, including the physical office location, LAN subnets, and the public IP addresses presented from that location. Locations can filter the reports to show performance for managed vs unmanaged locations. Note that it can take up to 72 hours before data is available for a location after creation.

Network Testing and Planning

Two network testing tools, and a planning tool are available to test, troubleshoot connection quality and plan for Teams media traffic. When running any connectivity test, you need to check at least two places: close to your network edge and again where users are located. By comparing the results, you can identify if there are any differences in quality between your network edge and user locations that might indicate bottlenecks in your network. Remember that a single result is not a sufficient sample size for an accurate overview. By running many tests at different times of the day over a sustained period, you will gather enough data to highlight trends within your network. By understanding the trends, you'll know if a more thorough investigation of internal network quality is necessary.

Microsoft 365 Network Connectivity tool is the most user-friendly and can be accessed via <https://connectivity.office.com/>. From there, you can run network tests from your current location, and when they are complete, you can upload the results. This tool feeds into the Microsoft 365 Network Connectivity report. It shows how you connect to the Microsoft network, which public DNS resolver is used, and the connectivity performance for Exchange Online, SharePoint Online and Teams.

When running the test, the site prompts you to download a file for more complete results. After downloading, this executable file runs several connectivity tests and returns the results to the service. The test almost seems to stop towards the end, with a long pause before completing. At this point, the test generates some sample calls; each call is 17 seconds long and helps measure audio, video, and desktop sharing performance. After completing, you can review the captured data and see if any metrics are below expectations.

If you are signed into Microsoft 365 when you run the test, the test automatically uploads the data to the tenant for aggregation into the Microsoft 365 Network Connectivity report.

Teams Network Assessment Tool is the second tool, providing a more manual method to gather network performance data. This [command line tool](#) measures only Teams performance and does not upload its results to the Microsoft 365 admin center. It has two main functions: one to check for open Teams ports and protocols (run with no command line options), and the second to generate sample calls (run with `/qualitycheck` switch).

This tool does not require any Teams components to be installed on the machine, so it can be run from servers in data centers to help map out your network paths. Figure 13-1 shows an example run from the start of the test; you can see the local IP, Reflexive IP (Client's public internet IP), and the Remote IP of the service alongside the key network metrics:

```
C:\Windows\system32\cmd.exe: x + v

C:\Program Files (x86)\Microsoft Teams Network Assessment Tool\NetworkAssessmentTool.exe /qualitycheck
Microsoft Teams - Network Assessment Tool

Initializing media flow.

*****
Starting new call

Media flow will start after allocating with relay VIP FQDN: worldaz.tr.teams.microsoft.com
If user wants to allocate with a particular relay VIP IP address, please specify in NetworkAssessment.exe.config.

Waiting for call to end after 300 seconds, displaying call quality metrics every ~5 seconds.
Change the 'MediaDuration' field in the NetworkAssessmentTool.exe.config file to change the media flow duration.

TIMESTAMP is in UTC. LOSS RATE is in percentage, out of 100.
LATENCY and JITTER are in milliseconds, and are calculated as averages in ~5-second windows.
PROTOCOL displays whether UDP, TCP (PseudoTLS/FullTLS), or HTTPS protocol was used to allocate with the relay server.
Note that for PROTOCOL, UDP protocol is attempted first to connect to the relay, by default.
LOCAL ADDRESS is the local client IP and port that media is flowing from.
REMOTE ADDRESS is the peer (relay server) destination IP and port that media is flowing to.
IS PROXIED PATH shows whether a proxy server is used to connect to the relay, only applies to TCP/HTTPS connections
LAST KNOWN REFLEXIVE IP shows what your latest public (NAT translated) IP and port is that the relay sees during media flow.

[If LOSS RATE is 100%, the output lines here will be in red]

Quality check source port range: 50000 - 50019

Call Quality Metrics:

2023-06-24 20:37:57      Loss Rate: 0          Latency: 18.98      Jitter: 19          Protocol: UDP
Local IP: 192.168.1.3:50006  Remote IP: 52.112.175.103:3478
Is Proxied Path: False      Last Known Reflexive IP: 212.159.102.162:23124

2023-06-24 20:38:04      Loss Rate: 0          Latency: 19.2       Jitter: 11.25        Protocol: UDP
Local IP: 192.168.1.3:50006  Remote IP: 52.112.175.103:3478
```

Figure 13-1: Microsoft Teams Network Assessment Tool

By default, the tool runs for 300 seconds and saves the output to `%localappdata%\Microsoft Teams Network Assessment Tool\<date_timestamp>_quality_check_results.csv`. You can open the results file and calculate your average for that run. Comparing results from locations and different times of day helps build up a picture of your overall network state. The `Usage.docx` file found at the tool install location contains information on configuring longer iterations and modifying other advanced parameters.

When doing client testing, performing a quick network path test can also be interesting to help identify any issues. A simple way to do this is to take the same IP address as shown as the destination in the Network Assessment Tool (or to `worldaz.tr.teams.microsoft.com` - which will resolve to your "nearest" transport relay) and use tracert. For example:

```
C:\>tracert worldaz.tr.teams.microsoft.com

Tracing route to b-tr-teamsc-euno-10.northeurope.cloudapp.azure.com [52.114.231.1]
over a maximum of 30 hops:

 1   1 ms    1 ms    1 ms Firewall.net [192.168.100.254]
 2   11 ms   11 ms   10 ms 250.core.plus.net [195.166.130.250]
```

```

3 12 ms 12 ms 11 ms 84.93.253.87
4 11 ms 11 ms 11 ms 195.99.125.140
5 12 ms 11 ms 12 ms peer3-et7-0-1.redbus.ukcore.bt.net [194.72.16.74]
6 13 ms 12 ms 11 ms ae60-0.1ts-96cbe-1b.ntwk.msn.net [104.44.13.46]
7 13 ms 13 ms 12 ms 51.10.1.17
8 22 ms 24 ms 22 ms be-126-0.ibr02.1on22.ntwk.msn.net [104.44.32.20]
9 22 ms 21 ms 23 ms be-13-0.ibr02.dub07.ntwk.msn.net [104.44.19.23]
10 30 ms 22 ms 22 ms ae120-0.icr01.dub07.ntwk.msn.net [104.44.11.76]
11 * * * Request timed out.
12 * * * Request timed out.
13 * * * Request timed out.
14 * * * Request timed out.
15 * * * Request timed out.
16 52.114.231.1 reports: Destination host unreachable.

```

In the trace, you can see that the transport relay address is resolved to one located in northern Europe, and the trace then commences. We enter the Microsoft network at about 5 hops and then lose responses from hop 11 onwards. Certain parts of the Microsoft infrastructure do not respond to pings and will not show in the trace. You should expect the hop count to be less than 20 before you reach the destination. If it is higher, try contacting your ISP to see if they can optimize the path for your connection. Higher hop counts introduce more opportunities for latency and jitter to exceed acceptable thresholds.

Network Planning can be done through the Teams admin center, available under **Planning** section. This can help estimate the network capacity required to support Teams based on the number of users, links between sites, and internet breakouts. Planning like this is not an exact science and the model is based on the use of personas to represent average or anticipated calling behaviors.

In the planning tool, you define personas, subnets, sites, and connectivity links to model how your locations connect to Teams. You can also add Microsoft Teams Rooms (MTRs) as specific personas, which is important as they usually consume more bandwidth than a typical user. The output from the planner is a report listing estimated constraints in your network, which is a good starting point for a deeper network assessment.

Remember that planner is only based on anticipated usage so may not match your real-world experience. During and after your deployment, you should check the data in **Proactive Call Quality Alerting**. To assist with proactive call quality monitoring, rules can be configured to alert via a Teams message (or webhook) when certain users are having calling issues. This feature does require a Teams Premium license for the users who can be monitored.

To configure real-time call alerting in the Teams admin center, expand Notifications & alerts and select Rules. Here you can select three types of real-time monitoring available for calls: Audio, video or screensharing quality. Each rule allows you to select:

- **Networking parameters to monitor:** Specify thresholds for Packet Loss, Jitter, Local heal ratio, and Round-trip time.
- **Time period:** Specify what length of time will trigger the poor call quality rule
- **Scope:** Select which Teams Premium users to monitor
- **Subnet:** if the rule should trigger for just internal, or internal and external subnets
- **Action:** Which team, channel or webhook to trigger when the rule conditions are activated

If you have Teams Premium licensing this is a great way to be proactive about quality issues for key users in your organization but be aware that you cannot specify different alerts or values for different groups of people. All users you want to monitor will be covered by the same rule.

Call Quality Dashboard (CQD), which monitors actual usage and user experiences. Examples for using the planner can be found on learn.microsoft.com.

Automate Planner: A [PowerShell script is available](#) to help with automating the population of the Network Planner for complex deployments.

Bandwidth usage via Resource Monitor: It is possible to use Resource Monitor on your PC to monitor Teams client network usage in real-time. You get an overview of how much bandwidth Teams uses at any moment, and you can upload information to Azure Monitor. This [blog post](#) shows how you could use this to build a custom monitoring solution.

Documenting Internal Networks and Subnets

Several Teams tools that help with planning, reviewing call quality, managing performance, and controlling calling behaviors (such as emergency calling) rely on data from the network. Unfortunately, Teams does not have a central location or networking configuration database that can be used so each tool has its own input requirements. If you are starting to plan your Teams voice journey or want to begin optimizing your deployment, it is recommended that you start gathering networking data that can be fed into these tools:

- Teams Network Planner.
- Network Topology in the Teams admin center.
- Microsoft 365 Network connectivity, part of the Adoption Score.
- Microsoft 365 Network connectivity test.
- Call Quality Dashboard.
- Reporting Labels in the Teams admin center.

Not all the tools need the same information, but if you create a complete data set in, for example, an Excel spreadsheet, you can reuse the data as needed. Here is the information you should consider gathering for your deployment:

- Site name.
- Internal network subnet range.
- Network Mask.
- Public IP(s) the client will present themselves with.
- Physical location address.
- Physical location City.
- Physical location State.
- Physical location Region.
- Physical location Country.
- Building name(s).
- The approximate number of users.
- Expected number of Meeting Room Devices.
- Internet breakout with bandwidth if local.
- If ExpressRoute is being used for connectivity to Microsoft.
- If branch site, which site is it connected to for internet breakout.
- If branch site, WAN link bandwidth.
- If using Teams Phone, how will it be delivered (Calling Plans, Operator Connect, or Direct Routing).
- The FQDN of the local Session Border Controller (SBC) if you are going to use Direct Routing.
- The proxy SBC FQDN, if you plan to use this with Direct Routing.

Location Awareness

Location is critical for several calling scenarios, including emergency calls, where reaching local responders is vital. Teams clients use multiple network indicators to determine where they are located. This section covers the key points about where and how Teams processes location-related data.

Trusted IP Address

The Teams client's first check is to validate if it is connecting from a company location. It does this using Trusted IP Addresses. When the Teams service receives an incoming client connection, it will usually only see the public IP address of the edge firewall that handles the outbound connection. For most companies, this will be part of their data center IP range or that of the internet connection at the local branch office.

If the reflexive IP of the client (the Public IP as seen by the Teams service) does not match one configured in the tenant, then the client concludes that it is not at a corporate location and stops processing other location-related policies.

Trusted IPs can be configured in the Teams admin center and are found under **Locations**, then **Network topology**, and in the **Trusted IPs** tab. Here, you can view and add new IP ranges. These can be IPv4 or IPv6 ranges or individual IPs. Trusted IPs can also be configured through PowerShell using the `*-CsTenantTrustedIPAddress` cmdlet family.

Best practice dictates that all public IP ranges used in the organization should be added to ensure no locations are missed, as this is the first step when processing location by the client.

Location Information Services – Emergency Address

Location Information Services (LIS) is a location database used when making emergency PSTN calls. The primary purpose of LIS is to identify a user's physical location so that if an emergency service needs to respond to the call, they are going to the correct physical location.

LIS can take four bits of networking information to help identify where a user is located:

- **Wi-Fi Access Point** takes the BSSID of the wireless access point the device is connected to.
- **Switch Port & Network Switch** uses Link Layer Discovery Protocol (LLDP) to identify the port and Chassis ID of the switch the device is connected to.
- **Network Subnet** is the IPv4 or IPv6 address of the network the device is currently connected to.

These identifying bits of networking information are used to associate the user with a Place or Emergency Address. Emergency Addresses are added to the tenant and are "verified" soon after creation. Once an Emergency Address has been verified, it can't be edited, you must create a new address and migrate any allocated numbers or users. An Emergency Address can contain one or more places, or the networking data can be associated directly with a site. Places are not validated but are used to indicate more specific locations for a large site, such as the floor of a user in a larger building.

You can view current addresses added to your tenant and their associated networking information in the Teams admin center under **Locations**, then **Emergency addresses**. Note that when working with these settings in PowerShell, Emergency Addresses are called Civic Addresses, and Places are Locations.

Address coordinates: When adding a new Emergency Address, you must provide the location's latitude and longitude (to 6 decimal places). If the automatic address detection does not populate this for you, you can right-click on most mapping websites to copy the latitude and longitude of the cursor position to the clipboard.

Legal requirements: The legal requirements for how emergency calls are handled varies worldwide, country by country. Teams can usually be configured to meet these requirements but it is crucial to check with a local legal team what behavior is required, and to validate your Teams deployment by thoroughly testing your emergency calling setup.

Network Topology in the Teams Admin Center

The next use for location is to dynamically assigning policies to clients based on their current subnet. Subnets are allocated to sites, and sites are grouped into regions (although regions do not impact the configuration or usage of subnets).

The following four policies can be dynamically allocated to a client:

- **Location Based Routing:** Used to optimize how traffic passes between a client and an SBC. Covered in more detail under Toll Bypass Restrictions.
- **Network Roaming Policy:** Used to restrict Teams' bandwidth for video calls. See below for more information.
- **Emergency Calling Policy:** Used to configure what happens when an emergency call is made, such as notifying building security personnel.
- **Emergency Call Routing Policy:** Used to determine the types of numbers used for emergency services, and where to route them if using Direct Routing for calling.

The location for Network Topology is done purely by matching the local IP address of the client against configured site subnets. Site policies have preferences over individual user or global policies and are evaluated for each endpoint.

To create a new Site or Subnet, go to the Teams admin center and, under **Locations**, expand **Networking topology**. You can add a new site, associate subnets, and allocate policies here.

Alternatively, you can use PowerShell to configure these, the following commands create a new site called "Site1" in region "Region 1" and associated with the subnet of 192.168.1.0/24.

```
New-CsTenantNetworkRegion -NetworkRegionID "Region1"
New-CsTenantNetworkSite -NetworkSiteID "Site1" -NetworkRegionID "Region1"
New-CsTenantNetworkSubnet -SubnetID 192.168.1.0 -MaskBits 24 -NetworkSiteID "Site1"

Identity NetworkRegionID Description CentralSite
-----
Region1 Region1          Region1
Site1   Region1
192.1...
```

Network Roaming Policy

A challenge for branch sites with network constraints is that calls and meetings can consume too much bandwidth for video and screen sharing. The Network Roaming policy is a per-site policy that ensures locations with low bandwidth are not overloaded by Teams traffic, regardless of their Meeting Policies. You can then avoid relying on users to remember that they shouldn't be using video in a particular location and inform them that video does not work in this location because of network restrictions.

Policies can be configured to allow or block video streams or limit the bandwidth used per endpoint for a video stream. To modify the default or create site-specific policies, go to the Teams admin center, then **Locations, Network topology**, and go into the **Roaming policies** tab.

To continue our site example from above, here we use PowerShell to create a new policy restricting the available bandwidth to 2000Kb (down from the 5000Kb default)

```
New-CsTeamsNetworkRoamingPolicy -Identity "Site1RoamingPolicy" -AllowIPVideo $false -MediaBitRateKb 2000 -Description "Site1 roaming policy"

Identity      : Tag:Site1RoamingPolicy
AllowIPVideo  : False
MediaBitRateKb : 2000
Description    : Site1 roaming policy
```

To finalize the setup, modify the site you created representing the location and add the new Network Roaming policy:

```
Set-CsTenantNetworkSite -Identity "Site1" -NetworkRoamingPolicy "Site1RoamingPolicy"
```

You can validate the site configuration with this command:

```
Get-CsTenantNetworkSite

Subnets          :
PostalCodes      :
Identity         : Site1
NetworkSiteID    : Site1
Description      :
NetworkRegionID  : Region1
LocationPolicy   :
EnableLocationBasedRouting : False
SiteAddress      :
EmergencyCallRoutingPolicy  :
EmergencyCallingPolicy   :
NetworkRoamingPolicy   : Site1RoamingPolicy
```

To ensure this setting applies to Teams meetings, *AllowNetworkConfigurationSettingsLookup* must also be enabled in your meeting policies (either Global or per-user). For example, this command updates the global Teams Meeting policy:

```
Set-CsTeamsMeetingPolicy -identity Global -AllowNetworkConfigurationSettingsLookup $True
```

Location in Reporting

Location information helps improve reporting when troubleshooting call quality in your environment. As users can be making Teams calls from many different network locations, differentiating between locations where you can influence network conditions and those you can't is essential.

The first is **Call Quality Dashboard** (CQD), which gives an overview of quality trends in your environment. The portal can be accessed from the Teams admin center under **Analytics & reports** or at

<https://cqd.teams.microsoft.com>. When opening the dashboard for the first time, you may feel that it does not give you much feedback. When location data has been configured you will also see the difference between outside traffic (typically unmanaged networks) and inside traffic (typically internal networks).

When uploading subnets to the portal, you should include the IP ranges for ALL internal networks, including VPNs with bypass. Having all networks captured will help identify any network configuration errors if subnets see significant changes in network traffic.

To import subnets into CQD you need to fill out a CSV file and upload it to the portal by navigating to <https://cqd.teams.microsoft.com/spd/#/TenantDataUpload> and using these steps:

1. Prep the CSV without headers, it should contain only the data you want to upload.
2. Select your file.
3. Select a start / end date if you need to process changed subnets after a particular date, otherwise leave it at default to apply immediately.
4. When imported successfully, you will see "Successfully uploaded file".
5. The reports may take up to 24 hours to reflect the new subnets.

The headers in the file are:

Network,NetworkName,NetworkRange,BuildingName,OwnershipType,BuildingType,BuildingOfficeType,City,ZipCode,Country,State,Region,InsideCorp,ExpressRoute

Here is an example showing how to populate the csv, using some of the information gathered at the beginning of this chapter:

```
192.168.1.0,US/Seattle/SEATTLE-SEA-1,24,SEATTLE-SEA-1,Contoso,IT
Termination,Engineering,Seattle,98001,US,WA,MSUS,1,0
```

The same data file can be uploaded as **Reporting Labels** to **Call Analytics**. Call Analytics shows the same metric information you found when running the Microsoft 365 Connectivity tests. You can use it to investigate individuals to see how their clients performed in calls and meetings. Call Analytics is covered further in the Troubleshooting and Monitoring Calls section.

Now that you understand the importance of documenting your network for Teams, make sure that you periodically update the information in CQD, Call Analytics, and other location services to keep it current.

Teams Meeting Enhancements

In an ideal world, any user on any device can join and participate in Teams meetings your users create, but this is not always possible, especially when inviting external users. For internal users, you can ensure they have the correct clients, managed networks, suitable devices, and meeting room equipment to use. Still, even then, you cannot guarantee sufficient bandwidth when users travel away from their offices. External users may not have Teams installed, be able to join from a browser, or have video conferencing equipment compatible with Teams, etc. It can be a long list of things that can add friction to the meeting experience.

As an administrator, you can create a more universal meeting experience that works with technologies beyond the Teams ecosystem, reducing or eliminating some of these issues.

By activating the Teams Audio Conferencing license, users can join meetings from any phone that uses the PSTN network, reducing the need for a good internet connection. Adding Cloud Video Interop integrations allows you to join Teams meetings from older, non-Teams native, standards-based video conferencing hardware.

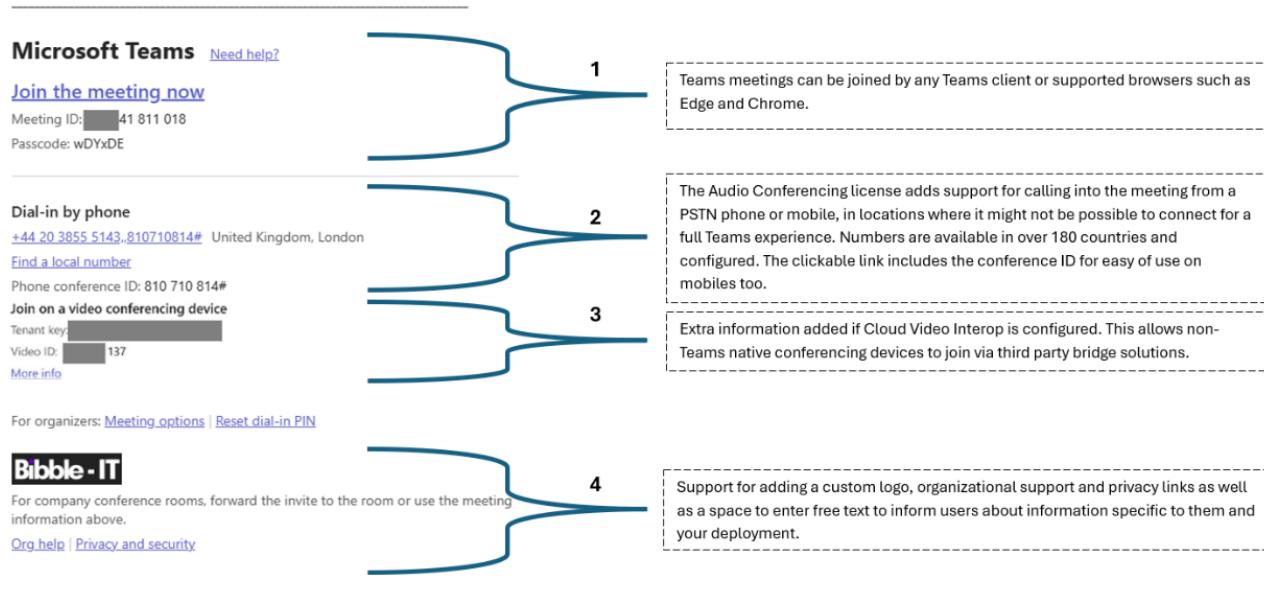


Figure 13-2: The anatomy of a Teams meeting invitation

When these are configured for a user, additional information is included in the meeting invite. Figure 13-2 shows a “universal” meeting invite breakdown:

- **Section 1:** contains the standard Teams meeting join information & clickable link.

- **Section 2:** is added by when Teams detects the availability of an Audio-Conferencing license to show dial-in numbers and join details.
- **Section 3:** is visible if the user has a Cloud Video Interop (CVI) license, these 3rd party solutions enable interop with other non-Teams meeting services and devices.
- **Section 4:** can be customized to contain additional information and help/privacy links.

To change the custom text and disclaimer shown in Figure 13-2, go to **Meetings** in the Teams admin center and open **Meeting Settings**. You can add a logo or an explanatory picture, a link to a support site, and additional information, such as a meeting recording disclaimer (if enabled). The meeting invitation can also include details in a secondary language and more than one dial-in number. Administrators can configure these settings in the meeting policy applied to the user (or at a global level).

Audio Conferencing for Teams Meetings

Audio Conferencing allows external users to dial into meetings using specified conference bridge numbers. These numbers can be both toll and toll-free and are available worldwide.

Licensing Audio Conferencing

The Audio Conferencing license operates independently of Teams Phone, it does not require the user to have a Teams Phone Standard license and covers any meeting they create.

You assign Audio Conferencing licenses to user accounts via the Microsoft 365 admin center or as part of your license lifecycle management via PowerShell or Group-Based Licensing (see the user management chapter). Teams automatically assign users a primary Audio Conferencing number based on their configured location (as specified in the Microsoft 365 admin center). You can change the assigned Audio Conferencing number by editing the user in the Teams admin center.

We recommend enabling Audio Conferencing for all users who may host meetings so that dial-in details will be ready if needed. If you do not have licenses such as Office 365 E5 that include Audio Conferencing, this could be an expensive outlay, however, there are two ways to purchase the service:

- Audio Conferencing service plan add-on to Office 365 E3 (included in Office 365 E5).
- A pay-per-minute license acquired through a volume license agreement.

The difference is that the regular add-on has a cost per user. In addition to enabling dial-in functionality, it also includes 60 dial-out minutes per licensed user per month pooled on a tenant level in [zone A countries](#). Dial-out minutes let you call out from a meeting to a PSTN number. When considering this licensing option, you should generally focus on the expected volume of dial-in minutes instead of dial-out, as this is commonly the more heavily used scenario.

The pay-per-minute license type is a free license you can assign to all users, but you need to use Communication Credits to pay for both dial-in and dial-out capabilities when consumed. Therefore, you should calculate how many dial-in minutes you might expect to use to help determine which license type is a good fit. Most volume licensing customers find the pay-per-minute model works out best, sometimes with a 90% cost reduction if covering all users. To help calculate costs for Audio Conferencing minutes, complete the form found at the bottom of the [Teams Phone sales site](#).

After deploying Audio Conferencing, you can monitor the available minutes and current usage from inside the Teams admin center. The report can be found under: **Analytics & Reports**, then **Usage reports** and selecting the **PSTN minute pools** report.

Configuring Audio Conferencing

If you deploy audio conferencing, there are some things to consider before rolling it out. First, the default setting is that all participants in the meeting hear a tone when someone joins a meeting using the Audio

Conferencing bridge. Some companies consider this a must-have requirement so that no one can join a meeting without everyone being aware. You can even force dial-in users to record their name that is played into the meeting. However, suppose you plan to have large meetings with many dial-in participants. In that case, these announcements can soon distract from the audio in the meeting itself with a constant stream of join/disconnect notices, so configure accordingly. The setting to control this behaviour is found under **Meetings, Conference Bridges, and Bridge Settings** in Teams admin center and applies across the tenant.

Secondly, when you assign the Audio Conferencing license as part of an onboarding process, Teams sends a welcome email to the user. This email gives the user some information about what Audio Conferencing is and their PIN (used to authenticate them if they were to dial-in to a meeting). However, this PIN is not something most users will need to use so that this email can cause more confusion than benefit.

If you want to disable the notification email, this can be done before configuring users with the `Set-CsOnlineDialInConferencingTenantSettings` cmdlet from the Teams PowerShell module:

```
Set-CsOnlineDialInConferencingTenantSettings -AutomaticallySendEmailsToUsers $false
```

Thirdly, if Direct Routing is deployed and integrated with your existing PBX (Private Branch Exchange – the term for a traditional Phone System) you could configure On-network Conferencing for Audio Conferencing. This allows users who have not yet been migrated to Teams to dial in to Teams meetings from their legacy phone without incurring any billable calls. Note that it is not intended to let you bring your own conferencing numbers to the Teams platform. The steps for configuring On-network Conferencing are available on learn.microsoft.com.

And finally, you can control how the phone numbers of external participants are displayed in the Teams meeting. By default, internal users can see the full phone numbers of those who join via audio conferencing, and external users will see a masked number like this: +35*****85.

The `MaskPstnNumbersType` setting managed with the `Set-CsOnlineDialInConferencingTenantSettings` cmdlet controls how Teams deals with participant numbers. The setting can be:

- **MaskedForExternalUsers:** This is the default value and means that external users see masked numbers.
- **MaskedForAllUsers:** Teams masks the number to all users.
- **NoMasking:** No masking of participant numbers is applied.

As an example, here's how to enable masking for participant numbers:

```
Set-CsOnlineDialInConferencingTenantSettings -MaskPstnNumbersType "MaskedForAllUsers"
```

The cmdlet is only available to tenants with the Audio Conferencing license.

Teams Meetings and Cloud Video Interoperability (CVI)

Even though Teams has many great native meeting room solutions, it may be too expensive for an organization to replace existing VTC's (Video Teleconferencing) in meeting rooms with new Teams Certified devices, or external users may be invited to your meetings who are not using Teams meeting room hardware. CVI is a mechanism through which certified third-party solutions can provide integration services that act as a bridge between the Teams meeting in your tenant and the other hardware or devices.

Note that the use of CVI is a one-way joining process, VTCs must always join the meeting with the details in the invite. A Teams client cannot dial out to them through the CVI service.

Four CVI providers are available today and are all pre-configured by Microsoft, so you need to select which ones you want to purchase and then enable it. You can access details of the providers via PowerShell:

```
Get-CsTeamsVideoInteropServicePolicy | Format-Table Identity, ProviderName
```

Identity	ProviderName
Global	DefaultProvider
Tag:PolycomServiceProviderEnabled	Polycom
Tag:BlueJeansServiceProviderEnabled	BlueJeans
Tag:PexipServiceProviderEnabled	Pexip
Tag:ServiceProviderDisabled	DefaultProvider
Tag:CiscoServiceProviderEnabled	Cisco

Each provider has its flavor of CVI:

- **Pexip** is the most flexible solution. You can choose to host the service yourself, use dedicated hosting from a suitable service provider, or access a shared service delivered by a service provider. Licenses are purchased through a Pexip partner. Pexip is the only solution that can differentiate between your internal VTCs and external ones, allowing internal VTCs to join directly while making external VTCs enter the meeting via the lobby.
- **Cisco** is the latest addition to the CVI platform, and their offering is delivered via their Webex cloud.
- **Poly** (now HP) offered a solution, RealConnect, but is transitioning to a new product provided in partnership with Pexip called CloudConnect.

Pexip differentiates itself with the ability to choose a flexible deployment method targeted at the enterprise market where there is a higher demand for integration with existing video infrastructure, customization, and control over media traffic. Additionally, with Pexip you pay for the capacity you need based on concurrency rather than per enabled user, so you can assign the capability to all users without extra licensing costs.

After choosing your preferred provider, you must run the `New-CsVideoInteropServiceProvider` command to configure the provider and its settings. You can set the provider up with false info in advance to see how it looks in your tenant. You can create the provider and grant the policy tenant wide or on a per-user basis:

```
New-CsVideoInteropServiceProvider -Name CVI -TenantKey "teams@yourdomain.com"
```

You can then grant the policy at a tenant wide level or per user. For example:

```
Grant-CsTeamsVideoInteropServicePolicy -PolicyName PexipServiceProviderEnabled -Global
Grant-CsTeamsVideoInteropServicePolicy -PolicyName PexipServiceProviderEnabled -Identity
ben.lee@office365itpros.com
```

Granting the policy formats your meeting with info from the correct predefined provider.

CVI Integration: To integrate with a CVI partner, you need to give the partner access to meetings in your tenant. Pexip has a [good writeup](#) of what permissions are used.

Content Delivery Networks for Large Scale Meetings

Teams has two types of special meetings for hosting large scale events: Live events (scheduled to retire soon but the original date was retracted) and Town Halls (introduced October 2023). These are both a special type of meeting designed to cover a broadcast-style scenario where a few presenters send content to many watching users. From a Teams point of view the same principles of networking optimization apply, however we also have the option to integrate third-party Enterprise Content Delivery Network (eCDN) solutions to minimize the streaming footprint on your internet connection.

eCDNs work as local caching repositories so that the required media is streamed once from the internet to a local destination. Clients nearby access that copy instead of downloading their own version. This can help reduce internet bandwidth by as much as 98% in the right circumstances. All Teams traffic is encrypted, so deploying custom eCDN solutions is impossible as the Teams media streams cannot be decrypted and examined. To work around this issue, Microsoft partners with several eCDN vendors, including their own

offering, to integrate their solutions into the Teams service at the source (like using third-party CVI solutions for meeting interop discussed above).

Each eCDN provider has their own pros and cons, so make sure to test different eCDNs against your specific scenarios. For example, Kollective offers a plug-in-free solution when viewing meetings through supported browsers. Alternatively, Microsoft's offering is simple to purchase via existing licensing agreements (or is included in the Teams Premium license). Whichever provider you select, you must configure the product in the tenant per the vendor's instructions.

This PowerShell command enables Hive Streaming for the tenant by amending the broadcast configuration.

```
Set-CsTeamsMeetingBroadcastConfiguration -AllowSdnProviderForBroadcastMeeting $True  
-SdnProviderName hive -SdnLicenseId {license ID GUID provided by Hive} -SdnApiTemplateUrl "{API  
template URL provided by Hive}"
```

If you run large Teams meetings with more than 1000 attendees, eCDN is used for all users in the overflow experience. This triggers automatically for user 1001 and up when they join the meeting. Here's where [to read more about eCDN](#).

Town Hall eCDN support: Microsoft is adding support for the same third party eCDNs as available for Live Meetings. This feature requires a Teams Premium license (as well as the relevant vendor licensing) to enable.

Teams Phone

Teams Phone is the general term for calling or answering calls through Teams over the phone or PSTN network. Teams Phone is a very mature solution, with many organizations worldwide relying on it as their only phone system. Many have undergone projects to remove costly legacy phone system solutions that require lots of support and upkeep.

Teams Phone Delivery Methods

To make and receive PSTN calls in Teams, besides having a Phone System Standard license, you must have some way of connecting to the PSTN (getting dial-tone) from inside your Teams environment. There are four broad categories of how you can manage this:

- **Calling Plans** with numbers from Microsoft if they are available in your region. Microsoft provides calling minutes and numbers.
- **Operator Connect** lets certified voice carriers/partners bring their telephony services directly to your tenant. The carrier provides calling minutes and numbers.
- **Teams Phone Mobile** is a variation on Operator Connect that works only with certain mobile carriers and allows your mobile number to be shared between Teams and your cellular mobile phone.
- **Direct Routing** provides a BYO approach where you (or a partner) provide SBCs and PSTN connectivity. Call charges and numbers provided by you or the chosen hosted DR provider.

Tasks such as allocating numbers or configuring policies, are shared across all delivery methods.

Calling Plans

Calling Plans provide the highest level of convenience for managing numbers in the tenant as it is Microsoft's native solution, but it can be inflexible or costly depending on the type and volume of calling your users will be doing. See the options in the Calling Plan Licenses section for details on the bundles or Pay As You Go options.

No other configuration beyond simply purchasing the licenses is required to enable Calling Plans in the environment. When you buy your first Calling Plans license, you can then start ordering user numbers as

described in the Number Types section. Be aware that numbers are regionally sensitive, so you can only acquire numbers from a location where Calling Plans are available. The user's *UsageLocation* attribute must also match the country whose numbers you are trying to assign.

When you assign a Calling Plans license to a user account, the following happens:

- The user's Voice policy is set to *BusinessVoice*.
- You can assign a user number to the account using PowerShell or Teams admin center.
- After assigning a Calling Plans license, it may take some time for the dial-pad to appear in the calling tab of the user's Teams client.

Operator Connect

Operator Connect bridges the gap between the management simplicity of Calling Plans (where no tenant configuration is required) and the freedom of Direct Routing (selecting your providers and negotiating minutes outside of what Microsoft can provide). It is a certification program where voice carriers or Partners (operators) must meet minimum requirements for connectivity into Microsoft 365 and maintain certain levels of calling quality. Once a partner has been certified, they are available for selection via the Teams admin center. The certification program only covers the technical aspects of the carrier-to-Teams integration; you and the provider handle all billing for PSTN services directly without Microsoft's involvement. Operator Connect is a simple way to add connectivity to the Teams in regions that Microsoft cannot cover with Calling Plans, and offers better flexibility to negotiate costs or continue using existing telco contracts.

Operator Connect settings appear under **Voice** and **Operator Connect** in Teams admin center. Here you can send a request to one of the operators offering services in your required countries (or contact them directly, outside of Teams). A notification goes to the operator, who will contact you to discuss packages and options for enabling their service in your tenant. Microsoft is not involved in the billing aspects of Operator Connect services. After completing the Operator Connect agreement, you can configure users and deal with number management as you would with Calling Plans. Many providers also have their own number management platforms outside of Teams where you can handle number provisioning.

Operator Connect Conferencing exists as an extension of Operator Connect, it can be used to bring your own carrier numbers to the dial-in conferencing platform. This can help if Microsoft does not have the required coverage or if you want to reuse existing conferencing numbers without porting them. Operator Connect Conferencing still requires either a standard Audio Conferencing license or a specialized Operator Connect Conferencing license.

The testing process behind Operator Connect is very rigorous and lengthy. To help rapidly onboard more carriers, Microsoft introduced a program called the Operator Connect Accelerator (OCA). OCA allows smaller partners to bring their PSTN offerings to Teams through several pre-certified providers, thus reducing their certification time while maintaining quality. The growth and expansion of the Operator Connect program also allows telcos to offer services in traditionally challenging locations such as India.

Teams Phone Mobile

Initially announced as Operator Connect Mobile, Microsoft rebranded this mobile variant of Operator Connect as Teams Phone Mobile. The goal is to deliver a true single-number reach solution for users who rely heavily on mobile connectivity.

Teams Phone Mobile expands the capabilities of Operator Connect by deeply integrating Teams calling with a mobile phone contract, giving users a single number that works across their mobile device (through an integrated e-SIM) and in the Teams client. This solution operates without requiring any complex forwarding rules or number masking to provide true single-number reach.

With carrier support requiring that they also provide mobile services, the list of supported operators is smaller than for Operator Connect. Rogers Business, Telia, T-Mobile, Swisscom, Verizon, and BT currently offer Teams Phone Mobile for their key regions. Other carriers are working through the certification process.

Without Teams Phone Mobile, a Teams Phone user can make and receive calls on their Teams number via the Teams client over a suitable data connection (GSM or Wi-Fi). Should they make calls using the cellular network, the call would present with their mobile number, and they could only receive inbound calls from Teams if they enabled call forwarding or simultaneous ring.

Teams Phone Mobile makes the user's cellular and Teams numbers identical. When they place a cellular call, the mobile carrier handles this like a Teams Operator Connect call with their back-end connections into Microsoft, so the user always makes a Teams call from their mobile phone. No forwarding or simultaneous calling configuration is required. Because any mobile call is effectively a Teams call, user presence updates and internal calls do not use the PSTN.

Direct Routing Architectures

Direct Routing is the fully flexible way to bring existing PSTN connections into Teams. Teams does not care what the actual PSTN connections are, they could be legacy Integrated Services Digital Network (ISDN), analog connections or SIP trunks to either another PBX or your carrier. What Teams does care about is that you:

- Have a [compatible SBC](#).
- Provide internet access to the SBC.
- Have an internet-resolvable DNS name for the SBC.
- Provide a public certificate for the SBC.
- Configure your firewall to allow Teams traffic to the SBC.

This SBC can be hosted in many different ways, and you may not even need your own SBC but can pay to use a service provider/partner's hosted SBC with whatever PSTN connectivity they provide.

Three main scenarios exist for deploying Direct Routing:

- Installed in your data center.
- Installed in Azure.
- Hosted by a Service Provider.

SBCs for analog devices: Some SBCs are certified to connect analog devices to Teams. Read more about it in the [Microsoft documentation](#).

Installed in Your Datacenter or Offices - You may install your own SBCs in a datacenter or local office, depending on what needs to connect into the SBC. This option is for companies that need to manage and maintain their own SBCs and have full control of call paths. This could be for a number of reasons such as: providing coverage in countries where neither carriers nor Microsoft can deliver Teams numbers (commonly countries such as Russia, China, or Brazil) or wanting media to stay on their network as much as possible.

Installed in Azure - You could install virtual SBCs in Azure to still have full control over them and include them as part of your managed infrastructure but do not have to maintain any hardware. This is a good choice if you have a strategy of removing on-premises equipment and wish to downsize your datacenter infrastructure. The leading SBC vendors (Ribbon and AudioCodes) have software-only versions of their SBCs and AudioCodes has a [whitepaper on how to set up their virtual SBC in Azure](#).

The requirements from Microsoft's side are still the same regardless of where the SBC is running and if it is a physical or virtual device.

Hosted by a Service Provider - Since the integration with Teams using Direct Routing is just a SIP trunk connection, service providers can easily connect to multiple tenants from a centralized SBC deployment. Microsoft supports a specific variation of Direct Routing designed for just such a scenario. The service provider registers a subdomain per customer from their infrastructure and uses this to connect to the customer tenant. This subdomain is then activated in the customer tenant and is available for use. The planning documents for supported multi-tenant Direct Routing scenarios can be found [online](#).

Consuming Teams Phone from a service provider is a good choice for organizations that do not want to manage any SBCs with their upstream connections and do not need close control of the calling traffic.

[When to Use Calling Plans, Operator Connect, or Direct Routing](#)

From an end-user perspective, all these delivery methods look the same. The difference is in what happens behind the scenes to make calls connect. The good news is that you can mix and match these solutions in the same tenant, depending on your specific requirements. For example, Calling Plans can be a quick and easy way to test out Teams Phone, but for broader deployment, you might find Operator Connect a cheaper solution, or you may want the flexibility to manage your own SBCs and migrate your current numbers and contracts.

Emergency Calling: [Emergency calling support](#) is available for Calling Plans, Operator Connect, and Direct Routing, but for Direct Routing, you are responsible for more parts of the process. With emergency calling support, you can configure settings such as notifications to your organization's security desk, include them in the call, or add in-client notification messages that your users must acknowledge.

Configurations for Direct Routing

When dialing from a Teams client, the following are all configuration elements used to determine where Teams will send the call:

- **Online PSTN Gateway:** contains the DNS name for an SBC and any configuration to send calls to it, such as forward P-Asserted-Identity (PAI) or Preferred Codecs.
- **Voice Routes:** matches the pattern of the number dialed against Online PSTN Gateway entries.
- **PSTN Usages:** hold one or more Voice Routes. They can be shared across different Voice Routing Policies.
- **Voice Routing Policy:** contain one or more PSTN Usages. These are assigned against users.

The configuration can be found in Teams admin center under **Voice** and is split between the **Voice Routing Policy** and **Direct Routing** sections.

This call routing can be confusing to set up initially and can become very complex when you have multiple SBC gateways and routes. This [article](#) provides a good reference for handling failover and other scenarios.

Detailed routing diagram: [This Microsoft diagram](#) gives an in-depth look at how routing works in Teams.

By default, the traffic path taken by media flows from your Teams client to the Media Processes (in the Teams service) and then to the SBC before being placed onto the downstream PSTN connection. However, this may not be ideal in scenarios where the user is already inside the firewall with the SBC, or if we want to reduce the volume of internet traffic generated.

With Direct Routing, three techniques can help with optimizing the media paths:

- Media Bypass for Direct Routing.
- Local Media Optimization for Direct Routing.
- Survivable Branch Appliance (SBA) for Direct Routing.

These scenarios do not apply to Operator Connect and are unlikely to be helpful when using Direct Routing hosted in Azure or Direct Routing hosted by a service provider, as the SBCs are outside your core company networks.

Media Bypass for Direct Routing - Media Bypass shortens the path of media traffic and reduces the number of hops in transit for better performance. This is a great option if you host an SBC in your data center or in Azure using Express Route. With media bypass, media is kept between the Session Border Controller (SBC) and the client instead of sending it via the Microsoft Phone System relay service. By enabling Media bypass, media traffic can negotiate to travel between the Teams clients and the external public leg of the SBC.

You must ensure that the SBC and firewall are configured to allow the correct ports (even if they are just from inside your network). Internal clients also need to resolve the public leg of the SBC and send media traffic to that IP address on the port range of 50,000 – 59,999. On some firewalls, this can cause [hairpinning issues](#) where internal traffic goes to an IP on the outside edge of the firewall. Only the media goes directly to the SBC; signaling still goes via the Teams services.

When Media Bypass is enabled, you can still limit access to the SBC from non-Microsoft external [IP ranges](#), forcing internet clients to relay via the Teams services and reducing your external attack surface area.

To support Media Bypass, the SBC must have ICE light negotiation configured, among other configuration changes. Each SBC vendor will have instructions specific to their devices on how to configure them. After configuring the SBC you then must enable Media Bypass against the SBC object in your tenant either via Teams admin center, or with the following PowerShell cmdlet:

```
Set-CSOnlinePSTNGateway -Identity "SBCSite1.office365itpros.com" -MediaBypass $true
```

Local Media Optimization for Direct Routing - Local Media Optimization is very similar to Media Bypass but takes things further by allowing internal clients to send media directly to an internal IP address on the SBC (rather than relaying to the external interface). This avoids firewall hairpinning and allows end-to-end QOS on the media traffic if needed. It can also hide multiple internal SBCs (for example, at branch sites) behind one master SBC (say, in the datacentre). Helping with scenarios where branch sites might not have suitable internet connections to support their own Direct Routing connections.

Local Media Optimization uses the same Trusted IP Address detection as discussed previously to determine if a client is inside a company location. If it is deemed external, Local Media Optimization is not used at all. It then shares the same location configuration data as the Network Roaming Policy to determine which configuration policy to apply if, depending on if the site of the client and SBC match or differ.

When configuring Local Media Optimization, you have two choices:

- **Always** sends media to the internal leg of SBC regardless of where the user is located if they are internal. The SBCs internal leg must be available from all internal networks.
- **Only for local users** uses the internal SBC leg if the users site and the site allocated to the SBC (*GatewaySiteID*) match. This can be helpful in deployments with multiple countries where you need to control traffic flow.

To enable Local Media Optimization, configure it via Teams admin center against the SBC object, or connect to the Teams PowerShell module and use the following cmdlet:

```
Set-CSOnlinePSTNGateway -Identity "SBCSite1.office365itpros.com" -GatewaySiteID "Site1" -MediaBypass $true -BypassMode "OnlyForLocalUsers" -ProxySBC $Null
```

In this command, the *ProxySBC* property is set to *\$Null* as this setting is mandatory even if not being used. This attribute is used when you have an SBC branch site without internet connectivity. The branch SBC routes its calls to a centralized SBC and then to Teams, using the central SBC as a proxy. You can still use Local Media

Optimization in this scenario, but clients need to be able to send media traffic to the internal leg of the branch SBC. To enable the *ProxySBC* functionality, the SBC is registered in Teams and a relay SBC configured. Here is an example PowerShell command to run to create a branch SBC using our existing SBC as the proxy:

```
New-CSOnlinePSTNGateway -Identity "SBCBranchSite2.office365itpros.com" -GatewaySiteID "BranchSite2" -MediaBypass $true -BypassMode "OnlyForLocalUsers" -ProxySBC "SBCsite1.office365itpros.com"
```

To complete the configuration, you would need to have a site called Branchsite2 with the correct local network subnets defined. Microsoft has some good example configurations available on [learn.microsoft.com](#).

Survivable Branch Appliance for Direct Routing - Because all processing happens in the Teams service, Teams Phone relies on an active internet connection to make and receive calls. If you have users at a location with unreliable connectivity or who need to be able to make PSTN calls during network outages, you can consider deploying a Survivable Branch Appliance (SBA).

An SBA is an SBC that, in addition to handling call routing, can also run software provided by Microsoft to maintain a limited amount of Teams services for local users if the internet is unavailable. The SBC must have dedicated connectivity to the PSTN to make and receive calls without an internet connection available.

When considering the deployment of an SBA, consider the following limitations:

- The SBA may require extra hardware or licensing from the SBC vendor.
- Does not support all Teams clients.
- Limited support for Voice Apps and call forwarding.
- No support for Voicemail.
- Clients must have been “online” before the internet dropped, so they can register with the SBA.
- The SBA receives/refreshes an authorization token with Microsoft that is valid for 24 hours. If this cannot be renewed, it may expire during the outage, which stops service. The 24-hour counter is from the time of the last refresh, so it is unlikely that you will receive a full 24 hours of coverage during an outage.
- Supports limited PSTN / Calling functionality in the Teams client.
- Emergency calling using e911 is not officially supported.

When an internet connection is unavailable, eligible clients connect to the SBA services. The SBA then handles signaling for setting up calls and directs the Teams client to route media to the local SBC. Although setting up the SBA can be complicated and requires Azure configuration, each vendor provides their own [documentation](#) relevant to their devices.

The configuration in Teams is simple and consists of creating the SBA object, and then an SBA policy that is applied to users containing what SBAs they can access.

The following three commands create a new SBA, configure a policy with the SBA, and assign it to an end user:

```
New-CsTeamsSurvivableBranchAppliance -FQDN "SBABranchSite2.office365itpros.com" -Description "SBA Branch Site 2"
```

```
New-CsTeamsSurvivableBranchAppliancePolicy -Identity "Branch Site 2" -BranchApplianceFqdns "SBABranchSite2.office365itpros.com"
```

```
Grant-CsTeamsSurvivableBranchAppliancePolicy -PolicyName "Branch Site 2" -Identity "ben.lee@office365itpros.com"
```

An overview of the SBA specific Direct Routing configuration and settings can be referenced

SBA limitations: An SBA may seem like an excellent solution to maintaining calling during an internet outage, but the limitations described above mean that it is often unsuitable. Most customers considering

one choose to improve resiliency in their internet connections (such as providing backup lines) to critical sites. This saves spending on hardware appliances that need to be maintained, and improving WAN connectivity helps sustain other services, such as access to documents and email.

Calling Configuration

After you decide how to consume telephony in Teams with Calling Plans, Operator Connect or Direct Routing, it is time to assign the Phone System license to users to enable calling capabilities. One account setting that is easy to overlook is the *UsageLocation* attribute. The location is assigned at account creation and influences the services available to accounts, especially phone services.

When Teams makes a call, the number format needs to be in the [E.164 format](#), a universal format that includes '+', country code, and subscriber number. Before the call is routed, the number is normalized into the E.164 format by dial plans. All users with a Phone System license are assigned a dial plan by default. This basic dial plan provided by Microsoft covers simple number conversions for the user's home country.

The *UsageLocation* attribute of a Microsoft 365 account controls the default dial plan, Audio Conferencing number, and whether a Calling Plan license can be assigned to the user. To check *UsageLocation* and the location-based *DialPlan* assigned, use the `Get-CsOnlineUser` cmdlet:

```
Get-CsOnlineUser ben.lee@office365itpros.com | Select-Object DisplayName, UsageLocation, DialPlan, TenantDialPlan
```

DisplayName	UsageLocation	DialPlan	TenantDialPlan
Ben	GB	GB	

To change the *UsageLocation*, use the `Update-MgUser` cmdlet (part of the PowerShell Graph SDK):

```
Update-MgUser -ObjectId ben.lee@office365itpros.com -UsageLocation US
```

Dial plan automation: Typically, the default dial plan covers most local, mobile, and national/international number types, but it may not capture certain country-specific special number types. The site [ucdialplans.com](#) has a broad set of scripts to help implement comprehensive normalization rules that are ready to import into your tenant. The site generates the necessary code to create *TenantDialPlans* that you can assign on a user level for the correct normalization of numbers. *TenantDialPlans* works together with the default dial plan. When dialing out, the normalization process looks at *TenantDialPlans* first and then at the default *DialPlan*.

Calling Policies

Calling Policies control the calling features available to users (Teams to Teams or Teams Phone, not meetings). A default global calling policy is available within a tenant found under **Voice** then **Calling policies** in the Teams admin center, but administrators can also create and assign custom calling policies. The settings controlled in a policy are:

- **Make private calls:** Acts as a control switch for all calling functionality in Teams.
- **Cloud recording:** Allows calls to be recorded.
- **Transcription:** Allows calls to be automatically transcribed by Azure voice services.
- **Routing for PSTN calls:** Controls how to route an incoming PSTN call, can be treated as an unanswered call, straight to voicemail or controlled by the user.
- **Routing for federated calls:** Same controls as for PSTN calls, but for incoming Teams-Teams call from users outside the Organization.
- **Call forwarding and simultaneous ringing settings:** Controls if incoming calls can be passed on to either other internal users, or external PSTN numbers.

- **Voicemail is available for routing inbound calls:** If inbound calls can be sent to voicemail. It can be either enabled, disabled, or left to the end-user to decide.
- **Inbound calls can be routed to call groups:** Controls if call groups can be configured to receive incoming calls.
- **Delegation for inbound and outbound calls:** Control access to calling delegates.
- **Prevent toll bypass and send calls through the PSTN:** Helps meet any legal requirements if international calling cannot pass over an IP network and must use the PSTN.
- **Music on hold:** If system music should be played when a call is on hold.
- **Busy on busy when in a call:** What should happen if a user is already on a call and a second one is received. **Enabled** rejects the call outright, **unanswered** triggers the users missed call settings and **user-controlled** lets users decide via client-side settings.
- **Web PSTN calling:** Allows PSTN calls to be made from the Teams web client.
- **Real-time captions in Teams calls:** Allows in-call captioning to be enabled.
- **Automatically answer incoming meeting invites:** Useful to configure against a meeting room account where you want the room to join if invited automatically.
- **Spam filtering:** Options to include SPAM notifications as part of the incoming call toast if Microsoft identifies the number as suspect.
- **SIP devices can be used for calls:** Ability to place calls from SIP registered devices.
- **Open apps in browser for incoming PSTN calls:** Allows integration with browser-based applications, can be used to show things like CRM data or support information relevant to the incoming caller ID.

Some of these settings can have an impact on the traffic path used. For example, suppose a user enables cloud-powered services like recording, transcription, or captioning. In that case, the media must go through the Teams service for processing. You may want to control other features at a more granular, country, or regional level (with corresponding policies) as different regions have different expectations. For example, with busy on busy some countries expect second calls to be rejected by default, and others expect them to ring through.

Cloud Voicemail

Another setting controlled by the **Calling policies** is Cloud Voicemail, which is available by default in the Teams client, even without the Phone System license. The voicemail capability replaces the old voicemail hosted by Exchange Online and Exchange on-premises servers. Microsoft hosts the voicemail service in Azure, and you control the availability of voicemail for users through the Teams calling policy assigned to their accounts. You can decide if users can enable voicemail manually, make it mandatory or disabled. If it is set to user-controlled, users can decide if unanswered calls go to voicemail by configuring it in the Teams client under settings. Sending a call to voicemail does not mean someone only has the choice to leave a message; you can further control the behavior of unanswered calls. These controls can be found under **Manage voicemail** in the **Settings, Calls** menu of the Teams desktop client.

Integrating cloud Voicemail with a hybrid Exchange solution is possible, but the user's mailbox must be in Exchange Online for voicemail to work with Teams. Voicemail supports depositing voicemail messages only in an Exchange Online mailbox and doesn't support any third-party email systems. As a fallback mechanism, Cloud Voicemail can resend messages using SMTP, which means the third-party email system could receive voicemail messages, but this has no guaranteed availability or support for features, so it is not recommended for production use.

Transcription of voicemails is enabled by default for all users enabled for Cloud Voicemail and can be turned off using the `Set-CsOnlineVoicemailPolicy` command. [Twenty-seven languages](#) are available for greetings, and transcription is available for ten.

Language support: Some countries have language laws requiring that callers must have the option to choose which of the country's official languages they wish to be served in. Voicemail has [Dual Language support](#) to meet this need.

Toll Bypass Restrictions

Over 50 countries, including India, China, Brazil, Algeria, Bahrain, and UAE have some form of toll bypass restrictions in their local law or telephony regulations. Essentially, they mandate that all international PSTN calls go through a local endpoint so that the (usually state-owned) telecommunications provider handles the call. So, for instance, if an organization has a support center in India, calls to international numbers must dial out from India. Therefore, modern call routing methods, such as least cost routing, are unhelpful in these scenarios. Essentially, we need to apply most cost routing for users in those countries.

Legal exceptions: Some countries do allow legal exemptions for such toll bypass restrictions depending on the intended use case, for example, if hosting an out-of-country contact center. You should seek legal advice on what is acceptable for your company and locations if in doubt so that you can configure Teams appropriately.

Microsoft has introduced [Location Based Routing](#) (LBR) to support this in Direct Routing based scenarios, LBR does not apply to Calling Plans as Microsoft does not offer services in these locations, and with Operator Connect your provider needs to manage it via their network. LBR is assigned on a site level and ensures that all international calls break out from the local SBC, enforcing international toll on international calls. Here is an example.

If you have users in India dialing a UK number and have SBCs in both India and the UK, ideally, you would route that call to the UK SBC and only pay the cost of a UK local call. However, this is not legally allowed as India has toll bypass restrictions. LBR would be configured to route these calls to the India SBC, which would be at full international cost. If one of those Indian users travels to the UK, LRB will match the new user and route calls to the UK SBC for the duration of their trip. If a UK user travels to India for a short period, they can still have their calls routed via the UK gateway.

LBR re-uses the same External IP, region, site, and subnets described at the beginning of this chapter. To use LBR, we need to enable the capability against the site we configured and assign a pre-defined Calling policy using the Teams PowerShell module.

```
Set-CsTenantNetworkSite -Identity "Site1" -EnableLocationBasedRouting $true  
Set-CSOnlinePSTNGateway -Identity "SBCSite1.office365itpros.com" -GatewaySiteLbrEnabled $true -  
GatewaySiteID "Site1"  
Grant-CsTeamsCallingPolicy -PolicyName "AllowCallingPreventTollBypass" -Identity  
"ben.lee@office365itpros.com"
```

The last command grants the built-in Calling policy called *AllowCallingPreventTollBypass* (where *PreventTollBypass* is set to `$true`) to a user. If you have a list of all users in a site, you can use the *New-CsBatchPolicyAssignmentOperation* to assign it to multiple users at once.

Number Management

There are three ways to consume phone numbers in Teams:

- Ordering them via Microsoft for Calling Plans
- Getting them from carriers via Operator Connect
- Acquiring them from carriers via sip trunks for Direct Routing

Service numbers, Calling Plan numbers, and Operator Connect numbers can be found in the Teams admin center by going to **Voice** and **Phone numbers**. However, Direct Routing numbers are not displayed in the

Teams admin center as Teams does not hold a record of your downstream ranges. You will see the location they belong to if they are available and details of how they can be assigned (available usage).

To manually assign a number to a user, use the filter in the top right to search by Unassigned status and match the location to your user. After finding a number you want to use, select it and use edit to assign it. Using these filters is a good way to investigate how many available numbers you have at any given time for a location. This page also gives you access to your Microsoft number order history, and you can get support using the link under the Actions menu for number-related issues, such as porting queries or changing number assignment types.

For a large enterprise deployment, it is important to think about number management lifecycle and automation because it can be a difficult task to handle. The Phone number portal in the Teams admin center is good, but it's data cannot be accessed via Graph API. If you use Direct Routing, or want to classify numbers by desirability, then you need to create your own management processes.

The following PowerShell command can retrieve all standard numbers used in your environment:

```
Get-CsOnlineUser -Filter {LineURI -ne $Null} | Format-Table DisplayName, LineURI
```

It will include numbers assigned to CAP, MTR, and Voice App Resource Accounts. With this, if you know your full number ranges, you could then programmatically find the next available number. [There is an example script](#) available to get you started with this number management automation. You could integrate the script into an existing identity management procedure or use it as part of a standalone number management process. For a larger environment, you might want to store this information in a database to keep additional information with the numbers. For example, if you need to mark the numbers of recent leavers so that Teams does not automatically assign the numbers to new users. You can add your own numbers for retention, and it will not offer numbers classified as gold or silver.

Below, you can find some situations where users either do not have a regular number assigned, or where inbound numbers require different handling:

- Private Lines
- Shared Numbers
- Unassigned number routing
- Blocking numbers/nuisance calling

Private Line - As a rule, Teams supports a single number per user. However, you can route calls from other numbers to a user using call forwarding or unassigned number routing rules. There is one exception to this rule, which is a feature called private lines. Private Lines are designed to solve a particular use case where a user has delegates who manage calls for them. A private line is a second number associated with the user that bypasses any inbound calling rules such as forwarding, delegates, or group calling and rings only the user directly. These incoming calls will have a visual notification on the toast and play a different ringtone.

Private lines can only be assigned via PowerShell using the `*-CsPhoneNumberAssignment` cmdlets, and the number type and delivery method must be the same as the user's main number. The private line cannot be used as the outbound number.

This feature should not be used as a workaround for assigning users numbers in multiple geographic regions. Instead, it would be best to consider configuring dummy accounts with delegates or using voice apps.

Shared Numbers - Historically, every Teams Phone user had a unique number assigned in Teams; however, [Shared Calling](#) allows multiple users to be configured for Teams Phone without having assigned numbers. Shared Calling also supports the use of a common base number with unique extensions per user to maintain internal extension based dialing capabilities.

Shared Calling uses an Auto Attendant with a Resource Account (covered in the Voice Apps section) with an assigned number and a PSTN delivery method set up. When a user is enabled for Shared Calling dials out, the resource account number is displayed, and any inbound calls to that number are routed to the Auto Attendant for processing.

Shared calling users are still required to have a Teams Phone Standard license but may not require their own Calling Plan license. Shared calling is supported by Direct Routing and Operator Connect; however, calling capacity and concurrency still need to be considered, so there may be additional costs or overheads.

Shared [Call Routing Policies](#) are used to define and configure the groups who will share a number.

Unassigned Numbers - Organizations often have vanity phone numbers, which have a specific meaning to your organization, such as a previous sales queue number or an old main number. These are numbers not assigned to any auto attendant, call queue, or user, but you need them to be answered. Unassigned numbers in Teams can catch numbers not associated with a specific user or account and then redirect them to another user, resource account, or play an announcement. An additional scenario is when people leave your organization, and you may want to route the calls to reception for a few months. You can configure unassigned number ranges that cover large portions of your full range, numbers assigned to users, resource accounts, or conference bridges that are ignored and routed to their correct destination.

Unassigned numbers can be managed in either the Teams admin center ([under Voice, Phone numbers, Routing rules](#)) or through PowerShell with the `New-CsTeamsUnassignedNumberTreatment` cmdlet. The rules are evaluated in order and when a match happens the appropriate action is taken, and processing stops.

The rules use regex to find patterns in the incoming number, and they are evaluated in the order specified until a match happens. No subsequent rules are then processed. The builder in the Teams admin center has some default templates if you are not familiar with regex that cover:

- Numbers starting or ending with
- Phone number range
- Single number

You can also select Advanced to enter your own regex code. Once you have a regex filter to match, you can choose an appropriate routing option, which can either be:

- Greeting: Upload an audio file to play to the caller
- Forward to a person or account in the organization (should be Enterprise Voice enabled)
- Forward to the resource account for a voice application (see this section)

Be aware that if you route the call to a Calling Plan user, Communications Credits must be available in the tenant to pay for it. This does not apply for an Operator Connect or Direct Routing user.

Some good examples of configuring unassigned numbers in PowerShell are provided in the [Microsoft docs](#), and [some online services](#) build clear visual diagrams from your regex code so you can check that your matches look correct before applying any changes.

Blocking Numbers - Like the regular phone system, your users might receive calls from spammers or others offering dubious services. Users can block callers in the calling app in the Teams client, but it can be more effective to put an organization-wide block in place. This is configured using PowerShell by creating a block rule with the `New-CsInboundBlockedNumberPattern` cmdlet. As the name suggests, the block works by defining a number pattern for Teams to recognize inbound calls to block. The pattern can block a single number, a sequential range, or multiple separate numbers. For example, here's how to block a single number:

```
New-CsInboundBlockedNumberPattern -Name "Spam Block" -Enabled $True -Description "Blocks spammer from Tunisia offering Microsoft support services" -Pattern "\+21690373633"
```

After setting up a rule, you can test it using the [*Test-CsInboundBlockedNumberPattern*](#) cmdlet.

Managing User Calls

One of the primary benefits of deploying Teams Phone for users is that it gives them great flexibility in choosing how to manage their phone calls. The availability of these features is controlled through Teams calling policies, which are covered in the earlier section. These features are all included in the standard Teams Phone license.

Users can choose to forward their calls to other users or numbers in several different ways:

- **Call forwarding** sends the call straight to an alternative destination number or user.
- **Simultaneous ring** forks the call and rings both Teams and the destination number. Whichever endpoint answers first takes the call.
- **Call Groups** allow users to create a personal hunt group containing users they are working closely with who can receive the call on their behalf.
- **Delegation** for calling lets another user make or receive (subject to configuration) calls on the original user's behalf.

Forwarding notification: When a call is forwarded to another Teams user, the incoming call notification will include a visual indicator to tell the user that it has been forwarded from another source. Teams will not apply call forwarding settings from the destination user that would cause calls looping.

In this section, we will cover features that are relevant to the call flows of individual users:

- Call forwarding configuration
- Delegates
- Group Call Pickup
- Call Park

Business call flows are covered next under Voice Apps.

Configuring Call Forwarding options on behalf of Users - These settings can be updated through Teams admin center under **Manage Users**, select the user then in the **Voice** tab, or via the `Get-CsUserCallingSettings` cmdlet. As well as seeing the current configuration, you can update the timeouts before actions happen, for example, allowing calls to route to the user's Call Group after 20 seconds of trying the original user first. Forwarding can also be controlled in [PowerShell](#).

Call Delegation - [Call delegation](#) allows another user to make, take, and manage calling for someone else. Depending on the policy, users can change their delegate settings in the Teams client, or an administrator can do it via the Teams admin center or [PowerShell](#). Having users take responsibility for their calling behavior, including delegates, is recommended as the best practice. Delegates can be configured with different permissions, including making, receiving, or managing calls. Managing call capabilities includes adding more delegates for the original user, and both parties will have a shared view of their calling history.

A typical use for delegates is executives with personal assistants who must screen and handle calls on their behalf. Ideally, the executive can configure their first delegate in their Teams client by going to **Settings**, **Calls**, and **Manage delegates**.

Once the first delegate has been assigned, this user can configure any subsequent delegates needed. Alternatively, as executives do not usually want to handle setup tasks, you could use the Teams admin center to find the executive under **Users**, **Manage users**, and then add the first delegate in the **voice tab**.

There is a limit of 25 delegates or managers per user, and delegation assignments cannot be circular. There is, however, no limit to the number of delegation relationships in a tenant.

Group Call Pickup - Group call pickup lets users create small personal hunt groups of other user accounts that can be called if the original user is unavailable. Call groups can be configured in the Teams client by the end user, an administrator in the Teams admin center, or through PowerShell. A tenant can contain a maximum of 32,768 call groups.

If configuring it via the Teams client, the option will only display when selecting a call forwarding scenario. The configuration can be found under **Settings, Calls**, and then selecting **Call group**. In this selection, it is possible to choose which accounts are part of the personal call group, and how calls should ring to the group (one by one, or all together), [this documentation explains](#) how users can configure group call pickup themselves.

Call Park - Call Park (CP) is not strictly a user-calling action, as you cannot park calls automatically. However, it is important to know about the feature as it is crucial for some niche scenarios. Companies use call park where employees are hard to contact. Users (such as receptionists) can assist and connect the caller to the employee. When the call arrives, the receptionist (or any user) parks the call by using the "more actions" icon after first picking up the call. Teams generates a unique code that can then be given to the destination user. The target employee can then retrieve the call from a Teams client or device using the code provided. The user enters the code into the Teams client on the calling page by clicking on the **Unpark** button and entering the code.

Call Park is controlled via the call park policy assigned to user accounts. New call park policies are created using the `New-CsTeamsCallParkPolicy` cmdlet, or in the Teams admin center under **Voice, Call Park Policies**. Users must be covered by the same call park policy to be able to retrieve each other's calls, so standard practice is to have separate call park policies per site or region. Administrators assign policies to specific users using `Grant-CsTeamsCallParkPolicy`. If you want to remove the policy from a user, you still use the grant command but set the policy name to `$Null`. Here is how you create the policy and grant it to a user:

```
New-CsTeamsCallParkPolicy -Identity "SalesPolicy" -AllowCallPark $false  
Grant-CsTeamsCallParkPolicy -PolicyName SalesPolicy -Identity "ben.lee@office365itpros.com"  
Grant-CsTeamsCallParkPolicy -PolicyName $Null -Identity "ben.lee@office365itpros.com"
```

Policy-based Recording

As covered in the policy configuration options for calls and meetings, Teams supports "convenience" call recording (recording on-demand). However, some organizations may need to ensure that all calls for selected groups of users are recorded. This type of recording requirement is common in the financial sector.

Microsoft does not support this type of recording natively. However, an API and recording framework is available to allow third-party products to plug the gap. This functionality was initially called compliance recording, and some documentation refers to it in this way. As the integration works service-side, it supports capturing calls from any endpoints or devices where the recorded user is signed in.

All the different policy-based recording solutions capture the media streams from Teams the same way, using "hidden" meetings and Azure bot services. The system places the user and the destination party into the hidden meeting when a recorded user makes a call. An Azure Bot joins the meeting as a hidden participant. This meeting is not visible in the Teams client, so the call looks and feels the same as a non-recorded one to each party, other than a visual recording notification is present. The bot captures the media streams for the call and sends them to whatever back-end platform the recording solution uses for storage and further processing. The applied policy dictates if the recorded party sees a notification and what should happen if the Azure bot is unavailable. For example, if the recording requirement is legally mandated, you may need to prevent the call if recording is unavailable.

As each vendor records the media streams using the same method, they differentiate through how they process and store the recordings. Features include automatic sentiment analysis, transcription with search

capabilities, and automatic categorization, or application of retention/deletion policies based on the source and destination numbers.

The Teams clients can notify when recording is taking place, but it is also possible to enforce agreement from all parties before they can participate in a recorded meeting. This option is not available in the Teams admin center, but can be controlled through the [Teams Meeting Policy](#) PowerShell cmdlets. When enabling explicit consent, participants must confirm their agreement to recording or transcription if they unmute themselves, share content, or start their camera. This policy setting is not specific to policy-based recording and can apply to recording on demand too.

[Microsoft publishes](#) a list of vendors who have gone through the certification process.

Assigning App Permission Policies with PowerShell

The `Get-CsTeamsAppPermissionPolicy` cmdlet lists the Teams app permission policies available in the tenant. Use the `Grant-CsTeamsAppPermissionPolicy` to assign a policy to a user. For example:

```
Grant-CsTeamsAppPermissionPolicy -PolicyName "Unrestricted App Access" -Identity  
Kim.Akers@office365itpros.com
```

To assign an app permission policy to the members of a team, we need to retrieve the members of the team and then assign the policy. Here's how to do it using the `Get-Team` and `Get-TeamUser` cmdlets from the Teams PowerShell module followed by a call to `Grant-CsTeamsAppPermissionPolicy` to assign the policy to the individual members:

```
$HRGroup = Get-Team -DisplayName "Human Resources Group"  
$TeamUsers = Get-TeamUser -GroupId $HRGroup.GroupId -Role Member  
$TeamUsers | ForEach-Object { Grant-CsTeamsAppPermissionPolicy -PolicyName "HR App Policy" -Identity  
$_.User }
```

Assigning App Permission Policies with PowerShell

The `Get-CsTeamsAppPermissionPolicy` cmdlet lists the Teams app permission policies available in the tenant. Use the `Grant-CsTeamsAppPermissionPolicy` to assign a policy to a user. For example:

```
Grant-CsTeamsAppPermissionPolicy -PolicyName "Unrestricted App Access" -Identity  
Kim.Akers@office365itpros.com
```

To assign an app permission policy to the members of a team, we need to retrieve the members of the team and then assign the policy. Here's how to do it using the `Get-Team` and `Get-TeamUser` cmdlets from the Teams PowerShell module followed by a call to `Grant-CsTeamsAppPermissionPolicy` to assign the policy to the individual members:

```
$HRGroup = Get-Team -DisplayName "Human Resources Group"  
$TeamUsers = Get-TeamUser -GroupId $HRGroup.GroupId -Role Member  
$TeamUsers | ForEach-Object { Grant-CsTeamsAppPermissionPolicy -PolicyName "HR App Policy" -Identity  
$_.User }
```

Assigning App Permission Policies with PowerShell

The `Get-CsTeamsAppPermissionPolicy` cmdlet lists the Teams app permission policies available in the tenant. Use the `Grant-CsTeamsAppPermissionPolicy` to assign a policy to a user. For example:

```
Grant-CsTeamsAppPermissionPolicy -PolicyName "Unrestricted App Access" -Identity  
Kim.Akers@office365itpros.com
```

To assign an app permission policy to the members of a team, we need to retrieve the members of the team and then assign the policy. Here's how to do it using the `Get-Team` and `Get-TeamUser` cmdlets from the

Teams PowerShell module followed by a call to `Grant-CsTeamsAppPermissionPolicy` to assign the policy to the individual members:

```
$HRGroup = Get-Team -DisplayName "Human Resources Group"
$TeamUsers = Get-TeamUser -GroupId $HRGroup.GroupId -Role Member
$TeamUsers | ForEach-Object { Grant-CsTeamsAppPermissionPolicy -PolicyName "HR App Policy" -Identity $_.User }
```

Voice Apps

So far, we have covered scenarios for “individual calling” where calls are to/from specific users. However, it is very common for businesses to need to direct calls to groups of users, or have workflows associated with PSTN calls. For example, you can route calls among a support team or handle incoming calls to a main office number, where you might also need to take a message after business hours. Fortunately, Teams allows for these scenarios with two types of Voice Apps:

- **Auto attendants** let you define welcome messages, interactive menu choices, and program different behaviors based on opening hours.
- **Call queues** determine how calls are sent to different users (agents). You can define the group of agents, type of call distribution, and overflow options for calls in the queue. Call queues can be mandatory, where users are always in a queue when online, or you can allow opt-in and out so users can control their availability for receiving incoming calls.

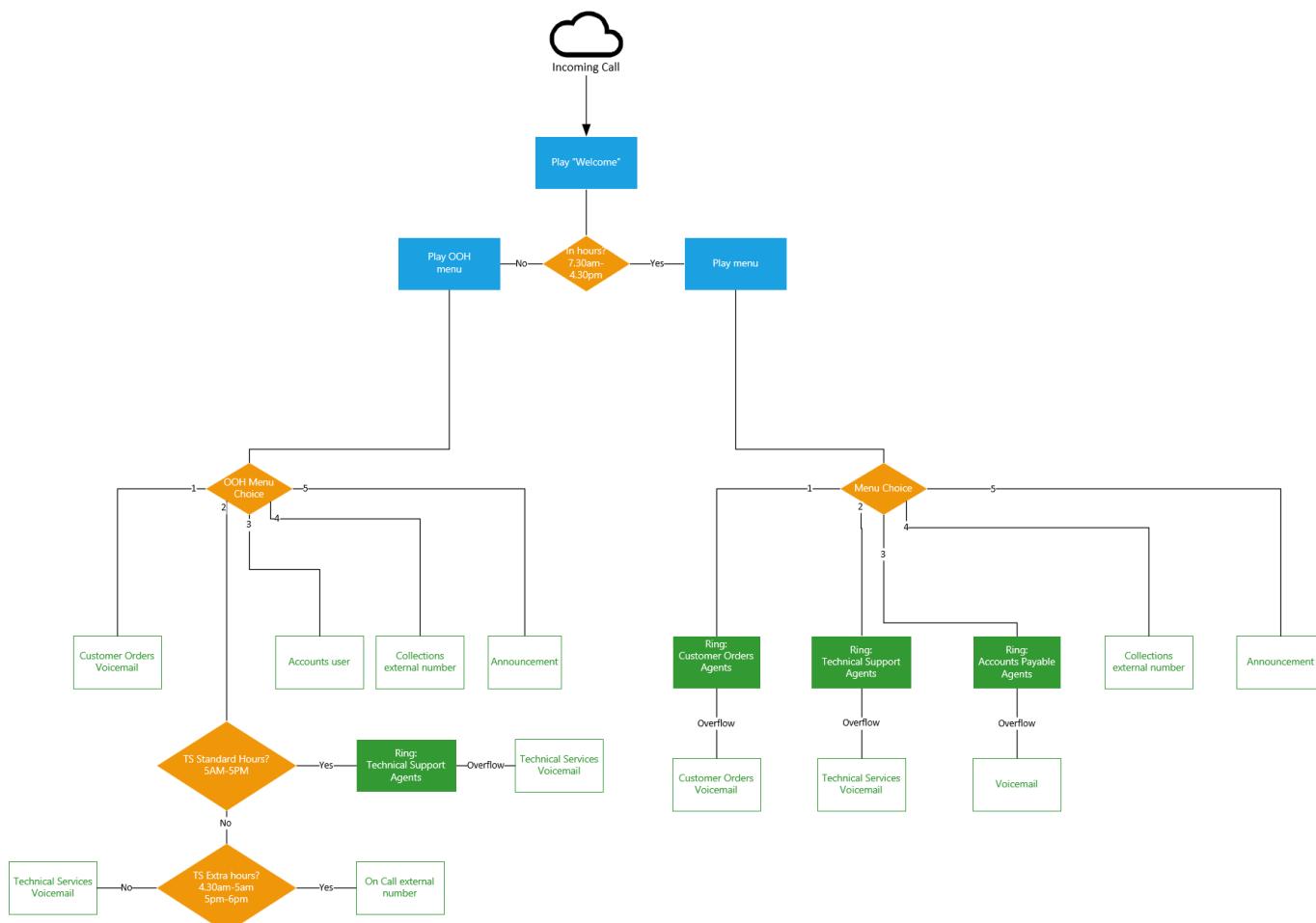


Figure 13-3: High Level Voice Apps diagram

All the features discussed under group-based calling require users and agents to be Enterprise Voice enabled, meaning they need to have a Phone System license and a number assigned through Calling Plans, Operator

Connect, or Direct Routing. If the tenant has Teams Phone Standard licenses, the functionality provided by auto attendants and call queues is essentially free.

It is common practice for organizations to combine auto attendants (which allow time-based routing and an options menu) with call queues to meet their calling workflow requirements. A typical main office reception number workflow can consist of:

- One auto attendant answers the inbound call, provides a greeting and presents an option of choices to direct the call.
- Multiple call queues are used to handle the directed call, such as Accounts or IT Support.
- Overflow queues to handle any calls that do not get answered in time.

When thinking about creating Voice apps it can help to produce a high-level flow diagram showing what behavior you are looking for, this can then serve as a template when building them. Figure 13-3 shows an example Auto Attendant flow, breaking out into separate call queues (green boxes) depending on the chosen menu option.

To help document Voice Apps, a good [third-party script](#) is available that can output a diagram showing how they are configured and interact.

Full Contact Center Solutions: APIs to build customized switchboards and call centers are available inside the Teams service, allowing third parties to extend Teams Phone capabilities into fully functional contact centers. Such solutions provide more advanced IVR functionalities and better reporting capabilities and are usually delivered through a customized interface. Microsoft also offer deep voice integrations into their Dynamics 365 Customer Service platform. Microsoft maintains a list of [supported third party vendors](#) and details its Dynamics integration [online](#).

Resource Accounts

Behind every voice app lies a resource account. The resource account is a disabled user account configured with the number used so Teams knows how to route incoming calls. The settings for resource accounts are located under **Voice** in the Teams admin center.

Resource accounts need a special kind of license called the Teams Phone Resource Account. This is a free license, and you can acquire 25 licenses with your tenant's first Phone System license. This allocation then increases by one for each ten Phone System licenses acquired. You can request the licenses from the Microsoft 365 admin center, from your CSP provider or as part of your Enterprise license Agreement.

Admins with the Teams Administrator role could create resource accounts, but a change ([due to complete in Q3 2024](#)) removes the ability to create these accounts with only that role. Resource Accounts will either need to be created by an account with a user admin role, or you need to add User Management permissions as a custom permission alongside the Teams management role.

To assign a number to the account you can use Teams admin center, or PowerShell. When assigning service numbers through the Teams admin center, you will only see those that match the usage location of the selected resource account, so remember to update this if you need to allocate numbers in different countries, refer to the Calling Configuration section above.

Here is a summary of the process of creating a resource account:

1. Obtain two or more service numbers as described earlier.
2. Obtain some free *Teams Phone Resource Account* license by going to the add-on licenses section in the Microsoft 365 Admin portal, under **Billing**, then **Purchase services**. Even though they are "free" licenses you must still provide valid billing details.

3. Create at least two Resource accounts under **Voice** in the Teams admin center and specify one as call queue and the other as auto attendant.
4. Assign the Teams Phone Resource Account to the resource accounts, preferably using Group Based licensing in the Entra admin center.
5. Assign a service phone number to the Resource accounts by going to the Teams admin center under **Voice**, then **Resource account**. Select the resource account you are working on and click **Assign/unassign**. Next, select the number you want to assign and click **Save**.
6. Create a call queue, assign a Resource account, assign agents, and choose the routing method.
7. Create an auto attendant with a welcome message and open hours. Assign a Resource account and route the auto attendant calls to the call queue that contains the agents.

Resource accounts can also be created in PowerShell using the `New-CsOnlineApplicationInstance` cmdlet. Give the resource account a name and define the type of service by setting the `ApplicationID` to define which service (AA or CQ) the resource account is to be used for. These IDs are the same across tenants as they reference the global Microsoft 365 IDs:

- **Auto attendant:** ce933385-9390-45d1-9512-c8d228074e07
- **Call queue:** 11cd3e2e-fccb-42ad-ad00-878b93575e07

```
New-CsOnlineApplicationInstance -UserPrincipalName "_service_TeamsRouting_CSDDR@office365itpros.com"  
-DisplayName "Service Desk" -ApplicationId "11cd3e2e-fccb-42ad-ad00-878b93575e07"
```

After assigning the account a Phone System Virtual User license, we can assign it a Service Number by using the `Set-CsPhoneNumberAssignment`. The `PhoneNumberType` defines the source as *CallingPlan*, *OperatorConnect* or *DirectRouting*:

```
Set-CsPhoneNumberAssignment -Identity "_service_TeamsRouting_CSDDR@office365itpros.com"  
-PhoneNumber +4714073200 -PhoneNumberType CallingPlan
```

Remember that you can mix and match calling delivery, so even if your users numbers come via Direct Routing, you can still take Service Numbers directly from Microsoft. This can be a good idea for some queues, like an internal support queue, where you would need it to be operational even if you have a fault with your infrastructure. After assigning a number to the resource account, you can then associate it with an auto attendant or call queue in the Teams admin center.

Call Queues

Call queues are simple hunt groups used to distribute incoming calls between different user accounts, called agents. Call queues have basic options to manage the flow of calls once a call is in the queue and are typically used in conjunction with auto attendants, which provide callers with a rich menu of choices. Each queue can handle 200 inbound calls and support 50 agents. Should you need to handle more, you can configure overflows and timeout behaviors to use multiple queues in the same workflow. The Teams mobile client supports call queues so users on the move can still take incoming calls; however, you should ensure they know how to update their presence correctly to avoid calls at inappropriate times.

To start building a queue, go to the Teams admin center under **Voice** and **Call queues** and select **+Add**. The following configuration sections are then available:

General Info – The first screen lets you name the queue and select what resource accounts will be associated with the queue. Remember that phone numbers are associated with the resource account and the resource account to the relevant voice app. You can also set up a resource account that an agent can use to make outbound calls. This lets a user hide their number and call as the queue. For example, if you want return calls to go to the mainline number instead of the agent. You can choose a different account here than the one

operating the queue. The language setting on this page is used later if you need to provide voicemail transcription services or to play a prompt to callers while they wait in the queue.

Greeting and Music – Used to configure options to play a greeting audio file (MP3, WAV, or WMA under 5mb) if required and what to play to the caller while the queue finds someone to answer their call. One trick here can be to find a royalty-free version of your country's ring-back tone and use it as the hold music so that callers know their call is continuing to ring.

Call Answering – This section dictates who will receive the inbound calls. Agents must have a Phone System license and have a phone number assigned to be selected.

Three ways exist to add agents to call queues. You can:

- Add users one by one.
- Add sets of users using a distribution list or Microsoft 365 Group.
- Enable collaborative calling by selecting a channel within a team.

Collaborative Calling adds a new tab in the chosen channel named Calls (not visible in the web client). Here users can see an overview of calls relating to the queue, and current active agents. In addition, they can see the call history, who answered calls, and what calls were sent to voicemail. When first configuring a channel for collaborative calling, it may take 24 hours for the Calls tab to be visible.

Conference mode is a setting that was introduced to speed up the time it takes to answer a call as an agent. The inbound call is held in a conference with audio established, so when an agent joins, they only need to add their audio instead of negotiating an end-to-end media path. Without conference mode, it can take longer for the agent to hear the audio of the inbound call.

Agent Selection – Dictates how calls are distributed among the eligible agents. The following routing methods are available:

- **Attendant** – sends the call to all agents at the same time.
- **Serial** – sends the calls in the published order each time.
- **Round-robin** – distributes the calls at random between the agents.
- **Longest idle** – sends the call to the agent who has had no call for the longest.

If you turn on presence-based routing, calls will only be presented to agents who have a status of Available.

The opt-out option allows users to voluntarily remove themselves from the pool of available agents at any given time. They can control this setting inside the Teams client under **Settings** then **Calls**, where toggle boxes will be visible for any configured queue.

The agent alert time dictates how long a call will attempt to ring a specific agent before moving on to the next one in the queue, which can be between 15 and 180 seconds.

Exception handling – This screen lets you choose what to happen to calls in three scenarios; when too many calls are already in the queue (overflow between 1-200 calls); when calls have waited too long (timeout between 15 seconds and 45 minutes); or there are no agents available to answer (new or existing calls).

Each of these scenarios allows you to either disconnect the call, let it wait (no agent only), or redirect it to:

- **Person in the organization** – a Phone System enabled user.
- **Voice app** – another call queue or auto attendant.
- **External phone number** – a PSTN number.
- **Voicemail (personal)** – a users voicemail.
- **Voicemail (shared)** – the voicemail for a Microsoft Group; this also provides options to skip the default mailbox greeting or to use a custom one.

Authorized Users – Allows the selection of standard user accounts that can manage certain aspects of the Call Queue. Currently, this supports changing greeting messages. Authorized users also need to have a Voice application policy applied to them that specifies what changes they are allowed to make (see Voice Application Policies).

Callback – [Several configuration options](#) are only managed through PowerShell. The most interesting of these is the ability to offer a callback to waiting callers when an agent is available. To become eligible for an offer of callback, there are three configurable criteria:

- **Time based** – The time spent on hold in the current queue (current callers).
- **Volume based** – When the number of waiting callers exceeds the configured value (new callers only).
- **Ratio based** – Configured agents vs waiting callers (new callers only).

In addition to meeting one of these criteria, the caller must also be from a valid E.164 number. The callback offer happens when the configured hold music has finished playing, and uses a customizable message. DTMF keys are then used to accept or decline by the caller. If any attempted call back fails, the system can email an alert to a specified email address.

With all the options and logical conditions at play in a call queue, it is vital to carry out thorough testing for all the key scenarios to ensure that call flow happens as expected. For example, if the queue timeout is two minutes, but the call back timeout is three minutes, or if the hold music lasts longer than three minutes, then a caller will never trigger the offer.

Call Reporting: Organizations that need to report on voice app answering performance and real-time call statistics may need to use third party solutions. This is an area where Microsoft is improving and as of October 2022, they [released](#) a new set of PowerBI reports along with a new data endpoint to improve reporting in this area.

Auto Attendants

The auto attendant is an automated interactive system for incoming calls that can generate welcome messages, give opening hours, provide interactive menu choices, and route calls to other auto attendants, call queues, and users directly. It also includes a voice-driven Directory Search to reach a person by name. Directory Search is a niche feature, but if you need it, be aware that the default configuration allows searching across the entire directory.

Configuration for auto attendants (and call queues), can be carried out via PowerShell, but it is a very disjointed and complicated process. Unless you have a good reason, such as bulk provisioning, it is best to stick with creating them via the Teams admin center. You can read more about the PowerShell capabilities in the [official docs](#).

To configure an auto attendant, go to the Teams admin center under **Voice**, find **Auto attendant**, and select **+Add**. The following configuration sections are then available:

General Info – Gives the auto attendant a name and allows the selection of an Operator. The operator can be a named person, another voice app, or an external number, or it is not required. Later options in the auto attendant will let you choose to route calls to the configured operator.

As auto attendants can be configured to operate differently during business hours or holidays, it is essential to ensure the time zone is correctly configured for the attendant.

The language setting determines which text-to-speech Microsoft engine will read out any prompts (if required) and what voice recognition engine is deployed to recognize caller requests.

Voice inputs can be used to control the call flow when building the options menu, and to search the directory if desired.

Call Flow – This section contains the primary options for how the auto attendant will handle calls. The greeting option controls what is played to callers when the auto attendant first picks up a call. This can either be a custom audio file, or you can enter text that the system will read out to callers using the previously selected language.

Call routing options are where you can redirect a call straight to another destination or build a menu of interactive choices allowing callers to select where their call is routed. If selected, the menu has its own greeting that can again be a custom upload or use text-to-speech services. The menu greeting is separate from the primary queue greeting, so you do not have to re-record the whole greeting if any options change or if you want different behaviors based on the time of day.

A menu can contain 12 options (if voice prompt enabled) or 10 if relying on the caller to press dial keys. Each item in the menu can redirect a call to:

- **Operator** – Whatever was selected on the previous configuration screen for the operator.
- **Person in organization** – Select a Teams Phone enabled user in the directory.
- **Voice app** – Another auto attendant or call queue.
- **Voicemail** – Voicemail of a Microsoft Group.
- **External phone number** – A standard PSTN based number.
- **Announcement** – Upload a custom audio file to be played to callers.
- **Announcement** – Read a message using the text-to-speech translation engine.

Directory search allows callers to search for internal users to call directly using either a search on their name or phone extension. This can be restricted using settings on one of the next screens.

Call flow for after hours – The current behavior is configured for when the business is open. Here you can define business operating hours broken down into 15-minute increments over all 7 days of the week. You can then define a second behavior with options similar to those on the previous Call flow screen for what happens to incoming calls outside these hours, or build a whole new menu of choices.

Call flows during holidays – Auto attendants can also operate differently during business holidays. Holidays are managed centrally across all auto attendants, in the Teams admin center under **Voice** settings and **Holidays**. Here you can define a set of holidays and assign them to multiple auto attendants. Adding holidays for a country programmatically [is possible](#), or you can update them across the whole tenant via a CSV. You can also create holidays directly inside the auto attendant builder, but it is easier to create them separately. When selecting a holiday that the auto attendant will observe, you can then also configure the call handling behavior in the same way as the out-of-hours options.

Dial Scope – If using voice search to let callers find users you can use include and exclude filters to narrow down the list of available users. For example, it might be sensible to exclude your C-level executives if external users can dial the auto attendant and search the directory. The search scope obeys the Exchange Online attribute “HiddenFromAddressListsEnabled” to align with other services.

Resource Accounts – Next, define the resource accounts used to handle the calls for the auto attendant.

Authorized Users – Lastly, this allows the selection of standard user accounts who can manage certain aspects of the Auto Attendant. It also requires a Voice application policy (see below).

Voice Application Policies

Voice Apps have a subset of delegated management options, and each call queue or auto attendant can have authorized users configured who are allowed to update relevant configuration items. Authorized users must be Enterprise Voice enabled (the term used for a user who has Teams Phone fully configured and a number allocated), they also need to have a Voice application policy that specifies what features they can configure for any Voice App they are given access to.

These policies are in the Teams admin center under **Voice** then **Voice application policies** and follow the same global/user behavior as most other policies. Options available for configuration include most greeting and music-on-hold options, and Teams Premium will allow changes to call forwarding settings and destinations.

When a user has a valid Voice application policy and is an authorized user of a voice app, they can update settings via their Teams client, under the **Settings** and then **Calls** menu.

Teams Devices

Teams supports a rich ecosystem of third-party devices where manufacturers have produced compatible devices that are then certified for use with Teams by Microsoft. Earlier, we discussed how to prepare a network to ensure you can make good calls, but a significant and often underestimated factor in the overall call quality is the device you are using. If you put bad audio or video into Teams, you will only get poor quality out of the other side. Audio quality can significantly impact the overall perception of the quality of experience.

It is not uncommon to get support cases where users complain about poor call quality in a meeting, only to find that their call streams were all good, but it was someone else broadcasting bad audio into the call (or picking up the conversations of everyone else nearby).

The Microsoft Teams device certification program not only guarantees a minimum level of quality for the key components of the device, but also means that all the expected functionality works. This includes proper mute/unmute synchronization between the device and your Teams client or answering a call directly from the device by pressing a button if your PC is locked.

Device Types

Traditionally, devices were split into two broad categories:

- **Personal Devices** are devices designed for use by a single person and typically refer to headsets, webcams, or individual phones.
- **Shared Devices** refer to equipment that more than one person uses, such as hardware in a meeting room or a phone in a communal workspace.

In the last few years, Microsoft has introduced several newer categories of devices, such as Teams Displays and Teams Panels, which blur these lines. There has also been a push to expand cross-device compatibility by introducing services like the SIP gateway. For this reason, phones and similar devices have been moved into a dedicated category called Phone Devices later in this chapter. You can either jump straight to or skip over that section, depending on where you are in your Teams Journey.

You can find a complete list of the currently certified devices & device categories in the [Teams Enabled Devices catalog](#).

Personal Devices

Personal devices typically refer to devices owned by or signed in as one user. It is an important category as your users will most frequently use these devices. Having a company strategy or approach towards personal devices is essential, as allowing people to use their own devices can be tempting. While these may work, generic devices like AirPods do not provide the best overall experience for everyone on the call, so let's explore this category.

Headsets and Webcams - The Teams client will accept the video feed from any USB camera the underlying Operating System can access. The main consideration with webcams should be whether you want to give laptop users an external camera. If you want to drive the use of "video first" meetings, you may find that

relying on the webcam in laptop lids doesn't provide the best quality video (or the most flattering up-nose shots).

For headsets, there are some specific benefits to having a certified device:

- Dedicated Teams button and LED indicator light. The button will activate the Teams client and perform context-sensitive actions such as answering calls, joining meetings or raising your virtual hand.
- Automatic selection as the default audio device in Teams. Removing some of the user friction and guesswork when selecting devices.
- Call control sync between the headset and Teams. Mute / unmute on the device synchronizes with the view in the Teams client.
- Extensibility and future compatibility. New device/client features can be delivered via firmware update.
- Minimum level of audio quality guaranteed. Testing audio quality to reduce things like echo or excessive glitches, echo cancellation across devices, wideband audio support, and comfort noise support.

[Microsoft lists](#) some benefits of using certified Teams devices, and you can read the [full specification](#) for certification for all Teams devices online.

Bluetooth headsets - The Teams desktop client keeps adding improvements to minimize audio issues, such as background noise suppression, but these do not negate the need for certified devices. You still get the best overall experience with certified kit.

Certified Bluetooth headsets usually include dongles to connect to the computer. This is because standard Bluetooth connectors in laptops are designed to support peripherals such as mice and keyboards, not high throughput audio or advanced HID functionality. Microsoft is also making changes here, such as supporting headset button presses without the dongle, but using one is still recommended to get the best audio performance when possible.

Ringer options: If you use different headsets for Teams calls and listening to music, you can use the secondary ringer option to control where incoming calls alert. You can define the device where you want to hear incoming calls. This setting is found in the Teams desktop client under **Settings**, and then **Devices**.

Most vendors have management tools you can use to centrally manage firmware upgrades and push configuration to their devices, such as [Jabra Direct](#) and [EPOS Manager](#).

To find what headsets are being used across the organization, you can query the Call Quality Dashboard (CQD) using PowerBI (covered in the Call Quality Dashboard section), but poorly defined device names can make this challenging.

Teams Displays - Teams displays are a newer category of device designed to act as an all-in-one touch screen device providing access to chat, channel conversations, switching tenants, meetings, making and receiving calls, and recent activity notifications. Originally intended as an extension of the Teams client on your computer, they now offer an excellent stand-alone experience with support for hotdesking (which supports logging in via QR code). When connected to your computer, they become available as a speakerphone. When connected to your computer, it acts as a speakerphone but can operate independently.

While these devices may not seem to have an obvious use case, they can prove popular in small offices or spaces where an executive spends lots of time in Teams meetings – perfect for that corner meeting space. However, they are unlikely to go down well in open office spaces as they are hands-free and would generate lots of noise when used as a speakerphone.

From a management perspective, they benefit from the same management capabilities as the other dedicated Teams hardware devices we will cover next. In the Teams admin center, you can find them listed under the **Teams displays** tab under **Devices**. You can create and assign the same configuration profiles as with IP phones and control settings such as time zone and language. Microsoft maintains a list of all [certified Teams displays](#), and a good list of the [latest features](#).

Meeting Room Devices

Meeting room devices are the collective term for hardware in a shared space where people work together. These can vary in size and type from very large board room type spaces to smaller fluid huddle rooms or pods. When looking at what hardware to put in your meeting room, you should consider its primary purpose; will it be used for just voice/video calls? Will it allow casual collaboration via whiteboards? Does the space need to flex to grow or shrink in size as rooms are combined? These considerations can be accommodated through different Teams hardware solutions and so should be included in any requirements gathering.

Meeting room hardware is an area experiencing a lot of growth with a robust ecosystem of partners driving innovation in both hardware capabilities and software functionality. Some features do not require the equipment to be in a Teams meeting, such as allowing walk-up whiteboards and [local screen casting](#) without the need for cables.

Several categories of meeting room devices exist and are covered below:

- Phones
- Teams Panels
- Teams Rooms on Windows
- Teams Rooms on Android
- Surface Hubs
- BYOD Rooms

Phones - We will cover phones in more detail in the next section, but it is worth mentioning here that the most basic type of meeting room device is a phone or speaker phone. Teams phones come in many shapes and sizes, even one that matches the traditional "spider phone" device that you may have seen in many standard meeting room layouts. Teams phones have a unique display mode better suited for use in a meeting room. More on this and their modes later.

Teams Panels - Teams Panels are Microsoft's solution to the growing requirement for status displays outside meeting rooms. They display the status of a room and show future meetings and availability. In addition, the panels allow users to search for an available meeting room and make an ad-hoc booking via the panel.

Panels support advanced scenarios such as meeting room check-in, where a user taps the panel or scans a QR code as they enter the room to acknowledge that they are using the booked meeting. If the room is not used after a predetermined length, the booking can be removed from the room and made available for someone else to use without worrying about clashes. Also, if a room is currently free, you can use the panel to book an ad-hoc meeting to claim the space as your own.

Teams panels are Android-based devices that can be managed in the Teams admin center under **Devices**. No extra user account or license is necessary for Teams panels as they are normally logged in with the same user as the Teams Room or Surface Hub devices already in the room. A list of all [certified Teams panels](#) is available from Microsoft, along with [planning considerations](#).

Teams Rooms on Windows - Microsoft Teams Rooms on Windows (MTRoW – yes, it's a mouthful), are a premium in-room solution for joining Teams meetings. Sitting at the heart of each room setup is a Windows 11 PC connected to the other devices in the room (cameras, screens, microphones, etc.). The system is controlled through a touch panel running a full-screen version of the Teams interface.

Many kinds of MTRoW devices are available from vendors and many different camera and microphone configurations to suit various scenarios. Some vendors also add customizations or integrations to the devices. Crestron, for example, supports managing other in-room devices (like raising or lowering projector screens or dimming lighting) from the MTRoW touch panel.

With a feature called Direct Guest Join, Teams Rooms can join meetings hosted natively in Cisco Webex or Zoom using WebRTC based technology. Users might be invited to meetings at other companies that use a different technology stack, and this capability lets them use meeting room equipment for a higher-quality experience.

Teams Rooms on Android - Microsoft Teams Rooms on Android (MTRoA) started out as Collaboration Bars. They were intended to be lower-specification meeting room hardware for smaller spaces where an investment in MTRoW wasn't worthwhile. As time has passed, the hardware and software capabilities of the MTRoA devices have caught up somewhat with their larger MTRoW siblings. In some companies, they are becoming the preferred hardware choice, as Android-based can be easier to manage and have (in theory) a smaller attack surface area. If an MTRoA device develops a fault and needs to be factory reset, these appliance-like devices are easier to restore than something running a full Windows OS. There are some features that MTRoA does not have. However, if you look at the latest [comparison list](#), you will see that the gap isn't that large. The major features currently missing from MTRoA are:

- Coordinated meeting join, where separate meeting room devices can be combined into the same meeting.
- Peripheral health management reporting in the Teams admin center.
- Intelligent capture features.
- Intelligent capture features.
 - Intelligent cameras (IntelliFrame) allow multiple camera streams for a single device with smart person tracking and framing.
 - Intelligent speakers – Allow the transcript to attribute words to individuals in the room if they have a voice profile. This is increasingly useful with the rise of Copilot driven meeting recap features.
 - Content cameras – Cameras to support the inclusion of traditional whiteboards into a meeting and allow remote participants to join in whiteboard usage.

The MTRoA appliance approach outweighs the slightly feature-rich MTRoW experience for most companies looking to deploy meeting room devices, but there is no right or wrong answer

Surface Hub - The Surface Hub is Microsoft's own variant of meeting room hardware. It is a 55" or 84" touch and pen-enabled screen suitable for use as a giant digital whiteboard. Originally the Surface Hub could run other Windows "modern applications" such as maps or a browser, operating almost like a large tablet at the front of the room. Some models of the Surface Hub can be mounted on a wheeled stand with a battery allowing them to be moved about freely, although your mileage may vary depending on your office layout.

You can also configure a Surface Hub and a MTRoW to work in tandem with each other. For example, the Surface Hub provides digital whiteboarding for meetings and an MTRoW device provides the voice and video streams.

Starting in December 2023 with MTRoW software 4.19 Microsoft started to transition Surface Hub 2S devices into standard MTRoW devices, removing the ability to run other applications, but bringing them in line from a feature parity for meetings. It is not expected that older Surface Hub devices will be converted, and will continue to operate until their end of serviceable life which is currently scheduled for [October 2025](#).

BYOD Rooms - Microsoft is beginning to support Teams in Bring Your Own Device (BYOD) spaces; these are areas where a user brings their laptop into a space and connects it to a large screen and associated

peripherals such as microphones, speakers, and cameras are made available on the computer. The challenge with these spaces is delivering a consistent experience to users. Vendor solutions such as Logitech's Swytch have tried to cater to this scenario previously, but Teams administrators have been unable to track usage. BYOD support brings visibility of these spaces to the Pro Management Portal, where the same collection of peripherals is seen consistently connected to different devices. From Microsoft's perspective, providing reporting on BYOD usage can help drive deployments for full MTR devices when usage hits certain criteria.

Teams Meeting Room Licensing

Microsoft Teams Rooms have their own special licenses available that bundle together all the sub-licenses you need by the room to operate. In September 2022 Microsoft significantly revised how they license MTR devices.

If you already have existing MTR licensing (Microsoft Teams Rooms Standard or Microsoft Teams Rooms Premium) in your tenant, you can continue to use them for the duration of your current licensing term. After that you must swap to the newer licensing model. Table 13-1 compares the available licenses.

	Teams Rooms Standard	Teams Rooms Premium	Teams Rooms Basic	Teams Rooms Pro
RRP (per month)	\$15	\$50	\$0	\$40
Availability	Legacy Plan	Legacy Plan	From Sept 2022	From Sept 2022
Included Licenses:				
Microsoft Teams	Y	Y	Y	Y
Audio Conferencing	Y	Y	Y	Y
Whiteboard	Y	Y	Y	Y
Teams Phone Standard	Y	Y		Y
Microsoft Intune	Y	Y		Y
Entra ID P1	Y	Y		Y
Skype for Business Plan 2	Y	Y		Y
"Intelligent" monitoring		Y		Y
Proactive support on issues		Y		
Other functionality			Limited	
Maximum available in tenant	unlimited	unlimited	25	unlimited

Table 13-1: Teams Rooms licensing comparison

A tenant can use a maximum of 25 MTR Basic licenses. Any MTR devices above this number must use an MTR Pro license. If you have some MTRs deployed with the legacy standard license, you should budget to migrating them to the MTR Pro license at renewal time if you want to maintain existing functionality. Since the end of September 2023 Microsoft has actively blocked signing into an MTR device using accounts not licensed with a Teams Room specific SKU.

Microsoft did not differentiate features available with different licenses under the previous model, but with the Basic and Pro licensing, some Teams functionality is only available with a paid Pro license. Table 13-2: Teams Rooms Pro key feature list. Table 13-2 lists some of the key Teams Rooms Pro differentiators.

Feature name	Description / Notes
Dual screen support	

Different screen layouts	Together mode, large gallery & Front Row.
Content camera	Physical analogue whiteboard support via dedicated camera stream.
Teams Phone	Ability to make or receive calls via PSTN.
Intelligent audio / camera features	Multiple camera support, panorama support, people counting, use of intelligent speakers for speaker ID.
Cloud IntelliFrame	Adds support for individual faces to be identified and "broken out" into their own video stream from a single camera in the room.
Entra Conditional Access	Support for enhanced account security protections.
One-Time password sign in (OTP)	Support for passcode based sign-in during the first boot setup of the devices.
AutoPilot deployment (with Autologin)	Ability to automatically deploy MTRoW devices using AutoPilot and configure automatic account login.

Table 13-2: Teams Rooms Pro key feature list

A full feature comparison of the licenses is [available online](#). The feature gap between the licenses will likely increase as Microsoft adds more features to the platform.

Licensing status: In the Teams Devices section of the Teams admin center, the device list shows what license is assigned to each device and any warnings or notifications about license validity or feature set issues.

Phone Devices

Teams supports several different types of phones, but only one category offers native support, the others operate through compatibility gateways. For legacy devices, check the SIP Gateway for supportability and, verify it supports the features you need. If you have no existing phones that are compatible with Teams, then you should only consider deploying native Phones for Teams as they provide the fullest user experience.

This section covers the two types of devices, along with licensing for shared phones:

- Phones
- SIP Gateway
- Teams Shared Device License

Phones for Teams (Teams Phone) – Microsoft has had hardware phones compatible with their platform for many years. The way those devices are built and operated has changed over the years. For Teams, Microsoft reset the phone delivery model and now allows manufacturers to produce their own specification hardware, but they must run a version of the Android OS. Microsoft then provides a variant of the Teams client to run on them. This way, manufacturers can keep up with current specifications, but Microsoft controls the application and the UI, providing users with a clear and consistent interface across different device types.

Features found on Teams IP Phones include:

- Native Teams experience with hardware button integration and LED notifications.
- Calendar integration and one-touch meeting join.
- Support for touchscreens.

As mentioned in the previous section, these devices can run in three modes depending on your requirements:

- User mode, with a focus on contacts, calendar, and voicemail.

- Meeting mode, with a focus on the calendar.
- Common Area phone mode provides quick access to just a dial pad.

It is easy for a user to set up a Teams Phone. Enter your email address, type your password, and answer the two-factor authentication challenge, and you are in! The phone inherits the same capabilities you have as a user, so if you have the Phone System license, you get the same capability when you are signed in with the device. For other scenarios, there is a **Teams Shared Device License** (see below).

SIP Gateway - The SIP gateway is a Microsoft 365 cloud service where specific compatible devices can be SIP registered against the Teams service. These phones download a firmware version provided by Microsoft that supports their registration to the gateway. They connect using the SIP protocol to the gateway to make and receive calls. Other supported features include hold, resume, mute, unmute, and perform call transfers. A presence indicator is not shown on the device, but the presence will update for other users in the Teams client.

The SIP Gateway gives options to re-use existing devices (subject to compatibility) or deploy lower-cost devices in locations where full-blown Teams functionality is not required. It has also allowed device manufacturers to cater to voice scenarios that native Teams Phones are not able to, such as:

- **DECT handsets:** manufacturers such as Spectralink, Ascom, and Poly produce DECT handsets and base stations that can be registered through the gateway as Teams users.
- **Analogue Telephony Adaptors (ATAs):** Cisco, AudioCodes, and Poly have ATAs that allow traditional analog endpoints to call via Teams.
- **Intercoms, Pagers, and speakers:** Algo has added SIP Gateway compatibility to some of their specialist voice equipment, allowing Teams integration with intercoms and announcement/paging devices.

When signing via the SIP Gateway, the option for "SIP devices can be used for calls" must be enabled for the user account's Calling Policy. This is not enabled by default. This setting controls access to the gateway as you are unlikely to want all user accounts to be able to sign in devices this way.

Microsoft maintains a [complete list](#) of compatible devices, including DECT handsets.

Fax: ATA support for analog devices does not include support for FAX devices. FAX should be catered for using alternative solutions such as 3rd party internet FAX services or dedicated external lines where possible. In some cases, businesses find forwarding fax numbers via a user account works, but this is not a supported solution.

Teams Shared Device License - Teams phones do not require a license for the hardware itself. They are covered by the license assigned to the user account they sign in with. However, you sometimes need to deploy devices not associated with specific users, such as in shared areas like canteens, reception waiting areas, or factory floors. You could create specific service-style accounts and allocate them full E3 or E5 licenses, but this isn't a very cost-effective solution.

The Teams Shared Device license is available for such scenarios and includes the following sub-licenses:

- Microsoft Teams.
- Teams Phone Standard.
- Microsoft Intune.
- Entra ID P1.
- Exchange Online Plan 2 (Cloud voicemail only).

The standard Android Teams client can also use the shared device license, unlocking functionality that Teams Phones in Common Area Mode cannot support, such as walkie-talkie and participating in Voice App queues. Using the standard Android client in this way can help meet more specialized telephony use cases, such as

needing Wi-Fi phone coverage in a warehouse. Numerous generic ruggedized Android devices are available in the market that, combined with this license, would be more than suitable.

When a Teams Phone signs in using an account with the Teams Shared Device License, the phone only supports the Common Area Phone screen layout and cannot function in personal or meeting modes. This license unlocks some unique functionality, such as a hotline, that restricts calling to only a specific number.

Common Area Phone License: Before November 2022, Microsoft called this license the Common Area Phone license. Microsoft rebranded the name to reflect better the intended uses that support scenarios beyond shared access phones. You may see this still referenced in documentation and articles.

Device Management and Security

Teams device management is evolving quickly, more options are becoming available directly in the Teams admin center, and the newer Pro Management Portal, making common tasks much simpler. For example, you can now remotely provision Common Area IP Phones, check the health status of MTRs, and receive alerts about status issues. However, a downside to these improved admin capabilities is that some features are only available via the Teams admin center and not via PowerShell or Graph API where they could be automated.

Most of the devices we have talked about run either Windows or a variant of Android and are capable of being included in any Intune management of your estate (subject to the right licensing). However, you would not normally want to apply the same policies as you do for standard user devices. The challenge is that they are Android based but not a mobile phone, or Windows based but not a PC. Policies in Intune or conditional access can block access, rendering the devices useless. Here are the steps you should take to cater for these devices.

Teams Pro Management Portal

Running meeting room solutions can be an administratively intensive task as users can plug and unplug devices or hardware can break with little warning. They are also often spaces that see a high volume of activity and users need to be able to rely on the devices working all the time. The [Teams Pro Management Portal](#) is a reworking of the device management experience from Microsoft as the native capabilities in Teams admin center are not always able to meet these demands.

The Pro Management Portal is available to tenants for managing devices that have the Teams Rooms Pro license. It is a richer management experience for Windows based devices, although support for Android hardware (MTRoA, Displays, Phones) is starting to become available and be integrated.

The capabilities available in Teams Pro Management portal can be broken down into the following areas:

- Solution monitoring – Providing better insights into the operational status of a room, including all required peripherals like microphones and speakers
- Solution remediation – Integrations to service desk tooling (ServiceNow) to help with fixing rooms when something has broken
- Solution planning – Creating standards that rooms of rooms by type to help with keeping the experience consistent across the organization
- Update management – Better controls for updating and dealing with the software lifecycle of meeting room equipment
- More granular access controls – A different set of RBAC controls aimed at allowing sites to better manage their own pool of devices.

Managing Meeting Room Devices

Meeting room devices (or other shared hardware) such as Conference Phones, MTRoA, MTRoW and Surface Hubs are typically used in open shared areas, so we need to ensure they are properly configured.

For example, you might consider not allowing these devices to make calls to international numbers. If using Calling Plans, this is easy, assign them a Domestic only Calling Plan and do not assign communication credits. However, if you are using Direct Routing, you must create an *OnlineVoiceRouting* policy per country for CAPs and MTRs. Below is an example for the Netherlands which enables dialing only to numbers starting with the correct country code.

```
New-CsOnlineVoiceRoute -Identity "NL-Amsterdam-NationalOnly" -NumberPattern "^\\+31\\d{3,14}$" -
OnlinePstnGatewayList @{}{add="SBCSite1.office365itpros.com"} -Priority 1
-OnlinePstnUsages @{}{Add="NL-Amsterdam-NationalOnly"} -Description "For CAP and MTR will be able to
call Netherlands numbers except premium numbers and international numbers"
```

You might also consider blocking premium numbers for these shared devices. A great [third-party resource](#) has data for premium numbers for more than 200 countries. You can use this information to create PSTN Usages and Voice Routes which restricts the use of premium numbers available for shared devices (or users).

This section covers configurations common to meeting room devices, including:

- Creating Resource Accounts for MTRs (Windows or Android)
- Managing Teams Rooms in Teams admin center
- Managing Surface Hubs
- Intune and Conditional Access for MTRoW and Surface Hubs
- Remote Provisioning for Teams Android Dev
- MTR Notification and Alerts

Creating Resource Accounts for MTRs - Configuring accounts for devices can be complicated, as there are many different elements to check, especially if you are running hybrid identity or hybrid Exchange. Microsoft has a good [starter article](#) for helping plan MTR accounts. Typically, when introducing a Teams component to a meeting room, you want to enable the existing Exchange meeting room resource account for Teams. Here is a checklist when configuring meeting room accounts:

- Make sure the network is ready with proxy exceptions and firewall configuration. These are the same as the Teams client on a PC.
- Create an Intune enrollment token, so that all MTRs are enrolled in Intune.
- Create conditional access rules for MTR accounts to avoid requiring MFA.
- Assign Teams Rooms license to the synced user.
- Change UPN to have a common prefix, such as MTR.
- Enable the Exchange meeting room account for sign in and give it a unique password that never expires. Do this from Active Directory in a hybrid deployment or through Entra ID if it is a cloud-only account. Migrate user to exchange online if part of a hybrid environment.
- It is usually enough to assign the Teams license to enable the room for Teams. If you have a hybrid SfB deployment, then you must migrate the account to Teams. If the resource account was not originally enabled for SfB and hosted on-premises in Exchange, consider enabling it as an online meeting room in the SfB deployment so that all attributes are configured correctly since this is a synced account. Run the below cmdlet from the SfB PowerShell module from one of the SfB Front Ends:

```
Enable-CsMeetingRoom -Identity "username@domain.com" -SipAddressType "EmailAddress"
-HostingProviderProxyFqdn "sipfed.online.lync.com"
```

- After the MTR is set up and Intune enrolled, evaluate changing the admin account password after deployment, as this password is the same for all MTRs by default. This [YouTube video](#) shows how to change the password.

When reusing an existing Exchange room resource account, you need to ensure calendar processing is configured correctly to work for MTR meeting invitations. It is important that the settings *DeleteComments*

and *DeleteSubject* are set to \$False, otherwise the join button for the meeting may not show up on the MTR. By using Exchange Online PowerShell, you can check this with the following cmdlet:

```
Get-CalendarProcessing -Identity mtr-room1@office365itpros.com | Format-List AutomateProcessing,
AddOrganizerToSubject, AllowConflicts, RemovePrivateProperty, DeleteComments, DeleteSubject,
AddAdditionalResponse, AdditionalResponse

AutomateProcessing          : AutoAccept
AddOrganizerToSubject       : False
AllowConflicts              : True
RemovePrivateProperty       : False
DeleteComments              : False
DeleteSubject               : False
AddAdditionalResponse       : True
AdditionalResponse          : This room has Teams enabled room equipment for up to 10 people
```

You can use a string stored in the *AdditionalResponse* property to tell users that this meeting room has Teams Room equipment installed. A common misconception is that it should be possible to forward external Teams meetings to the Teams Room account. This does not work by default and the reason is that *ProcessExternalMeetingMessages* is set to false. To fix this, *ProcessExternalMeetingMessages* needs to be set to true, which enables anyone to send meeting invitations to the room. To enable the feature, run the following cmdlet:

```
Set-CalendarProcessing -Identity mtr-room1@office365itpros.com -ProcessExternalMeetingMessages $True
```

In addition, you may see that the forwarded meeting invitation arrives at the MTR, but there is no join button. This could be because of the way that Microsoft Defender for Office 365 safe link processing works. You need to create an exception for your mtr-* devices and not rewrite https://teams.microsoft.com/* links. When this exception is in place, a forwarded meeting will arrive at the MTR with a working meeting join link. If you use Direct Guest Join with the MTRoW, add Zoom and Webex meeting links to the allow list.

MTR Security: A Microsoft article is available about [MTR security](#), covering hardware, software, account, and network security. The text is updated regularly.

Managing Teams Rooms in Teams admin center - MTRoW shows up under **Teams devices, Teams Rooms on Windows** in the [Teams admin center](#), while MTRoA show up under **Teams Rooms on Android**. From there, you will be able to see the health of the devices, peripherals connected, call activity, and management history of your MTRs. A typical scenario is to discover when a peripheral is disconnected or what software version the device uses.

You can interact with the device by gathering device logs and restarting the MTR, be careful though as it will restart even if in a call. You can also control most of the settings you find in *SkypeSettings.xml* (a file used during manual deployment of the devices) such as **Account, Meetings, Device, Peripherals, and Theming**. For instance, you can enable modern authentication under **Account**, turn on proximity join via Bluetooth beaconing under **Device** (beaconing is also required to let screen casting to the device work), and set the current theme under **Theming**. The custom theme still requires an upload of the image file to the device as a separate process.

The Teams admin center displays MTRoW status under **Teams Devices, Teams Rooms on Windows** where administrators can view the health of their devices. If you select a device (Figure 13-4), you can see the status of individual components that make up the MTRoW. You can use the [...] menu for each device and mark it as non-urgent, no-impact, critical or reset to default. In this example, you can see that the unit is aware that it has no screen attached so the overall health of the room is marked as critical.

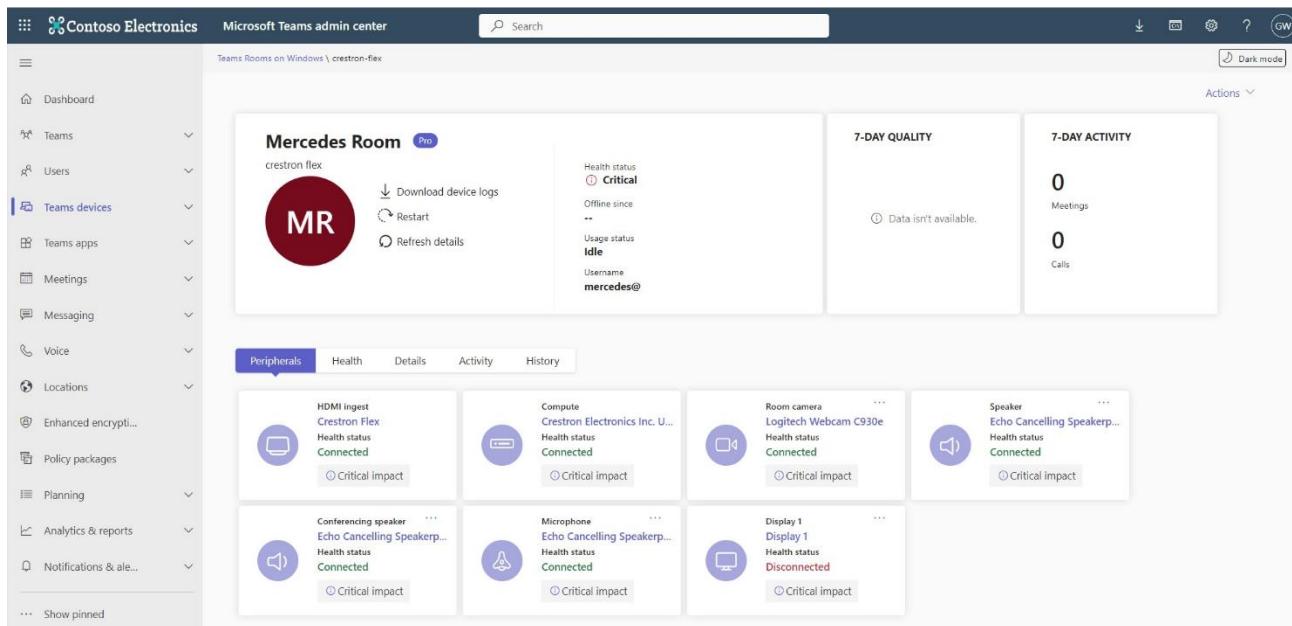


Figure 13-4: MTR management in the Teams admin center

MTRoW daily reboot: MTRoW devices reboot nightly at 2am local time. During the automatic reboot process, the device checks for updates installs any if available, and performs necessary maintenance. Microsoft wrote a [detailed article](#) about the difference between the quarterly updated Teams Room UWP application, pushed via the Windows store, and the Teams web app component, which updates at a higher interval with new features.

Managing Surface Hubs - In the Teams admin center under Teams devices, then Surface Hubs, you can see the inventory of hubs signed into your tenant (that have not transitioned to MTRoW devices). You can see the software version and network connectivity and if the devices run the latest software version. If a device is connected correctly, it is marked as healthy. Unfortunately, you cannot publish any settings to the devices, but you can restart them and collect device logs for troubleshooting.

Intune and Conditional Access for MTRoW and Surface Hubs - Teams is a cloud-only service, so it does not make sense to administer MTRoW devices with legacy on-premises techniques such as Group Policy. As such, there is little need to enroll them in Active Directory; instead, use modern management platforms such as Intune. When approaching managing these devices, consider the following points:

- **The account should have a UPN prefix such as MTR-xxxx to allow you to** create a dynamic group for all room accounts. Existing meeting room accounts can have their UPN updated as the display name will be what users see and can remain the same.
- **Conditional access policy:** Exclude the group you made above from MFA but restrict logon locations to trusted public IP address.
- **Compliance policy:** Create a Windows based compliance policy for Teams Rooms that includes BitLocker, secure boot, and Microsoft Defender.
- **Intune Bulk enrollment for Windows devices:** It is recommended that [bulk enrollment for Windows](#) be used for both MTRoW and Surface Hubs. The person performing the setup will not require any Intune enrollment rights.
- **Bulk deployment of MTRoW:** With Pro licensing, Microsoft supports the use of [Autopilot](#) for bulk deployments.

Teams application updates are managed through the Teams admin center for these devices, but the underlying Windows OS is not. You should make sure that you have a management plan in place to ensure the Windows based devices receive windows patches and updates if you are not using Intune for this.

Microsoft provide a [supportability table](https://learn.microsoft.com/en-us/MicrosoftTeams/rooms/rooms-lifecycle-support) <https://learn.microsoft.com/en-us/MicrosoftTeams/rooms/rooms-lifecycle-support> that shows the current supported Teams client and OS versions.

Remote Provisioning for Teams Android Devices - Remote provisioning lets you safely sign in to devices without giving anyone access to account credentials. To remotely provision a Teams Phone, Teams Panel, or MTRoA as a shared device, the MAC address must be added to the Teams admin center. Do this by selecting **Teams devices**, choose the sub-section for the device type you want to add, then in the top right corner, click **Actions** and select **Provision devices**. Either add MAC addresses manually or upload a .csv file containing MAC addresses and locations. The menu here contains a CSV template you can download. After adding the MAC address(es), select the phone or phones and click on **generate verification code**. This code will then be used at the initial stage of signing in. Distribute the list of MAC addresses and verification codes to the on-site technicians for deployment.

When the onsite personnel signs into the phone, click on the cog icon in the top right of the device screen. From there, they select the provision phone and enter the verification code provided. If the operation is successful, a welcome screen will appear. When a Teams phone is successfully provisioned, it can be remotely signed in using the Teams admin center.

Go to the same section to add the MAC address, except move to the **Waiting for sign-in** tab this time. Select a Teams Android device to which you want to sign in and click **Sign in a user**. Follow the instructions on the pop-up screen, navigate to <https://microsoft.com/devicelogin>, and paste the code. Select which account should sign into this specific phone. The list of supported devices [is available online](#).

Device store: Microsoft does offer a [store](#) integrated into the Teams admin center in some regions where you can directly purchase Teams compatible hardware. If you buy Android-based devices, Microsoft will automatically provision the MAC addresses for you so they are ready for initial sign-in.

MTR Notification and Alerts - A default alert rule is available to get notifications on changes to MTR health status, which can be found in the Teams admin center under **Notifications & alerts**, followed by **Rules**. These rules are near real-time, but you may have up to a 30-minute delay before you get a notification of an MTR being offline or unhealthy. It isn't ideal but does allow you to respond more or less proactively to an incident.

You need to add the MTR user accounts to the rule manually, and there is no PowerShell or Graph API approach to automate this. The monitoring rule looks at all the devices to which the account is signed in. You can receive the alerts in a Teams channel and/or via a [webhook](#).

Managing Phone Devices

Traditionally, phone devices used to be placed in segregated network sections (the Voice VLAN!), where they had direct access to the PBX onsite. While you can still use this technique to separate your phones from user traffic, it can be less helpful as the devices connect over the internet to the Teams service and generate more than just voice traffic. Therefore, you need to ensure any QoS rules you have for user networks also apply to these devices. Removing this type of VLAN separation can help simplify your overall network topology.

If you use 802.x authentication on your network, you should pre-register the MAC addresses for Teams devices so that they can access the network. Many Teams devices can be configured with Wi-Fi enabled, but while this might work, it is not technically supported, so you should plan to have ethernet connectivity available to ensure the best quality calls. Most of these devices also support Power over Ethernet to help reduce cabling requirements.

In this section, we cover specifics for managing SIP Gateway and Android phone devices:

- Common Area Phone Configuration
- IP Phones and Teams Displays
- Intune and Conditional Access for Android Teams devices

- SIP Gateway Registration
- Intune and Conditional Access for SIP Gateway

Common Area Phone Configuration- The Teams IP Phone policy, *CsTeamsIPPhonePolicy*, applies configuration settings specific to Teams common area phones. Available policy settings are:

- **AllowHomeScreen** – A Teams phone home screen displays a summary of contacts and future meetings.
- **AllowBetterTogether** – The user's settings and experience will be synced when connected to a computer.
- **AllowHotDesking** - Allows any user in the organization to sign into the phone temporarily.
- **HotDeskingIdleTimeoutInMinutes** – How long before a temporary logged-in hotdesk user will be logged out.
- **SignInMode** - Determines the sign-in mode/experience for the phone: User, CAP, or Meeting room.
- **SearchOnCommonAreaPhoneMode** - Determines whether searching the Global Address List is possible when CAP sign-in mode is set.

You may not want to enable hot desking on CAP devices since there is a long timeout. By default, the timeout is 120 minutes. If the user goes to lunch and the phone remains signed in as that user, then anyone can answer calls or make calls on behalf of this user.

To turn off the feature, use this command:

```
New-CsTeamsIPPhonePolicy -Identity "CAPNoHotDesking" -SignInMode CommonAreaPhoneSignin  
-AllowHotDesking $false -SearchOnCommonAreaPhoneMode Disabled -AllowHomeScreen Disabled  
-AllowBetterTogether Disabled
```

We also disable *SearchOnCommonAreaPhoneMode* so that access to search for the Teams global address list is impossible. To apply an IP Phone policy to a CAP account, use the *Grant-CsTeamsIPPhonePolicy*:

```
Grant-CsTeamsIPPhonePolicy -Identity CAP-MainOffice@office365itpros.com -PolicyName CAPNoHotDesking
```

IP Phones and Teams Displays - Management of IP Phones is performed in the Teams admin center, under **Teams devices**, then **Phones**. There you can differentiate the view on All phones, User phones, Common area phones, and Conference phones. You can also download device logs, update software and firmware, and restart the devices. You can get the details on each device, including MAC address and call history. If you have people specializing in device management and setup, then the Teams Devices Administrator role gives them access to just this part of the Teams admin center. Be aware that holders of this role do not get access to call history, so combining this role with the Teams Communications Support Engineer could be beneficial.

You can create configuration profiles to ensure all phones have the correct time zone, language, and time format. You can configure device settings such as display screensaver timeout, backlight timeout, and office hours. DHCP is recommended for these devices, but you can manually configure network settings.

Configuration policies can be assigned to multiple devices in one go by selecting more than one device at a time. For example, sort them by IP address and select a batch to configure all devices in one location together. Make sure to name the configuration policy to reflect the location to which you want the devices assigned, as you need to search for them when assigning. Unfortunately, there is no way to automate this procedure, so you should make this process part of a device onboarding routine.

Intune and Conditional Access for Android Teams devices - Despite many Teams devices running Android, they are not mobile phones. It can be a common mistake to try and manage them in the same way as user mobile devices. To approach managing them with Intune and Conditional Access policies, consider the following:

- For Android devices signing in as personal devices:

- Create an Intune enrollment restriction policy for Teams Phones to require the preregistration of the serial number in Intune before enrollment is possible. This maintains control over who's devices have access to corporate resources.
- For Android devices using shared access accounts, such as Common Area Phones, we need to look at the account signing into the device in addition to the above enrollment restriction:
 - **Account prefix:** Add a prefix, for example, CAP-xxxx, to identify them with a dynamic group.
 - **Compliance policy:** Exclude the dynamic group from other policies and require that the device is not rooted.
 - **Enrollment restriction policy:** Target the dynamic group and allow for "legacy" Device Admin management, as IP Phones do not yet support Enterprise Admin Device management. It is also recommended that you use a corporate device identifier by pre-registering the serial numbers of the devices to control access to the environment.
 - **Conditional access:** Exclude the dynamic group from all other Conditional Access policies and create a dedicated policy that blocks platforms except Android, limits connections from trusted public IP addresses, and requires a compliant device to bypass MFA.

Filter issues: When adding exclusions for conditional access there can be issues with how and when the filters apply during the initial device provisioning. A great overview of some possible workarounds is [available online](#).

SIP Gateway Registration - You can get a full list of all SIP devices logged in to your environment through the Teams admin center by going to **Teams devices** and **SIP devices**. From here, you can provision new devices by adding the MAC addresses to make sure that only devices approved by administrators can sign in. Limited capabilities are available to manage these devices: you can restart the device and see if the device is signed in. No configuration policies are available. You cannot define the device's language as this is done by appending a [code string](#) at the end of the registrar URL. To sign in a device the following conditions must be met:

- The user must have a Teams and Phone System license (or Teams Shared Device license).
- The user must be assigned a phone number through Direct Routing, Operator Connect, or Calling Plan.
- "SIP devices used for calls" must be enabled in the Teams Calling policy assigned to the users.
- MAC address must be pre-registered in the Teams admin center under **SIP devices**.
- [URLs and IP ranges](#) must be opened in the network where the phone is located.

The PowerShell code below is an example of creating an appropriate Calling policy. Note that these phones depend on call redirect, which must be set to enabled.

```
New-CsTeamsCallingPolicy -Identity "SIPPhones" -AllowSIPDevicesCalling $true -AllowCallRedirectEnabled
```

After registering the MAC address of the devices, assigning the correct licenses, and calling policy to user accounts they are ready to sign in. The device must be set up with the correct registrar address, either through DHCP or manually. The registrar addresses for each region are published in the [help pages](#). When the user signs in, a pairing code appears, and the user must navigate to the URL shown, type in the pairing code, and sign in using their credentials. The process is the same for Common Area Phones, except that an administrator can perform the final sign-in steps from the Teams admin center as these are special accounts.

Intune and Conditional Access for SIP Gateway - Devices connecting via the SIP Gateway need to bypass conditional access policies because the actual sign in does not happen from the phone but from a Microsoft trusted IP address (of the Gateway service). You should create a separate conditional access policy and add the accounts you expect to sign in on these devices, be it regular users or common area phone accounts. In this rule, you add the six IP addresses used to sign in the accounts. There are two IP addresses for EMEA, two

for North America, and two for APAC. The current addresses are [published online](#). Your organization might only need to sign in from one or two regions, which means you can limit the authorized set.

Teams Android Open Source Project Device Management

Microsoft is significantly [overhauling the Intune management functionality](#) for Android based Teams devices. The current legacy method relies on using Device Administrator enrollment, which uses functionality that existed in Android for many years, but is now considered outdated. In fact, Google depreciated this method in 2020. Android Open Source Project (AOSP) Device Management is the preferred replacement. AOSP is a much more flexible, modern, and secure management framework.

During the last quarter of 2024 and the start of 2025, Microsoft will deliver firmware updates to supported Teams Android devices that migrates to the new management method. If you use Intune to manage Teams Android devices, prepare your tenant by creating a new AOSP management enrollment profile. This profile will target Teams devices only and will be used during the migration process and when onboarding new devices. If Intune is not used, you can treat the firmware upgrade like a regular update, since nothing will change for you.

To create the new enrollment profile, browse to [intune.microsoft.com](#), then under **Devices, Device Onboarding, Enrollment, Android** find **Corporate-owned, user-associated devices**.

Here, create a new profile with a sensible name. Microsoft suggests "**AOSP – Teams Devices**." Set the token expiration to be 90 days from today (this is the maximum it will let you select). Leave Wi-Fi not configured but toggle "**For Microsoft Teams devices**" to Enabled. Save and create the policy.

If a suitable policy exists when the firmware upgrade is deployed, the devices will automatically remove themselves from Device Administration and re-enroll using AOSP Device Management. Without the policy, the upgrade/migration process will fail. The configuration screen described above shows a tally of devices enrolled against the new policy to help track the upgrade process.

Once you have an enrollment policy configuration, create AOSP specific configuration and compliance policies to manage the devices. This is not required for a successful migration, but it is recommended that you replicate, or update any legacy device management policies to ensure a consistent management experience using AOSP. [Microsoft provides](#) some good guidance and starting points for creating Teams suitable policies.

Initially, applying the firmware updates containing the AOSP upgrade will be a manual process, giving time for testing and troubleshooting. However, prepare your tenant as soon as possible to be ready as Microsoft will make the upgrade automatic in early 2025.

Troubleshooting and Monitoring Calls

So far, we have covered a lot of technical details about calling configuration, device types and setup, as well as how to prepare your environment to support calling. Lastly, we will talk about how to keep on top of all these things, looking at what tools are available to help proactively monitor and troubleshoot any issues as and when they occur.

Validating functionality for Teams Phone

When implementing Teams Phone, testing all features you expect to use before making it widely available is essential. The goal is to find niche scenarios that may not work as intended, as troubleshooting can be complex when the system is fully live.

You should develop a structured testing process to document what is tested, how it was tested, what the result was. Then you will have a good overview of what was working when telephony was implemented. If it

should stop working at some point, you know how it was working initially. Typical scenarios you want to verify when testing include:

- Normalization of numbers per country and region when dialing out.
- Forwarding and transferring of calls to mobile phones or Teams users.
- Your PSTN usages are working as expected, for instance, restricting calls to premium numbers.
- Verify that you can have calls longer than 30 minutes.
- Verify that calls can sit on hold for more than 5 minutes.

These last two tests apply more if you have deployed your own Direct Routing solutions, as sometimes firewalls can interfere with sessions and disconnect long streams.

Troubleshooting Teams Phone for Users

Many settings must be in place for telephony to function. Users must have the correct policies, the right set of licenses, and the correct settings in Entra ID. [Microsoft covers many of the settings in its documentation](#), but this PowerShell one-liner will help you gather the key information you need for an account to evaluate a user's settings:

```
$User = "Ken.Bowers@office365itpros.com"

Get-CsOnlineUser $User | Format-List UserPrincipalName, DisplayName, SipAddress,
OnlineVoiceRoutingPolicy, TenantDialPlan, DialPlan, TeamsVideoInteropServicePolicy,
TeamsUpgradeEffectiveMode, EnterpriseVoiceEnabled, AccountEnabled, LineURI, OnPremLineURI,
FeatureTypes, TeamsCallingPolicy, UsageLocation, City, HostingProvider, InterpretedUserType

UserPrincipalName : Ken.Bowers@office365itpros.com
DisplayName : Ken Bowers
SipAddress : sip:Ken.Bowers@office365itpros.com
OnlineVoiceRoutingPolicy : AzureSBC1
TenantDialPlan : US-NY-NewYorkCityZone01
DialPlan : US
TeamsVideoInteropServicePolicy : PexipServiceProviderEnabled
TeamsUpgradeEffectiveMode : TeamsOnly
EnterpriseVoiceEnabled : True
AccountEnabled : True
LineURI : tel:+19175428xxx
OnPremLineURI : tel:+19175428xxx
FeatureTypes : {CallingPlan, AudioConferencing, Teams, PhoneSystem}
TeamsCallingPolicy :
UsageLocation : US
City : New York
HostingProvider : sipfed.online.lync.com
InterpretedUserType : PureOnlineTeamsOnlyUser
```

Let's go through each attribute and discuss how to validate them:

- **UserPrincipalName:** This is the UPN of the user account.
- **DisplayName:** Not much can go wrong here, it is based on *DisplayName* as set in the user account.
- **SipAddress:** The SIP address is based on UPN. If the SIP address has not populated, there may be a conflict. Use the following cmdlet to locate the user:

```
Get-CsOnlineUser | Where-Object {$_.SipAddress -match "ken.bowers@office365itpros.com"} | Format-List UserPrincipalName, DisplayName, SipAddress
```

You can manually overwrite the SIP address by populating the *SIP:ProxyAddresses* value in Exchange or the *msRTCSIP-PrimaryUserAddress* in AD.

- **OnlineVoiceRoutingPolicy:** To be able to dial out via Direct Routing, this attribute must be populated with the correct policy. To assign the correct value, use the following cmdlet:

```
Grant-CsOnlineVoiceRoutingPolicy -Identity $user -PolicyName "AzureSBC2" -Verbose
```

- **TenantDialPlan:** Make sure the correct *TenantDialPlan* is set on the user. This setting is configured manually. A good attribute to match with is the *UsageLocation* or *City*, depending on if you have multiple locations in the same country:

```
Grant-CsTenantDialPlan -PolicyName "US-NY-NewYorkCityZone01" -Identity $user -Verbose
```

- **DialPlan:** This is the default dial plan assigned to the user based on the *UsageLocation* attribute. If it is blank and *UsageLocation* is set correctly, make sure the user has a Phone System license assigned.
- **TeamsVideoInteropServicePolicy:** To make sure users get the correct CVI settings in their meeting invite if it is configured in the tenant. Set one of the three built-in policies if you need to:

```
Grant-CsTeamsVideoInteropServicePolicy -PolicyName PexipServiceProviderEnabled -Identity $user -Verbose
```

- **TeamsUpgradeEffectiveMode:** Used when Skype for Business is deployed (only available for on-premises hybrid now) and shows what workloads Teams is responsible for. Teams Phone only works when operating in TeamsOnly mode. To set the correct [mode](#), run the following command:

```
Grant-CsTeamsUpgradePolicy -PolicyName UpgradeToTeams -Identity $user
```

- **EnterpriseVoiceEnabled:** If it is set to false, ensure the user has a Phone System license. If you migrate from SfBS and the user was disabled for enterprise voice, but should be enabled online, this attribute is still set to false. To enable the user, run the following command:

```
Set-CsPhoneNumberAssignment $user -EnterpriseVoiceEnabled $true
```

- **AccountEnabled:** indicates if the account can sign into Entra ID. If the account is disabled, you can enable the user with the following command (after connecting with *ReadWrite* Graph API permissions):

```
Update-MgUser -UserID $user -AccountEnabled:$true
```

- **LineURI:** Defines a user's actual telephone number and shows when dialing out from Teams. If you use Direct Routing, this attribute is synced with *OnPremLineURI*. If the *LineURI* attribute does not sync, validate that the user is not also assigned a Calling Plan. If Calling Plans are used, use this cmdlet to set the correct phone number:

```
Set-CsPhoneNumberAssignment -Identity $user -PhoneNumber +15555428572 -PhoneNumberType CallingPlan
```

- **OnPremLineURI:** Is the phone number provided to the user through Direct Routing. If you have migrated from SfBS to Teams, you need to clear out the *msRTCSIP-Line* attribute in Active Directory.

```
Get-ADUser -Filter "UserPrincipalName -eq '$user'" -property * | Set-ADUser -clear 'msRTCSIP-Line'
```

Wait until Azure AD Connect has synced the setting to Entra ID, and then set the phone number using *Set-CsPhoneNumberAssignment*, which almost instantly populates the number. The *PhoneNumberType* option defines the source of the assigned number, this can be either *CallingPlan*, *OperatorConnect* or *DirectRouting*.

```
Set-CsPhoneNumberAssignment -Identity $user -PhoneNumber +15555428572 -PhoneNumberType DirectRouting
```

- **FeatureTypes:** Shows an array of values depending on what features are enabled. Values you may expect to see here include: *Teams*, *AudioConferencing*, *PhoneSystem* and *CallingPlan*.
- **TeamsCallingPolicy:** Defines the calling policy assigned to the user which defines calling features such as voicemail.

- **UsageLocation:** Based on the *UsageLocation* property of the user account. This attribute affects Calling Plan availability and the default dial plan assigned to the user. Use the *Update-MgUser* cmdlet to update the *UsageLocation* attribute:

```
Update-MgUser -UserID $user -UsageLocation GB
```

- **City:** A typical location-defining attribute. A great way to determine which *UsageLocation* to assign to the user account.
- **HostingProvider:** If a different value than *sipfed.online.lync.com* is shown here, the user is considered an on-premises user. If you have migrated all users online and decommissioned your on-premises environment, use this Active Directory PowerShell cmdlet to clean up the attributes for SfBS. First, to check the current value of the attributes:

```
Get-ADUser -Filter "UserPrincipalName -eq '$user'" -property * | Format-Table 'msRTCSIP*'
```

Clean up at least the *DeploymentLocator* attribute. The *PrimarySIPAddress* should remain as it helps the SfB client with SSO the first time a PC logs on. *LineURI* should remain as it is the user phone number when using Direct Routing:

```
Get-ADUser -Filter "UserPrincipalName -eq '$user'" -property * | Set-ADUser -clear 'msRTCSIP-DeploymentLocator'
```

- **InterpretedUserType:** Displays the overall Teams status of the user account. There are many different values this can take, but this [GitHub article](#) has a good rundown. This value should be one of the first things to check for any troubleshooting, especially helpful in hybrid environments. If the user displays as *HybridOnpremSfBUser* when they should be a *DirSyncSfBUser* user, it may indicate residual SfBS attributes. To see the SfBS attributes for a user, run this command on a server that has the Active Directory PowerShell module installed:

```
Get-ADUser -Filter "UserPrincipalName -eq '$user'" -property * | ft 'msRTCSIP*'
```

It is a best practice that all attributes, except *msRTCSIP-PrimaryUserAddress*, should be cleared out when decommissioning an SfB environment. *msRTCSIP-PrimaryUserAddress* is used by the SfB client to discover the user's SIP address and populates the Sign-In address for newly deployed PC's. If *Disable-CsUser* was not run as part of decommissioning, these attributes are likely still populated. Here is how to clear out the common msRTCSIP attributes. Make sure you capture all *msRTCSIP-Line* values if they are configured so that you can configure users online with the same number:

```
#Get all msRTCSIP properties for a user that has a value
$Properties = Get-ADUser -Filter {UserPrincipalName -eq "stale.hansen@office365itpros.com"} -Properties * | Select-Object -Property 'msRTCSIP*'

#Clear all properties for a user
Get-ADUser -Filter {UserPrincipalName -eq "ken.bowers@office365itpros.com"} -Properties * | Set-ADUser -clear ($Properties | Get-Member -MemberType "NoteProperty" | % { $_.Name })
```

Missing dial pad: Sometimes, in the v1 Teams client there can be a significant delay before the dial pad appears for newly enabled Teams Phone users. In the v2 client this should be less likely. However, to troubleshoot it, run through the [documentation](#) to ensure settings are configured, and there is a test button to run self-diagnostic tests against named accounts in the Microsoft 365 admin center.

Call Quality

To succeed with a Teams voice deployment, you must ensure that calls connect properly and that call quality is good. What constitutes good call quality? This is highly subjective, but packet loss, jitter, and latency are key network metrics you can measure. At the start of this chapter, we covered basic best practices for approaching

your networking setup, but here we go deeper into how Teams calling uses network resources. This is where Teams gets challenging to understand and master, but luckily, we can work with several tools to assist with the task, such as the Network Assessment tool, Call Quality Dashboard, and Call Analytics. The final section covers these tools.

Understand Signaling and Media

Every call has two parts, signaling and media. Signaling is the part that manages your call such as establishing, maintaining, and terminating it. The concept used in Teams for signaling is the same as SfB, even if the protocol differs. SfB uses the Session Initiated Protocol (SIP) while Teams uses HTTPS REST signaling. Media communication is still based on UDP and travels as directly as possible between endpoints in all scenarios.

In 1-to-1 calls, media attempts a direct connection between clients after establishing signaling. This will likely succeed for clients on the same corporate network or subnet, as shown in Figure 13-5 where media can establish directly, but signaling still passes through the Teams service. As a result, voice and video here will have a higher chance of being good quality with fewer packet drops than when passing through the internet.

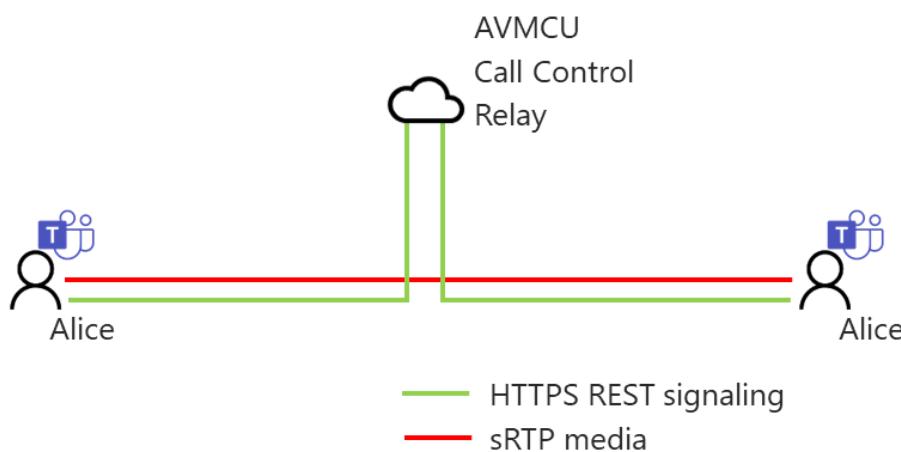


Figure 13-5: Signaling goes via the Teams Service and media goes directly between the clients

In 1-to-1 calls where media cannot go directly, because a firewall is between subnets or one user is external, the media will be relayed as shown in Figure 13-6.

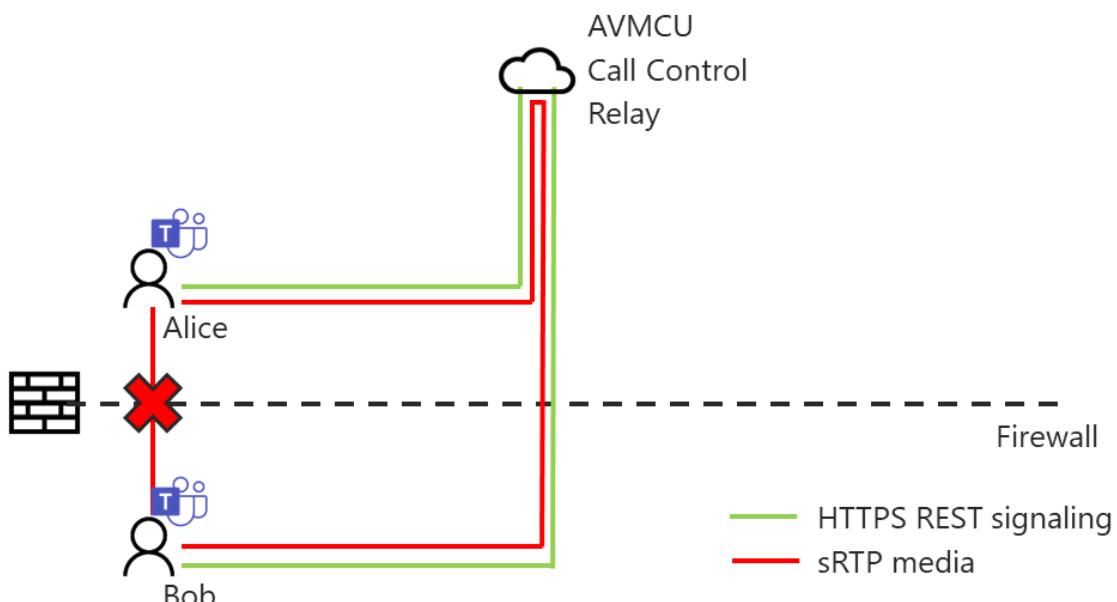


Figure 13-6: Signaling goes via the Teams Service and media goes via the relay services in Azure

In an ad-hoc multiparty call with more than two participants or a scheduled meeting, the media will go to the conferencing service as shown in Figure 13-7. Regardless of who is invited to the scheduled meeting, the first participant to join dictates where the conference is hosted. For instance, if you have three participants in the US and 10 participants in the EU and a US participant joins first, the conference will be hosted in a US data center, and all 10 EU participants must join the call hosted in the US.

If you use a VPN, you should measure the effect this has on traffic. For example, in Figure 13-7, Alice's media traffic would need to first come inside the firewall before going out to the AVMCU (Audio/Video Multipoint Control Unit – or media processing point). Teams networking best practice is to allow at least the media traffic to pass outside the VPN tunnel. Teams traffic on the network is always encrypted, so it does not need the additional protection of a VPN which adds overhead to the packets (for processing and hops).

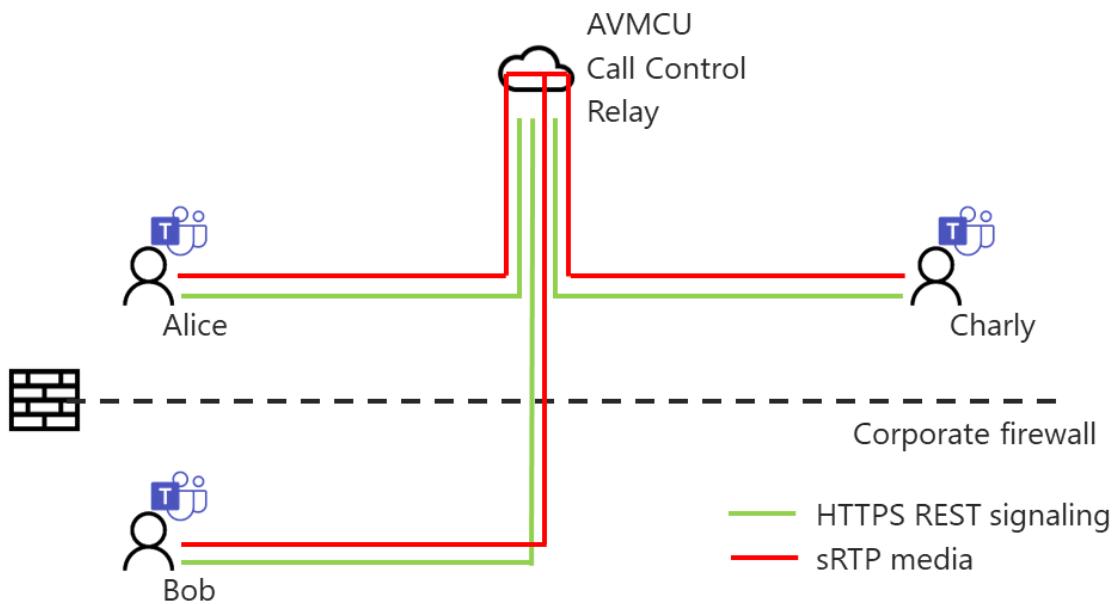


Figure 13-7: Signaling goes via the Teams Service and media goes to the AVMCU where the first joiner is homed

If you must use a VPN, try to allow at least the Teams Optimize media IP ranges to go outside the VPN tunnel.

Local logs: By default, the Teams client only collects media related logs locally on high-end computers. If you raise a support call to Microsoft these local logs may be required, which can be hard to capture if issues are intermittent. There is a policy that can be configured to force the Teams client to produce local [media logs](#) as required.

The Impact of Codecs

There are four codecs used for Teams depending on the scenario and devices used on either end of the connection:

- **Satin** is the primary codec for 1-to-1 calls and soon for meetings. It uses AI to optimize for high quality under high packet loss and starts at a bit rate for wideband voice at 6 kbps. At 17 kbps it can produce full-band stereo music. There are some [interesting examples](#) available online showing how Satin functions.
- **SILK** is the primary codec in meetings and is both wideband and narrowband across clients except for Edge and Chrome.
- **G.722** is the secondary codec that is available in all scenarios across clients.
- **G.711** is the secondary codec in PSTN calls.

Table 13-3 shows the typical bandwidth usage of Teams codecs. Microsoft has not released data for Satin.

Audio codec	Scenarios	Audio payload bitrate	Bandwidth Payload, IP header UDP, RTP	Bandwidth payload, IP header, UDP, RTP, SRTP	Bandwidth Payload, IP header, UDP, RTP, SRTP, Forward Error Correction
SILK Wideband	Meetings	36.0	52.0	64.0	100.0
SILK Narrowband	Meetings	13.0	29.0	41.0	54.0
G.722	Secondary in all	64.0	80.0	95.6	159.6
G.711	PSTN	64.0	80.0	92.0	156.0

Table 13-3: Teams and codec bandwidth in kbps for audio

Forward Error Correction: FEC is used when you start having packet loss in the network. Teams compensates by sending overlapping information per packet, so that even if packets are lost, the overall impact is minimized.

Video is based on X.264 and hasn't changed much in recent years. Teams can scale video by resolution and framerate. Resolution may vary based on the screen the participants use in the meeting and the resolution they request. Each client sending video will send a stream to the Teams service at the best quality that can be supported (or is needed). The participating clients in the meeting then request different quality streams from the server depending on what layout is displayed to the user. For example, there is no point in the client requesting a full 30FPS 1080p video feed from all users when they are only being shown as thumbnails alongside a screen share. Usually, the more participants there are in the meeting, the smaller the requested video to accommodate extra thumbnails.

The Large Gallery view is available only when more than 10 people are in a meeting. In gallery view, the meeting service stitches together the video from all participants and then sends one video stream of this combined image to the user's client.

Screensharing in Teams uses either Video Based Screen Sharing (VbSS) where the screen share is another specialized video stream, or more recently switching the AV1 codec that is up to 60% more efficient while providing better overall quality.

PowerPoint decks can be presented independently through the PowerPoint online viewer, which is not video-based and so isn't captured as part of any meeting recordings.

Table 13-4 lists some video scenarios and potential bandwidth when using 1080p resolution. Be aware of the equipment your users are using and where most of them may run video meetings and make sure you scale available bandwidth to anticipate the estimated load. This is where the network planner will help.

Participants/Activity	Max resolution	Total max download bit rate (Mbps)	Total max upload bit rate (Mbps)
2 Participants	1 * 1920x1080	4	4
3 Participants	2 * 1920x1080 (Full Bleed) 2 * 1280x720	8 5	6.5
4 Participants	1 * 1280x720 + 2 * 960x540	5.5	4
5+ Participants	4 * 960x540	6	1.5

Video Based Screen Sharing (Only)	1 * 1920x1080	4	4
N Participant + VBSS [N=0-4]	1 * 1920x1080 + N * 424x240	4 + (N*350 Kbps)	~4.34

Table 13-4: Teams and bandwidth for video (bit rate in Mbps)

Keep in mind that when Teams uses the large gallery and together mode in meetings, it is one video stream.

Network Factors Affecting Voice Quality

Network metrics such as packet loss, jitter, and latency affect voice quality. These network metrics affect real-time media and are experienced in different ways.

Users experience packet loss in two ways. If you hear metallic and variable sound quality, it can be caused by random packets being dropped. Sometimes you may hear the person talking go silent for several seconds, which is caused by burst loss of packets, where contiguous packets are lost.

Packet loss is typically caused by transmission errors and router congestion. If contiguous packet loss exceeds 10 seconds, the call may be disconnected. This is typically a problem over Wi-Fi that is designed for access and not throughput. Especially if you walk around with an active call and need to switch access point, the handover time may be too long, and the call gets disconnected.

Jitter is caused by packets arriving in a different order than the order they were put on the network and with longer intervals. It is typically caused by packet taking different routes due to load balancers or re-direction due to router congestion. You experience jitter when you hear a short silence and then the person talking faster than normal. This is caused by the Teams client buffering packets and playing them back when enough have arrived. If there is more than a 20 millisecond gap between packets the audio healer will start dropping them and the experience will be the same as for packet loss.

Latency is the time it takes for a packet to travel from the sender to the receiver. When measuring latency, it is important to put the result in context. Latency higher than 100 milliseconds within the same country is not good. A latency of 150 millisecond across continents is very good. Latency is typically caused by distance, queuing, and buffer overflow on the network. You experience latency when people you talk to on a call seem to take a long time to answer. A call with a lot of latency can be quite difficult to manage and those on the call may end up talking at the same time.

Table 13-5 shows the target network metrics in an unmanaged network, which include all the locations the network administrator has no control over such as the internet, home office, or favorite coffee shop. Table 13-6 shows the target network metrics in a managed network, typically inside corporate offices. Meeting these network metrics is important to meet user expectations of good voice quality and dependent stability of calls. We look at managed networks in two scenarios, where the users are and the corporate network edge. The goal is to know when it is an internet problem or where it is a local network problem.

Unmanaged Network Voice	Optimal	Acceptable	Poor
Inter arrival packet jitter (average)	$\leq 5\text{ms}$	$\leq 10\text{ms}$	$> 10\text{ms}$
Inter arrival packet jitter (maximum)	$\leq 40\text{ms}$	$\leq 80\text{ms}$	$> 80\text{ms}$
Packet loss rate (average)	$\leq 1.0\%$	$\leq 5.0\%$	$> 5.0\%$
Network latency one-way	$< 100\text{ms}$	$\leq 100\text{ms}$	$> 100\text{ms}$

Table 13-5: Unmanaged network targets

Managed Network Voice	Teams client to Microsoft network edge	Corporate edge to Microsoft network edge
------------------------------	---	---

Latency (one-way)	<50 ms	<30 ms
Latency (round-trip)	<100 ms	<60 ms
Burst packet loss	<10% during any 200 ms interval	<1%
Packet loss	<1% during any 15s interval	<0.1% during any 15s interval
Packet inter-arrival jitter	<30ms during any 15s interval	<15ms during any 15s interval
Packet reorder	<0.05% out-of-order packets	<0.01% out-of-order packets

Table 13-6: Networking requirements for Teams media in managed networks (source: Microsoft)

Teams and QoS Tagging

Teams uses two QoS port ranges, 1-to-1 port ranges and meeting port ranges. 1-to-1 calls use the port range of:

- Audio using TCP/UDP: 50,000–50,019
- Video using TCP/UDP: 50,020–50,039
- Screen Share using TCP/UDP: 50,040–50,059

As well as using network-based tagging, you can create a GPO to make Windows apply DCSP tags against the Teams.exe client for your Windows clients. You can add different markings for audio, video, and screen sharing. Audio is typically the highest DCSP value of 46.

If you use Direct Routing with Media Optimization, the audio port range is UDP 50,000 to 59,999 for traffic going directly to the SBC. In the future, media bypass ports may change to 3478 and 3479.

Conference media traffic goes via the Teams media relay services in Office 365. Some of that transport is over the internet, but you can still add [QoS tagging](#) and prioritize the traffic while it is in the internal network. All media that goes via the Teams media relay use port UDP 3478 by default. To separate audio, video, and screen sharing traffic you need to go to the Teams admin center, **Meetings**, and **Meeting settings**, and turn on **Insert Quality of Service (QoS) markers for real-time media traffic**.

When this is done, port 3479 will be used for Audio, 3480 for video, and 3481 for screen sharing. The QoS markings will persist if used with ExpressRoute, and traffic from Android, iOS, and Mac clients will have DSCP tagging on these ports.

Media flows deep dive: The [Media in Teams - Media Flow YouTube video](#) does a great job of deep diving into media flows and bandwidth considerations.

Monitoring and Validating Call Quality

Teams includes two ways to monitor and troubleshoot call quality problems: Call Analytics and Call Quality Dashboard (CQD). Call Analytics is designed to help review call quality for individual calls, here you can see and explain why a call was experienced as poor. You get information about what equipment was used, if it was a wired or wireless call, and information on network metrics. CQD is meant to look at trending quality within your environment. CQD is a separate portal, linked from the Teams admin center, but the CQD data is best consumed via Power BI reports, this is covered at the end of this chapter.

Reporting Teams Phone Activity

Organizations that use Teams Phone probably want to report on how people use Teams Phone with the intention that by understanding usage, they can make sure that they do not pay too much for PSTN services. A usage report of PSTN calls for Calling Plans and Direct Routing is available in the Teams admin center. The report is good, but you can also access the data programmatically to create custom reports. You can do this using the [callRecord: getPstnCalls API](#). The information retrieved includes who called, duration, dial plan used, and destination, amongst other attributes. Microsoft provides an [open source script](#) to export call records (CDRs) to Cosmos DB or Kusto for further processing. Alternatively, this third-party [PowerShell script](#) shows

how you can build your own solutions. A [PowerShell module](#) is also available to simplify access to the Teams phone activity list.

In October 2022, Microsoft introduced a new set of PowerBI reports that used a new backend data source called the Voice Applications Analytics Collector (VAAC). [These reports](#) provide better visibility of calls passing through Auto Attendants and Call Queues, which is missing from the default set of reports.

Client call log: Users can remove calls from their call history in the Teams client. However, the associated log entries will remain available in these tools for logging and troubleshooting.

Call Analytics

Call analytics, which can be accessed from the Teams admin center by going into **Users, Manage users** and then selecting **Meetings & calls**, shows the most recent calls and meetings for users. Call analytics focuses on single calls and meetings, providing a detailed analysis of the selected call or meeting for issue resolution by the helpdesk and requires one of the Teams Administrator, Teams Communications Support Specialist, or a Teams Communications Support Engineer roles.

The screenshot shows the Microsoft Teams Admin Center interface for Call Analytics. At the top, there are tabs for Overview, Advanced, and Debug. The Overview tab is selected, showing a summary for a user named Ben Lee. The summary includes a thumbnail of Ben Lee, a microphone icon, and the text "Complete 00:14:13". It also indicates "Audio quality Good". Below the summary, there are four tabs: Device, System, Connectivity, and Network. The Network tab is currently selected. A detailed table below the tabs provides network performance metrics:

Network Stream Metrics	Value
Average round-trip time	46 ms
Maximum round-trip time	65 ms
Average network degradation	0 MOS
Maximum network degradation	0 MOS
Average jitter	1 ms
Maximum jitter	12 ms
Average packet loss rate	0.00%
Maximum packet loss rate	0.00%

Figure 13-8: Call Analytics example for a conference call

You can analyze four core areas:

- **Device** shows you specific information about the capture and renders device the user was using during this call, and you can determine if it was a Teams certified device.
- **System** shows you system statistics such as OS and client patch level.
- **Connectivity** tells you how the system is connected, for example, via Wi-Fi.
- **Network** shows you networking statistics such as packet loss, jitter, and delay.

Figure 13-8 shows an example of the report's network section where we see a good call with acceptable performance, broken down by both stream type and direction. The report shows you real actionable statistics in each category described above. You can use what you have learned here to analyze the metrics collected.

Analyzing the metrics, you can tell the user why the call failed, whether it was because of packet loss on a Wi-Fi connection or if they used an unsupported audio device. You can also use the data to investigate further trends in the network location or the user's driver version. The report highlights poor calls for individuals and is only good for investigating individual calls. If you want to review further trends in your subnets, you should use the Call Quality Dashboard.

Call Analytics can also show near real-time statistics for in-progress meetings. Having access to real-time information about calls allows the IT/Helpdesk to deliver live support during high-stakes meetings. The data you will see is jitter, latency, packet loss, and frames per second for audio, video, and screen sharing. There are some [limitations](#) with the real-time view.

You can also find a **Call Health** feature in the Teams client when in a call. This is accessed via the **More, Settings** menu. Here you can verify what codec is used, compare the network metrics to the guidelines in Table 13-5 and dive into details broken into four categories: Network, Audio, Video and Screen Share. Be aware that this information is only what your client sends and receives and is not a total overview of all participants in the call.

Test calls: Users should be encouraged to use the **Make a test call** feature in the Teams client under **Devices** in the client **Settings** menu before meetings or important calls to verify that your sound is working properly.

Proactive Call Quality Alerting - To assist with [proactive call quality monitoring](#), rules can be configured to alert via a Teams message (or webhook) when certain users are having calling issues. This feature does require a Teams Premium license for the users who can be monitored.

To configure real-time call alerting in Teams admin center, expand **Notifications & alerts** then select **Rules**. Here you can select three types of real-time monitoring available for calls: Audio, video or screensharing quality. Each rule allows you to select:

- **Networking parameters to monitor:** Specify thresholds for Packet Loss, Jitter, Local heal ratio & Round trip time.
- **Time period:** Specify what length of time will trigger the poor call quality rule
- **Scope:** Select which Teams Premium users to monitor
- **Subnet:** if the rule should trigger for just internal, or internal and external subnets
- **Action:** Which team, channel or webhook to trigger when the rule conditions are activated

If you have Teams Premium licensing this is a great way to be proactive about quality issues for key users in your organization but be aware that you cannot specify different alerts or values for different groups of people. All users you want to monitor will be covered by the same rule.

Call Quality Dashboard

Call Quality Dashboard (CQD) is a tool that helps you identify and troubleshoot trends in your organizations calling usage. It is there to capture symptoms and help you get a feel of the solution and where to focus your improvement efforts. As such, you should try and build a habit of exploring CQD at least once a month as part of your maintenance processes. If you have only recently deployed Teams or added a new workload such as telephony, then you should be doing more regular weekly reviews to ensure things are working smoothly.

CQD is accessed via its own [URL](#) and is also found under **Analytics & reports** inside Teams admin center. All Teams admin roles can access CQD, which updates on average every 30 minutes. Due to compliance reasons,

Personally Identifiable Information (PII) data is kept for only 30 days, and all other CQD data is available for up to 90 days.

CQD is all about streams. A stream is a one-way direction of a media modality in a call. You can have multiple streams within a call, so the number of streams in a location is much higher than the number of calls. It depends on how many users were in the call and how many streams there were per user. The streams are classified into three categories which are Good, Poor, and Unclassified. The percentage of poor streams indicates how many of the total streams were graded as poor. However, make sure the total stream count is significant, or this can throw out the average. Unclassified streams are too short to collect data or calls with federated parties. Data from federated parties is not visible inside your tenant. Figure 13-9 shows a summary report from the CQD portal, showing the overall number of streams for any given month.

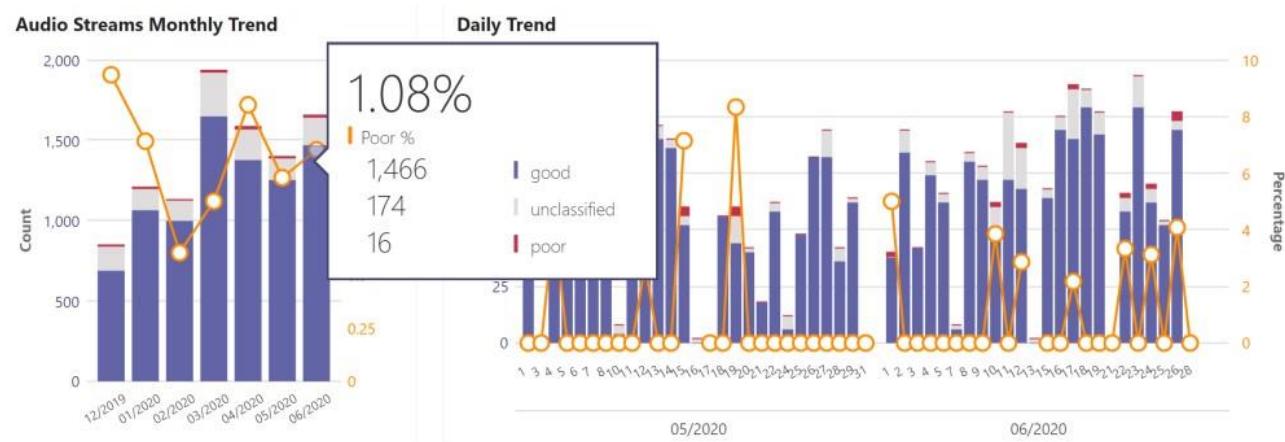


Figure 13-9: All Audio Streams default report in CQD

A good place to start is looking at the Quality of Experience Reports. Here you can follow a breakdown of calls split by those with quality issues or reliability problems. Each section lets you dig into calls by type, such as conference, 2-party or PSTN calling. From the previous section on Call Quality, you should now be able to help identify where issues may be on the network. One sub-report here that can be particularly useful is TCP Usage. If you see a high volume of TCP traffic in your media calls, this indicates something is blocking Teams traffic. Teams always tries to use UDP for media first.

While you should be aiming to drive down the overall percentage of poor calls, it is unlikely that you will get it close to zero. Quite simply, too many factors can influence call quality and too many scenarios where users are making calls. An administrator's job is to optimize as many of these factors as possible. Having a poor percentage figure below 4% means you are doing a good job.

CQD “secondary” indicator: When working with CQD you will see two sets of most metrics. Anything generated by the server (so Teams) is always referenced as “first” and the client as “second” so when working with filters make sure you use the “Second” value, for example, *Second Building Name*.

What is a Poor Stream?

Teams evaluates five factors to determine if a stream is considered poor, these are slightly different to the metrics we used previously for call troubleshooting. The stream is classified poor if one or all metrics are above the threshold shown in Table 13-7. These metrics are higher than what is considered bad, this way you know that a poor stream was terrible. Degradation average is when the network gets worse during a call, if the degradation average is above 1 then you have an unstable or constrained network. Look for routers or switches that are underperforming or overloaded Wi-Fi Access Points. Ratio Concealed Average is a technique used to compensate for dropped network packets, and the Ratio (%) is the percentage of packets concealed in a call.

Network Metrics	Poor Stream
Packet Loss Rate	> 10%
Round Trip Time	> 500 ms
Jitter	> 30 ms
Degradation Average	> 1
Ratio Concealed Average	> 0,07 (7%)

Table 13-7: Network metrics and poor streams

CQD training: If you want to learn more about CQD customization, the SOF CQD training videos on the [Skype for Business YouTube channel](#) are highly recommended and are still relevant to Teams.

Implement Power BI reports to view CQD Data

Microsoft has released a set of Power BI reports for accessing CQD data. These reports are better and more usable than the native CQD reports for looking at trending data and gives the helpdesk a better tool to look at call quality. The Power BI reports connect directly to the CQD dataset and may be a bit slow because of that, but they give valuable information, so it is worth the wait. To view the CQD data in Teams via the Power BI reports, you need to have one of the below admin roles assigned.

- Global Administrator
- Global Reader
- Teams Service Administrator
- Teams Communications Administrator
- Teams Communications Support Engineer
- Teams Communications Support Specialist
- Reports Reader

Note that the Teams Support Specialist and Reports Reader roles cannot see PII data such as SIP addresses and telephone numbers. The available reports are:

- QER (Quality Experience Report) – this is the primary report and should be the starting point for any review or troubleshooting.
- AACQ – contains reports about call flows through VoiceApps and high-level agent performance.
- MTOE – Two reports targeting the experience across MTRs and Phones.
- Legacy reports – contains older reports that have now mostly been consolidated into the QER

The helpdesk report is especially useful for day-to-day support to find calls by date or user. To start, download [the Power BI templates for CQD](#). The zip file contains detailed instructions for configuring the reports.

Chapter 14: Managing Clients

Paul Robichaux

Many Clients, One Service

In the same way that users say things like “My Outlook is down” when they mean that their Exchange Server mailbox is broken, many of us think of cloud systems through the lens of the clients we use. Microsoft has a sometimes-confusing mix of clients for its cloud services, including desktop clients for macOS and Windows; mobile applications for iOS and Android; web applications; clients for Windows Mixed Reality and Apple visionOS devices; and embedded clients built into desktop phones, Surface Hub devices, and so on.

It makes sense to consider these applications as individuals for two reasons. First, the same application (say, Outlook) may have different features on different platforms. For example, the classic version of Outlook has voting buttons, whereas neither its replacement nor the macOS version do. Second, different applications on the *same* platform (say, Windows) may have significant differences too—you may remember how long it took for all of Microsoft’s desktop applications to fully support modern authentication.

With that in mind, we can put Microsoft 365 clients into three basic categories:

- *Browser-based clients* run in a compatible web browser and communicate directly with the service. Their supported features depend much more on the browser you choose than on the underlying host OS. Every workload in Office 365 has some level of browser-based client support.
- *Rich applications* run on macOS or Windows and provide, usually, more functionality than their browser-based counterparts. For example, the macOS and Windows versions of Outlook both support accessing multiple Exchange Online accounts in the same client, whereas Outlook on the web does not.
- *Mobile applications* run on Android, visionOS, or iOS and provide on-the-go access from tablets and phones to some, but not necessarily all, of the service workloads and their features.

Within these categories, you’ll notice some interesting differences. For example, Exchange Online, Lists, Teams, and To Do all have clients in all three categories, while Planner and Stream don’t have desktop clients. It’s important to keep in mind that Microsoft thinks of these clients as ways for users to interact with the data maintained in the “intelligent substrate,” the collection of all the data and services that Microsoft 365 delivers. If you think of Microsoft 365 as a single unified service powered by the substrate instead of a collection of standalone services, this blurring of client boundaries makes sense. As explained in the tasks chapter, a task is a task, no matter whether you access it through To Do, Planner, or Exchange Online, and no matter where it’s stored. As Microsoft adds new services to their cloud platform, they introduce clients for those services but the feature set and supported platforms for each service’s clients may differ.

The Browser: The Base Microsoft 365 Client Platform

All Microsoft 365 workloads support web browsers. Most new services initially appear as web-only applications; some gain desktop applications later, but some do not. Some services launch on multiple platforms simultaneously. Teams is an excellent example, as it launched into preview with web, desktop, and mobile clients from day 1.

Microsoft's guidance for browsers used within Microsoft 365 is simple: the [Microsoft 365 system requirements page](#) recommends that you use the *latest* versions of the supported browsers. Right now, the "supported" list includes Edge, Apple Safari, and Google Chrome. Mozilla Firefox is labeled as supporting "most Microsoft 365 apps" but also says "Firefox does not fully support Microsoft Teams meetings." Other browsers, such as Opera or Brave, or older versions of supported browsers, may work, but Microsoft doesn't guarantee that every app feature will work. In all the non-Microsoft browsers, you may occasionally notice odd UI behavior or display problems. This situation is complicated by the fact that sometimes browser developers make changes that break things that worked properly before their intervention.

One more key thing you should know about browser-based clients: there are no special licensing requirements to use them (as there are for some of the desktop and mobile clients). There is also a specific license type, the kiosk or frontline worker license, which gives access mainly via web browser and not via desktop applications. Kiosk users can also access mailboxes using ActiveSync clients, as well as POP3 and IMAP4.

Rich Office Clients

Microsoft 365 supports any version of Microsoft Office desktop software that is still in [mainstream support](#). The Microsoft 365 Business Basic and Standard plans, and Enterprise plans from E3 upward, include the right to install and run the Microsoft 365 Apps suite of enterprise applications (Word, Excel, PowerPoint, Outlook, and so on). Companies can also license the Office desktop applications separately, without any of the other cloud services such as Exchange Online or SharePoint Online included in the plan, and gain the benefits discussed below. But because you are reading this book, we'll assume that you are doing more with Microsoft 365 than just using the desktop applications.

The desktop Office applications have historically been available in two forms. First is the familiar "perpetual license" version: you buy it once and keep it forever. Perpetual versions of Office for Windows have long been built on the Microsoft installer (MSI) format. The second, newer, form delivers Office as a subscription-based service. When you license Office this way, you only have the right to use it while you keep paying. In exchange for this ongoing fee, you get more rapid product updates. You will sometimes hear people refer to subscription-based Office as "click-to-run" or "C2R" because the Office apps themselves are built on an application virtualization technology (known as App-V) that allows application updates to be streamed on-demand. It is challenging to mix C2R and MSI versions of Office on the same machine, and Microsoft recommends that you not do it.

Real World: The Microsoft Teams desktop client doesn't use either the MSI or C2R mechanisms even though it is officially now part of the Microsoft 365 Apps suite. You can download a platform-specific executable installer that streams the Teams installation bits to the machine using App-V, but after that initial installation, the Teams client will automatically update itself. Bowing to user requests, Microsoft also offers an [MSI-based installer for bootstrapping Windows Teams installations](#) through Microsoft Endpoint Configuration Manager or Group Policy, but once the product is installed that's the end of your control over its updates.

The [Long Term Servicing Channel](#) (LTSC) version of Office is targeted at devices that cannot or should not be updated frequently. Microsoft cites examples such as process control systems on a factory floor or devices used in regulated industries such as healthcare or financial services. Office LTSC is intended for limited use on a subset of an organization's devices, not as the primary Office version in use. When LTSC first shipped, it included the Teams client; Microsoft stopped bundling Teams with it due to the European Union's decision that bundling Teams and Office was anti-competitive, but that change didn't affect existing installations, and you can still deploy Teams onto LTSC machines.

Microsoft announced the next perpetual version of Office for Windows will be Office 2024. They did this in a sneaky way: they've released a [preview of Office 2024 LTSC](#), which will apparently be the only perpetually-licensed version when it ships. Their description of Office 2024 LTSC gives the game away: "Office LTSC 2024 will include features from past Office releases as well as a subset of new features already available in Microsoft 365 Apps for enterprise." Their intent is clearly that enterprises will run the Office 365 apps on most of their machines, reserving the LTSC version (and its limited functionality compared to the cloud version) for a small subset. As of this writing, Microsoft is planning to release Office 2024 LTSC sometime in October 2024, but they haven't announced a firm date yet.

There's also a macOS version of LTSC, known today as "Office 2021 for Mac." "Office 2024 LTSC for Mac" is the forthcoming replacement for that version.

Real World: Many client applications, such as browsers, Teams, and the C2R version of the Office desktop applications automatically update themselves when new versions are released. Some enterprises prefer to disable automatic updates and control the deployment of updates. That is fine... if you don't prevent the updates from ever being deployed. Your update strategy should be either automatic or manual. Not updating at all isn't a valid strategy. For smaller organizations that are content to allow automatic updates, the IT administrators should at least maintain awareness of the vendor releases by subscribing to RSS or email notifications from those vendors.

Mobile Clients

Apple, Google, and Microsoft desktop and mobile operating systems all include basic applications for email and calendar access; they may also include apps for simple office productivity tasks, chat, and so on. Interestingly, Apple and Google also compete directly with Microsoft for productivity and cloud services dollars. That limits their willingness to put first-class support for Microsoft 365 into their native applications. That's perfectly OK, though, because Microsoft is doing that on their own.

Microsoft produces a wide array of Microsoft 365 client apps for Apple (iOS, iPadOS, and VisionOS) and Android, including:

- Authenticator (used for passwordless authentication, multi-factor authentication, and more).
- LinkedIn.
- Microsoft 365 Admin.
- Microsoft Lists.
- Microsoft Loop.
- Microsoft Teams.
- Microsoft To Do.
- Microsoft Lens (formerly known as Office Lens).
- Microsoft 365, which combines features of Word, Excel, and PowerPoint. This app used to be called just the "Office" app, but in October 2022 Microsoft renamed it.
- Outlook (including an "Outlook lite" version for Android).
- OneDrive (the same app can connect to both OneDrive for Business and OneDrive consumer).
- OneNote.
- Planner.
- SharePoint Online.
- Sway.
- Whiteboard.

Companion mobile apps typically appear soon after an application reaches General Availability. For example, Microsoft Lists became generally available starting in July 2020, and later in the year Microsoft announced

released the Lists mobile client for iOS, with the Android version following in late 2021. Some differences might exist between the iOS and Android versions of mobile apps due to the different capabilities available to developers on the two platforms. For example, many versions of Android support separate user profiles for personal and work use, and now Microsoft has started to take advantage of this feature (e.g. by allowing admins to prevent personal accounts from connecting to Microsoft To Do, or by allowing work and personal profiles to both see the same unified calendar data in Outlook).

More details about how to manage mobile devices and application access are in the Intune chapter.

Managing the Microsoft 365 Apps Suite

The pace of innovation and development in Microsoft 365 makes it impossible to maintain support for older versions of client software without incurring high development and support costs that Microsoft would then need to pass on to customers. When you consider moving to the cloud, one factor in your decision must be an implicit commitment to keep your clients up to date. If you allow your client applications to become outdated, you can expect the quality of the user experience to degrade over time. Eventually, users might be unable to use some advanced features because their client software is unsupported or obsolete. For that reason, in this book, we've chosen to focus on Microsoft 365 Apps, the "service" version of the Office desktop applications. There are other versions; the full list of supported versions of Office includes:

- Microsoft 365 Apps: The Microsoft 365 Apps for enterprise suite of desktop Office applications is available both for Windows and macOS.
- The Office LTSC version, described earlier in the chapter.
- Office 365 Professional Plus ("Pro Plus"): desktop applications before version 2004 retain the Pro Plus branding.

These are just the product names. In terms of specific versions, Microsoft doesn't usually emphasize specific version numbers, and instead recommends that you apply the latest updates. There's no minimum update level specified at any given time, and if you are experiencing client problems with Microsoft 365 services the first step should always be to check for available updates and, if there are new updates available, apply them to your client installations to see if your problem is resolved.

Once a version of an Office suite or application enters extended support, it is no longer supported for use with the service. Microsoft says that it won't deliberately seek to block or prevent you from connecting with unsupported versions of Office applications, but no bug fixes or other updates will ever be applied to make them compatible with the service, and they always have the option to block specific older client versions from communicating. They also can, and have, deprecated protocols required for older clients, rendering them unable to connect.

Understanding Office Update Channels

Microsoft 365 Apps updates are distributed in what Microsoft now calls *channels*. There are [currently three channels](#), as shown in Table 14-1, and the support lifecycle for feature updates varies between channels. To summarize, the channels are:

- **Current Channel** releases features and bug fixes as soon as they're ready (but at least once per month), with security fixes released on the second Tuesday of each month ("Patch Tuesday") to conform with Microsoft's existing security release schedule.
- **Monthly Enterprise Channel** releases monthly updates on Patch Tuesday, along with bug and security fixes. Microsoft expects most enterprises to use this as the default.

- **Semi-Annual Enterprise Channel** releases updates twice a year (in January and July). Bug and security fixes are released monthly on Patch Tuesday.

In this model, each channel releases fixes and security updates on the same day of the month, each month. The primary difference in the channels is how often feature updates appear.

Channel	Feature Updates	Security Updates	Non-Security Updates and Fixes	Products that default to this channel
Current Channel	When they're ready	Monthly (Patch Tuesday)	Monthly	Visio Pro Project Microsoft 365 Apps
Monthly Enterprise Channel	Monthly, on Patch Tuesday	Monthly (Patch Tuesday)	Monthly	Microsoft 365 Apps
Semi-Annual Enterprise Channel	Every six months, on Patch Tuesday in January and July	Monthly	Monthly	None

Table 14-1: Microsoft 365 Apps Branches and Channels

Whether you use the Office Deployment Tool, the Office Customization Tool, or install from the Microsoft 365 admin center, when you install the apps, they will default to the Current Channel unless you have chosen another default as described below. The Current Channel is suitable for businesses that are willing to have their clients updated to the newest features rapidly (but at least once per month). Typically, these are customers who do not have special macros or Office add-ins that are critical to their business processes. Historically, these automatic updates have not caused major, widespread issues, and can be considered safe to use if you don't have the type of customizations or integrations in your environment that might break after an update. One important issue to keep in mind is that Current Channel release schedules can differ between applications and platforms. For example, Outlook for macOS Current Channel updates are delivered weekly, but Word, PowerPoint, and Excel (for Windows and macOS both) are still generally updated monthly.

There are also preview versions of the Current and Semi-Annual Enterprise channels. The intent of these preview channels is to let you test upcoming releases before they hit the corresponding channels and go into wider distribution. For example, a new feature is first released to Current Channel (Preview), then to Current Channel. Once it meets Microsoft's criteria for a wider release, it will be pushed to the Monthly Enterprise Channel. At some point before the next Semi-Annual Enterprise Channel release, the feature may appear in Semi-Annual Enterprise Preview, so that organizations using the semi-annual channel can test it against their release processes. However, the progress of a feature through these channels may be slowed or interrupted if it fails to meet Microsoft's criteria for usability, functionality, or quality—so just because a feature appears in (say) the Monthly Enterprise Channel in May, there's no guarantee that it will appear in the July Semi-annual Enterprise Channel.

If you have devices configured to use the Monthly Enterprise channel, Microsoft allows you to roll them back to a previous build in the channel. You might want to do this if you find that a Monthly Enterprise change breaks some part of a line of business application, for example. You can also skip an upcoming release. You access both these options from the **Office installation options** page in the Microsoft 365 admin center.

To control which channel a Microsoft 365 Apps installation uses, you can set the channel during installation, by using Intune, by using a servicing profile in the Microsoft 365 apps admin center, or by using the Group Policy administrative templates for Office. Setting the update channel using one of these methods has the advantage of allowing you to change clients to a different update channel than was used during the initial setup or allowing you to target different channels to different parts of your user population without designing a different installation configuration file for each of them. In June 2023, Microsoft began moving any device whose channel was not set through one of these methods to use whatever default channel is specified in the Microsoft 365 admin center. This resulted in some devices changing their update channels to whatever was selected in the **Microsoft 365 installation options** page.

Each update channel has a different period of support. For the Current Channel, support for a build (or release) is only applicable until the next build is released. If a security bug is found in the latest build of the Current Channel, a patch will be released for the latest build, but no patches will be released for any previous builds in the Current Channel. This means that the Current Channel builds are normally supported for one month.

The Semi-Annual Enterprise Channel versions are released every six months, and each build is supported for 14 months. Semi-Annual Enterprise releases that ship in January are supported until March of the next year; the July releases are supported until September of the next year. This [list shows all the build numbers and release dates](#) for Microsoft 365 Apps going back to 2017.

Because Microsoft supports both the current and previous Semi-Annual Enterprise Channel versions, there is no immediate pressure to update when a new version is released to that channel as there is with the other channels. Microsoft recommends this channel only for “those select devices in your organization where extensive testing is needed before rolling out new Office features.” If a security bug is found in today’s version of the Semi-Annual Enterprise Channel, a patch will be released for the latest version and the previous version, but no older builds.

This update cadence and support period for Microsoft 365 Apps are important to keep in mind when you’re planning your update strategy. If you decide to manually control updates, you need to ensure that you deploy new versions promptly and do not let your clients fall into an unsupported state that could put them at risk of a security vulnerability.

With multiple update channels to choose from, you also need to strike a balance between providing a stable version of the desktop applications for the bulk of your user population, while also ensuring that new builds are being tested on a sample of your user population before all users receive the updates. Sometimes Microsoft releases changes that users don’t expect or are not prepared for, and this can cause problems. One example: in August 2023 Microsoft pushed a visual change (including the use of a brand-new default font, Aptos, for all Office applications) to the Current Channel and to all perpetually licensed Office 2021 customers. This change was minor in the grand scheme of things (especially since it had already been released with a toggle that let users try the new appearance), but it’s a good reminder that Microsoft’s reasoning behind pushing changes to users may lead them to send out changes before your users are ready for them.

Microsoft recommends splitting up devices into two broad categories: one (which some Microsoft folks call “general purpose”) that doesn’t normally have or use any applications, macros, add-ins, or other business-critical tools that cannot be allowed to break, and another (“business essential”) set of devices that run line of business applications, belong to key employees, or otherwise need to be protected. You should assign the general-purpose devices to update directly from Microsoft or Endpoint Configuration Manager using the Monthly Enterprise Channel, then keep the “business essential” devices on the Semi-Annual Enterprise Channel to reduce the number and scope of changes you need to adjust to at any given point in time.

Other update channels you should know about: Other teams at Microsoft, including the Windows, Exchange, and Teams product groups, have their release strategies which are broadly like how Office does releases... but there are enough differences that you should carefully examine them to ensure that you’re getting the desired mix of update frequency and stability. In particular, understanding how the [Windows Long-Term Servicing Channel](#) (LTSC) works is critical for organizations that have strict change control requirements.

Operating System and CPU Support

For the most part, Microsoft seems to believe that customers update their computers to the latest operating systems whenever a new version is released, and they act accordingly. In practice, there are [specific requirements](#) for the underlying OS for the full Office clients.

Windows 11, Windows 10, Windows Server 2022, Windows Server 2019, and Windows Server 2016 are all officially supported. There is no blanket requirement for a particular version of Windows 11 or Windows 10, although at any time Microsoft might add dependencies that require a certain OS level for specific features.

For macOS, the three most recent major versions are supported. When a new major version of macOS is released, that major version of macOS and its two immediate predecessors remain supported. With the September 2024 release of macOS 15.0 ("Sequoia"), the Office applications became supported on macOS 14.x ("Sonoma") and macOS 13.x ("Ventura") only. Apple does not have the same predictable release schedule for its OS families that Microsoft does, so the gaps between major releases may be shorter or longer than you expect. Microsoft provides plenty of advance notice of their support requirements, though.

iOS, iPad OS, visionOS, and watchOS follow a similar pattern, but because users of those platforms tend to upgrade at an astonishing rate compared to desktop users, Microsoft only supports *two* previous versions. When Apple released iOS 18 and iPadOS 18 in September 2024, Microsoft stopped supporting Outlook and the other iOS apps on iOS version 16.

As in many other areas, Teams follows its own rules for version support—the Teams client only supports two previous versions of Apple operating systems also, but there has sometimes been a longer grace period. For example, although iOS 16 was released in September 2022, the Teams client continued to support iOS 14 until March 2023.

As a further complication, Microsoft sometimes draws an additional support boundary between a specific version of the host OS and the applications. For example, in January 2021, Microsoft announced that version 16.43 of the macOS apps would be the last supported version on macOS 10.13 and earlier. That is if you have an older Mac that can't run 10.14 or later (and thus can't run the latest release of the Office applications), you won't be able to update the Office apps themselves past version 16.43. In the same vein, in August 2021 they announced the forthcoming end of support for iOS 13 and earlier in the Teams Mobile client. Apple in general does a superb job of supporting older hardware (for example, my 2011 MacBook Pro shipped with macOS 10.6 and was supported until the release of macOS 10.14) but all good things must eventually end.

Microsoft has versions of Word, Outlook, PowerPoint, OneDrive, Excel, and Teams for macOS that are recompiled for the [Apple Silicon](#) CPU architecture. No timeline has been announced for Apple Silicon-native versions of any of the other macOS applications, but these applications run quite well using the Rosetta translator included in macOS 11.0 and later.

Faster Updates Through the Office Insider Program

Microsoft has three programs for those who like to add excitement to their lives by running early, and possibly unstable, versions of software. You've probably run beta versions of software for test purposes in the past; the Windows Insider and [Office Insider](#) programs offer a very similar experience. When you join one of these programs, you'll have access to builds of Windows or Microsoft 365 Apps before they are generally released. When you enroll in the Office Insider program, you'll get builds in one of two additional channels: Beta (formerly known as "Insider Fast") and Current Channel (Preview) (formerly "Monthly Channel (Targeted)"). These channels [generate releases](#) roughly weekly, which means you'll get earlier access to new features but also that you may run into problems with features that don't quite work properly. In exchange for

granting early access to Insider members, Microsoft wants to collect user feedback and bug reports, and they maintain a set of Insider forums for that purpose.

Interestingly, Office Insider exists both for macOS and Windows desktops; there isn't an equivalent for the mobile or web-based Office applications, although Microsoft does occasionally conduct open beta testing for the Office, Word, Excel, PowerPoint, Outlook mobile, Whiteboard, and Microsoft To Do client on iOS and Android.

In addition to a steady stream of small-to-medium feature changes, Microsoft also uses Office Insider for larger changes. For example, the now-standard Outlook for macOS interface was available as a preview for Insiders for several months, as was the "One Outlook" client for Windows (described later in the chapter).

What about the third program? Microsoft runs a [separate preview program and channel set for Teams](#). As with Office Insider, the Teams Public Preview program features three channels: Beta, Private Preview, and Public Preview. The details of these channels, how to join them, and how to manage your Teams Insider membership are covered later.

These three programs join the Targeted Release mechanism (described in the tenant administration chapter). Targeted Release is more about controlling which users receive new features from the *service*, not necessarily from a specific application. However, the [new Outlook client uses Targeted Release](#) as a means of controlling new feature delivery, so if you want to allow (or block) fast feature releases for users of the new Outlook, you do it by controlling who has Targeted Release access.

Installing Microsoft 365 Apps

Microsoft 365 Apps is packaged as a "Click-to-Run" application, using application streaming and virtualization technologies to reduce the amount of time between beginning the installation of the software and being able to start using the applications. Microsoft 365 Apps is included in the Microsoft 365 Business Standard, Office 365 Enterprise E3 and E5 licenses, as well as a standalone Microsoft 365 Apps license (this used to be called Office Pro Plus).

Users May Self-Install the Apps

Microsoft 365 users who have a license for Microsoft 365 Apps can install the desktop applications by logging into the Microsoft 365 portal and clicking the installation link on the top right side of the page.

For macOS users, Microsoft 365 Apps are also available from Apple's Mac App Store. This might seem like a pointless offering, given that licensed users can download the apps from the portal, but it allows organizations using [Apple Business Manager](#) to centralize and manage Office deployments. Just downloading the apps from the Mac App Store gives you read-only access to documents and email; if you want to create or modify documents, or send or receive emails with Outlook, you'll have to activate the apps by signing into the service using an account that has an appropriate license.

On both Windows and macOS, installing or updating the Microsoft 365 Apps package will get you the Teams client too. Microsoft considers Teams to be a full-fledged peer of the other desktop applications and treats it accordingly. If you don't want the Teams client installed, your options are limited. You can block that installation by building a custom configuration using the Office Deployment Tool (as [described here](#)), or you can use Group Policy, or you can allow the installation but use Group Policy to [stop the client from starting](#) when the user signs in. There's no obvious way to stop this behavior in the user interface, but you can control it via a registry or [Group Policy setting](#).

Controlling User Software Installs

You can disable software downloads from the portal for users, which is often preferred by organizations who are using existing software licensing for Office clients, or who want to fully manage the installation process and not allow users to install the software at all.

1. Log into the [Microsoft 365 admin center](#) with your administrator account.
2. Navigate to **Settings**, then **Org settings**, then click the **Services** pivot.
3. Select **Microsoft 365 installation options**.
4. On the **Installation** pivot, choose the user software options you want.
5. Click **Save** to apply the changes.

When users log into the Office portal with their normal user accounts, they'll see installation options based on your selections above. Users must hold local administrator rights on the computer where they install the applications, which is not likely to be an issue in a BYOD environment but may present a challenge for organizations that do not grant local administrator rights to end-users.

Real World: Although your corporate-owned computers may prevent users from installing Microsoft 365 Apps themselves, each license entitles the user to install on up to 5 computers, so if they are allowed to download the software at all, they will be able to log into the admin center from home and install the Microsoft 365 Apps software there.

Managing Desktop Application Updates

Updates to Microsoft 365 Apps can be managed in different ways to suit the needs of the organization. However, Microsoft recommends that you let them do the management by allowing all clients to individually download updates from the [Office 365 content distribution network](#) (CDN). Microsoft maintains multiple CDNs (including one that's used purely for caching web libraries used in Microsoft web applications), but the Office 365 CDN is unique in that it is used only to push application updates for the Microsoft 365 Apps suite and other Office 365 components. Using the Office 365 CDN allows the network and client to intelligently negotiate exactly which updates are required and transmit them as efficiently as possible, as described in [this Microsoft article](#).

Users who install Microsoft 365 Apps from the Office portal will find that their clients' updates are automatically downloaded from the internet and installed as they are released by Microsoft, and no other action is required by the end-user other than restarting applications when prompted that an update is ready.

If you've deployed the applications using ODT, then the XML configuration file you used will determine how updates are applied by enabling updates and configuring an update path. If you want your clients to automatically update themselves using the Microsoft 365 Apps update behavior, you'll have to re-run the Office Deployment Tool for Click-to-Run to download the latest build of Microsoft 365 Apps to the appropriate location on the network. Once the updated build is available in the update path your clients were originally configured with, the computers will automatically apply the updates.

Many enterprises prefer to use Microsoft Endpoint Configuration Manager, System Center Configuration Manager, or other similar tools to provide them better control over the operating system and application updates. When Microsoft releases updates to the Microsoft 365 Apps suite, they also release installer packages that can be deployed using these types of tools. Keep in mind that if you're using the Current Channel, Microsoft will be releasing updates at least once per month... and they only support the current version of each application against the service, meaning that if you're managing updates yourself you may wish to force your clients to use the Monthly or Semi-Annual Enterprise channels.

If you need to disable automatic updates completely, the ODT XML configuration file you use must specify the exact build number of Microsoft 365 Apps that you want to install. If automatic updates are disabled in your XML file, any new builds that you download using the Office Deployment Tool for Click-to-Run will need to be manually deployed to end-user computers.

Peer-to-Peer Delivery Optimization

Peer-to-peer update delivery can reduce the amount of time required to deploy updates throughout a large organization. Apple and Microsoft have used this technology for some time for operating system updates. The basic idea is that one client on a network downloads the updates, then caches and redistributes them to other nearby computers on the same network. Compared to having every computer download updates from a CDN over the internet, peer-to-peer delivery (which Microsoft calls [Delivery Optimization](#)) promises to speed deployment significantly when implemented properly.

The good news is that, by default, Windows 11 computers automatically use Delivery Optimization for OS updates, and when you install Microsoft 365 Apps, so will those applications *if* the prerequisite requirements are met:

- The client device must be running a supported build of Windows 10, or any version of Windows 11.
- If you want users to be able to request updates (by going to the application backstage and using **Account > Update Options > Update Now**), the client device must be running Windows 10 build 1908 or later.
- You must have version 1912 or later of Microsoft 365 Apps. That version was released in January 2020, so you should certainly already have it.

Keep in mind that Delivery Optimization only works with computers that are configured to download their application updates. If you're using Microsoft Endpoint Configuration Manager or another distribution-management tool, the client applications won't use it.

If you want to check whether an individual Windows device is using Delivery Optimization, you can use the `Get-DeliveryOptimizationStatus` and `Get-DeliveryOptimizationLog` PowerShell cmdlets. Microsoft has lots more [documentation of the Delivery Optimization feature](#) available if you're interested but, in general, most Microsoft 365 administrators can ignore the feature and let it work silently in the background.

Managing Updates for MSI Builds of Microsoft 365 Apps

The update mechanisms and Channels described so far apply only to the C2R versions of Office. Licensed Microsoft 365 customers also get access to the traditional MSI packages for Office client deployment. If you use these MSI packages, you'll need to manage updates yourself using tools such as Microsoft Update, Windows Server Update Service (WSUS), System Center Configuration Manager (SCCM), or the Microsoft Endpoint Configuration Manager.

For C2R clients, all update types are released at the same time on the second Tuesday of each month, also known as "Patch Tuesday." The MSI clients are handled differently. Non-security updates are released on the first Tuesday of each month, while security updates remain on the second Tuesday of each month.

MSI deployments are still widely used by customers for a variety of reasons, but update management is more complex and time-consuming because you must do it all yourself with whatever deployment tool you're using. As with so many other aspects of cloud services, if you want a higher degree of control, you can get it, but at the cost of increased overhead and inconvenience. For your client deployments, consider the C2R service as your first choice, and only revert to the MSI package if you have a good reason to. It will save you time and effort overall that can be better spent elsewhere.

Managing Updates for macOS Versions of Microsoft 365 Apps

You can get the macOS versions of the Microsoft 365 Apps suite by downloading them from the Office 365 portal, or Apple's Mac App Store. In both cases, you'll find that Microsoft has an app update mechanism operated by the Microsoft AutoUpdate (MAU) application. MAU is automatically installed when you install any of the Microsoft 365 Apps family; it runs periodically to download and install updates to the component applications, or you can trigger it manually by choosing **Help > Check for Updates** from the apps. The MAU app uses the same Office 365 CDN that Windows does, just with a different set of update bits. Interestingly, Teams client updates for macOS are delivered through MAU, as well as through the normal Teams app self-update mechanism. The Intune Company Portal app is likewise automatically updated through MAU.

Edge WebView2 and Office Apps

Many parts of the desktop Office applications create or display web-compatible content. Some of the features you use in Outlook, for example, aren't built into the Outlook desktop client, but are instead loaded from a different Microsoft service and rendered inside Outlook. Examples include the Meeting Insights view and the room finder view. These components are called OWA experiences (OCX) and use an Edge component called WebView2. The Outlook "Monarch" client also uses WebView2, as does the Teams client.

Microsoft loads the WebView2 component onto PCs through:

- The Edge browser.
- The Microsoft 365 enterprise apps.
- Windows 10 and Windows 11 updates.

After deployment, a program called Microsoft Edge WebView2 Runtime (msedgeview2runtime.exe) is available on a PC. You can manually install the runtime in advance if you want to, or you can prevent it from being installed by changing a setting in the Apps admin center (both operations are [described here](#)).

Managing Support for ActiveX Controls

Microsoft first introduced [ActiveX controls](#) in 1996, and they have been causing security problems since then. The idea of having individual components that you could reuse in different web pages or documents seemed like a good idea, but in practice it was riven with security issues. Office documents can contain ActiveX controls; the controls are loaded when the document loads and execute when the user interacts with them. The Office 2024 LTSC applications will default to blocking access to ActiveX controls; users will still see the controls in their documents but can't add new objects or interact with existing ones. This blocking default will apply in the Office 365 Apps for enterprise versions starting in April 2025. In both cases, previously created documents that have ActiveX control will still load, but the user will see an infobar telling them that the control is blocked. Users can unlock the controls themselves with the [settings in the Office apps Trust Center](#), or you can do so as the administrator.

If you need to change this default, you can:

- Teach users how to use the **Prompt me before enabling all controls with minimal restrictions** option in Trust Center for the applications they need to use;
- In the registry of any targeted machines, create a new REG_DWORD value called DisableAllActiveX at HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Security and set its value to 0.
- Use the Office Group Policy templates to set the DisableAllActiveX setting to 0.

Troubleshooting Office Clients with SaRA

Although Microsoft 365 is a very reliable service, there will naturally be problems that occur from time to time. Part of that is due to the scale and complexity of the service; it is impossible to keep that much software and hardware in 100% healthy condition all the time. Part of it is also due to factors outside of Microsoft's direct control. A large proportion of the support calls that Microsoft receives are client issues that are due to the software on the computer, network issues, DNS issues, or other factors that can be difficult to identify quickly. The more time Microsoft spends supporting these types of issues, the costlier it is to run the service.

That's why the [Support and Recovery Assistant](#) (SaRA) exists. This downloadable troubleshooting tool has a wizard-driven interface to allow users to identify the issue they are experiencing, and then allow SaRA to perform diagnostic tests and suggest solutions to the most common client-side issues. SaRA can check for issues around mail flow, access to shared mailboxes and calendars, Outlook freezes, and repeated authentication prompts. Although it doesn't exhaustively test for every possible cause, it's still a useful tool. In May 2021, Microsoft added a [new command-line version of SaRA](#), which is useful for enterprises that want to allow technicians to remotely diagnose Office problems.

In the tenant management chapter, you read about the network health monitoring features in the service. Microsoft extended SaRA to share its network discovery results with that feature. When you run SaRA on a user workstation, its [network test results](#) feed into the network health monitor, just as if you ran the connectivity test manually.

SaRA requires administrative rights on the computer to be able to install the software and run the tests. For BYOD users or environments where local admin rights are given to end-users, this won't be a problem. However, you can also imagine that the existence of SaRA may not be known to end-users who do not have an IT focus. They're likely to call Microsoft for support anyway, but if they were to try to raise a support ticket using the admin center SaRA can be suggested to them automatically as part of that process. For customers with IT support staff, it is a simple matter of the IT personnel installing the tool on client computers and running the diagnostic tests.

It's easy to think that Microsoft should just provide working support tools like this to customers. And indeed, with all the data they have from telemetry and from analyzing support trends, Microsoft can make reasonable guesses about the most useful diagnostics to develop for SaRA. That said, it's important that customers and IT professionals provide feedback to drive the development of tools like SaRA, by letting Microsoft know when the tools don't have any information about our problems, or when they fail to detect and suggest fixes for issues. To that end, SaRA has multiple places where feedback can be submitted to Microsoft.

Using the Microsoft Apps Admin Center

Traditionally, there have been several ways of enforcing Office client configurations: you could build a custom installation of the MSI version, you could use the Office Configuration Tool to specify a configuration applied with the installer, or you could specify a configuration template and push it to clients using Group Policy or another similar configuration management tool. This latter method is probably the most common approach, but it has a significant limitation: the target machines must be able to apply Group Policy settings. For devices that are only joined to Entra ID, or for BYOD-style devices that aren't joined to any directory, there was no good way to enforce or change client policy settings. As an alternative, Microsoft offers a suite of cloud-based tools for managing Microsoft 365 Apps clients, the Microsoft Apps Admin Center (<https://config.office.com>). You can use this admin center to manage several aspects of the Microsoft 365 Apps deployed to your end-

users without MEM, Office 365 MDM, or Group Policy objects. Currently the Apps Admin Center is available worldwide, except for Office 365 GCC, GCC High, Office 365 DoD, and Office 365 operated by 21Vianet.

The combination of desktop applications delivered by a cloud-based content delivery network and then managed by a cloud-based service is interesting and offers several potential benefits to customers. For now, the Apps Admin Center contains six items in its left navigation bar. Note that some of these services are marked as being in preview):

- **Cloud update** (formerly known as "Servicing") allows you to create and manage servicing profiles. Earlier in the chapter, I mentioned Microsoft's recommendation for creating "business essential" and "general purpose" device sets—you can follow this recommendation by creating servicing profiles, assigning devices to them, and then assigning update channels to them. You can define profiles that exclude devices based on the amount of free disk space they have, whether Office application macros have been used in the preceding 28 days, what channel they're currently in, and whether they have Office add-ins installed. Each profile can have exclusion dates, during which devices in the profile won't receive any updates. You can also deactivate cloud update for the Monthly Enterprise and/or Current channels; Microsoft hopes that the ability to turn cloud update off for those channels will encourage customers to switch to cloud update instead of having each client update its own local installation.
- **Customization** contains tools that allow you to define and deploy custom configurations and policies for the Office apps.
- **Health and Inventory** allow administrators to monitor which applications are installed, whether they are healthy, and whether they are receiving updates as you expect—read on to learn more.
- **Learn More** is a collection of links to documentation, videos, and so on that may be useful as you learn to manage your Microsoft 365 apps using the Apps Admin Center.
- **Setup** has very little in it; it contains a control for generating what Microsoft calls a tenant association key (a base-64-encoded key that lets you tie devices in a specific tenant to your portal) and a slider that allows you to adjust how long the tool will remember devices that haven't updated their inventory data (the default is 30 days).

Microsoft is in the midst of an extensive set of changes for the Apps admin center. Because they are rolling these changes out in phases, I'll summarize the changes here, and as they make progress, the updated names and links will be rolled into this chapter:

- Servicing profiles are being renamed to Cloud Update, as noted above. Until you enable Cloud Update, you'll see a card on the main page suggesting that you do so. Once you do, you'll see a Cloud Update summary card on the home page.
- Some settings, such as 'Exclude Groups' and 'Exclusion Windows,' will be moved from the settings tab to the 'Tenant Settings' tab in the Updates Overview page under Cloud Update
- Some of the previous device selection controls have been deprecated. You will only be able to select or exclude by putting devices in Entra ID groups and then using the 'Exclude Groups' capability.
- A new Update Validation feature gives you tools for validating newly released updates before you blast them out to your entire tenant. By creating multiple "waves" (or sets of devices to which updates should be deployed), and deploying to those waves in graduated stages, you can gather statistics on the success of the updates and their quality before proceeding with the delivery. This feature is currently in public preview, with additional functionality for validating Office add-ins promised as a private preview in calendar 2024.
- The Inventory page will get an additional column called "Cloud update status" that indicates whether this device is currently updated by profiles.

Customizing Microsoft 365 App Configurations

Some organizations are happy to allow users to install local copies of the Microsoft 365 Apps packages. Others want or need centralized control or have constraints that make it impossible or impractical to install using the normal process of launching the small bootstrap installer and letting it download the required software over the Internet. Fortunately, the setup files can be downloaded in advance and then distributed through a network share or other means to avoid a dependency on the Internet connection. In addition, you can customize exactly what parts of the Microsoft 365 Apps suite are downloaded, where they are installed, how they're configured, and several other settings. To do this, you'll use two tools:

- The [Office Deployment Tool](#) (ODT) is a command-line tool that you run to apply a configuration file (formerly known as a transform) to the installation files. The result: the settings specified in the *configuration.xml* file drive the installation.
- The [Office Customization Tool](#) (OCT) is now part of the Apps Admin Center, under the **Customization** section in the left nav bar. The OCT provides a web-based tool for creating and modifying configuration files to be used with the ODT. You can also create a configuration file and then apply it to existing installations (as you might wish to do if you don't want the Teams client to auto-start).

You can find a full reference for how to customize the XML configuration file on the [Microsoft Support website](#). However, Microsoft recommends that you use the OCT to avoid making mistakes in XML formatting that will cause your installation to fail. In addition, OCT allows you to upload and store configuration files in the cloud, making it easier to keep track of them.

Normally you'll use these tools by following a process like this:

1. Install the ODT. That will give you two files: *setup.exe* and a sample *configuration.xml* file.
2. Navigate to <https://config.office.com> and either create a new device configuration from scratch or modify an existing configuration. It's a good idea to create a new configuration every so often to verify that you are taking advantage of all available settings in the OCT; Microsoft occasionally adds new features that may not be included in your older configuration files.
3. Test the configuration file to verify that it does what you expect, and that the resulting installation is set up the way you want it.
4. Use OCT to adjust the configuration file as required.
5. Once you're happy with the results from your configuration file, use the ODT to complete the installation.

You can run the ODT to complete the installation using any tool that can execute a command-line program. This includes almost every endpoint-management tool out there, plus Group Policy, plus even having users run the command themselves from a desktop shortcut you've previously deployed.

Real-world: If your environment doesn't provide good Internet connectivity, you might want to host the installation files on your internal network. You can do so using a conventional network share, a DFS share, or even removable media. To install in this manner, you'll need to run the ODT with the */download* switch to download the files. To do this, after customizing the XML configuration file, copy it to the same folder that you placed the *Setup.exe* file in. Open a command prompt on a computer on the network and run *Setup.exe* with the */download* switch to download the Microsoft 365 Apps source files.

```
C:\> start /wait \\obcdc1\installs\Office365ProPlus\setup.exe /download \\obcdc1\installs\Office365ProPlus\configuration.xml
```

The source files will be downloaded and placed in a folder structure automatically. Do not change or rename the folder structure created by Setup. After the download is completed, you can deploy the apps

from the install point by running *Setup.exe* with the */configure* switch. You can also run this command line using software deployment tools such as Group Policy or Microsoft Endpoint Configuration Manager.

Pay close attention to the "Product ID" that you configure in your XML file. The correct product ID must be used for the Microsoft 365 license assigned to the user. If the wrong product ID is installed on the computer, the user will not be able to activate it with their Microsoft 365 credentials and will need to reinstall the correct version. You will normally use a value of O365ProPlusRetail for most product SKUs (except Visio and Project, which have unique product IDs). Microsoft publishes a complete list [of product IDs matched to license types](#).

If you do not specify an update channel in your configuration file, and none is specified via Group Policy, the default branch or channel will be used (refer to the earlier section about Update Channels).

A [tutorial and sample PowerShell script](#) are available to help in deploying Microsoft 365 Apps using GPOs.

Real World: If you've already purchased licenses and provisioned Microsoft 365 accounts, you can begin your client deployments before you start moving mailboxes and other data to the cloud. The client applications can connect to on-premises servers such as Exchange, within the limits of the normal client system requirements for those on-premises products. Outlook is generally smart enough to automatically deal with mailboxes that have been moved from on-premises servers to the cloud without user intervention.

Creating and Managing Application Policies

The Apps Admin Center includes the Cloud Policy service (formerly known as the Office cloud policy service, or OCPS). You use Cloud Policy to define policies that are applied from the cloud to desktop Office applications (**Customization > Policy Management**). In its current release, it doesn't support all the policy settings available through Group Policy templates, although it does have a *lot* of settings (for example, there nearly 300 individual policy settings just for Microsoft Word and more than 2,200 policy settings in total)! Perhaps more importantly, the Apps Admin Center only allows you to set up user-based policies, whereas with GPOs you can apply Office policies to machines.

Note: The only Teams-related policies currently implemented in the Apps Admin Center allow you to prevent the Teams client from starting automatically on Windows machines or to restrict which domains Teams may sign into. If you want to control other aspects of Teams client behavior, you'll have to use the Teams policies described in the Teams management chapter.

Cloud Policy settings are applied to the applications in a way very similar to how Group Policy settings are applied. When a user signs into Office 365 on a device, the application she signs into immediately checks the Cloud Policy service for any applicable policies. If no applicable policies are found, the application checks again every 24 hours; any time a policy is found and applied, the application will recheck for policy changes every 90 minutes while the app is open. Each time a Microsoft 365 App is launched, it will check for policies (this includes Visio and Project, but not Power BI or To Do). It is important to understand that policy changes are not applied until the app is *next* restarted though—so if a user launches Outlook at 8 am, and you update the policy at noon, the new policy will be downloaded but not applied to that user until the next time she launches an Office application.

The Policy Configurations page in the Apps Admin Center shows which policies you have defined, their relative priority, and the scope to which they apply. Microsoft used to show a policy health indicator, but they deprecated that feature and promised, per MC335282, to replace it with "advanced health reporting and compliance monitoring features", which they haven't done quite yet.

Creating a policy using this toolset is very simple: you add the new policy, give it a name, select the users it should apply to, and then select one or more policy settings to apply. The **Configure Settings** blade of the policy management tool lists all the settings available, but you can search or sort them. Of note, the **Area** column allows you to quickly find policies that Microsoft recommends either as part of the [security baseline](#) or [accessibility baseline](#) for Office applications. There's no way to automatically apply the full set of baseline policies to your clients, so if you want to use them, you'll need to create policies and then manually choose the baseline items you want to include.

To use the service, you need version 1808 or later of the Microsoft 365 Apps suite, and the users you want to target must all have accounts that are either homed in or synchronized with Entra ID. You assign policies to users based on their group memberships, so you'll need to create groups for whichever sets of users you want to assign policies to. You can also create a policy that applies to anonymous users who read or edit documents using sharing links sent by users in your tenant.

Audit records for changes made to the policy set in your tenant (including adding, removing, or renaming policies, or changing their settings) appear in the Purview audit logs.

Managing User Feedback Policies

For a concrete example of a policy that you can manage with the Apps Admin Center, consider the user feedback mechanism described in the user management chapter. There are [six policy categories](#) that let you control whether and how users may submit feedback, including free-text comments and surveys, to Microsoft. Individual policies control whether users may attach screenshots or attachments to feedback, whether they are allowed to submit log files and content samples, and whether Microsoft is allowed to follow up with individual users on their feedback. These Cloud Policy feedback policies are enabled by default.

From August 2024, Microsoft began moving control over in-app feedback for Teams to OCPS policies and is deprecating the use of Teams feedback policies from the teams admin center. Until this change is complete (not yet completed by October 2024), you will need to make any changes you want for Teams feedback submission both to the Teams feedback policy and in Cloud Policy. As part of this change, Microsoft updated the Teams user interface for feedback management to match the other Office 365 applications. There's now a **Feedback** menu under **Settings and more** and a new form to submit feedback.

Managing Office Macro Policies

Perhaps Office macros are a better example. These have long been used by attackers as a quick and simple way to sneak malware onto target machines. Microsoft introduced a feature colloquially known as "mark of the web" (MOTW) that labels downloaded programs and documents as having come from the big bad Internet; Windows and Office can use MOTW to apply extra scanning, or to block content. To provide better security, Microsoft decided to completely block Office macros in files tagged with MOTW. After announcing this change in February 2022, they got a lot of feedback, all negative, which led to them pushing it back (and forth, and back again) until full deployment began with the July 27, 2022 release of [version 2206 to Current Channel](#). Organizations which had previously used the Cloud Policy service to apply a policy to block macro content in Office documents would have been spared all this back-and-forth flapping.

Managing Desktop Application Access

To control the public preview of the Loop desktop application in April 2023 Microsoft used the Cloud Policy mechanism in a new way. Before people can use the Loop desktop application, you must [create a policy](#) to allow its use, including creating (or repurposing) a security group to define who's allowed to use it and then applying the policy setting. This approach continued with the GA release of the Loop application in November 2023, marking an interesting change from the way the other Microsoft 365 apps for business work. In fact,

[access to all of the Loop workspace features](#) is controlled by use of Cloud Policy. In the same vein, you can prevent users from toggling to the New Outlook via Cloud Policy.

Monitoring Application Health

The **Health** section of the Apps Admin Center contains four sections:

- The **Apps Health** section is meant to show you data about individual machines' applications and how healthy they are. You'll only see data for users who have an E3, E5, or equivalent license, and only if they are running version 2008 or later of Microsoft 365 Apps for Windows. The **Add-in Health** pivot shows the health of COM and VSTO add-ins for Office if the add-ins came from public sources. Note that this pivot will only appear if you've enabled inventory collection.
- **Security Update Status** shows you which machines are behind on security updates for the Microsoft 365 apps (not general Windows Update updates, sadly). This is based on the release date of the most recent Microsoft 365 apps security update; the [most recent update](#) was September 10, 2024, so any device that doesn't have that update will be marked as "not up to date". You can set goals for the percentage of devices you want to be up to date or the average time between patch release and deployment; these are useful to track.
- **OneDrive Sync** shows reports and data about the sync health of OneDrive for Business clients on Windows and macOS, including how (or whether) the [known folders sync feature](#) is enabled, and how many clients have reported sync errors, and an aggregated view of issues by type. You must [enable reporting of OneDrive health data](#) by the clients in order for these reports to work.
- **Service Health** shows you whether the Microsoft 365 Apps portion of the Apps Admin Center is itself healthy.

There's a lot of potential for Microsoft to improve and extend the features of this section of the Apps Admin Center, including linking "who's not up to date" lists with the policy tools, or a notification mechanism, to help automatically notify users and/or bring their machines into compliance.

Inventorying Your Application Estate

Keeping track of which devices have which versions of the Microsoft 365 apps on them is an enduring hassle for many Microsoft 365 customers. This hassle is magnified if you don't have a solution such as Microsoft Endpoint Configuration Manager running; as individual machines can freely self-update, you can quickly end up with a confusing mess of different versions spread across your tenant. The **Inventory** section of the Apps Admin Center is intended to help address this by summarizing which devices, which builds, and which add-ins are present in your tenant. There's a new client-side component of Office known as the Serviceability Manager (SM) that gathers this data and provides it to the service. SM only starts collecting this data after you do two things. First, you must sign into the Apps admin center, and second, you must accept the onboarding prompt. Once you've completed both of those tasks, SM will start gathering data and passing it to the service and you'll see it appear.

Each of the sections in the inventory report (Figure 14-1) has links that allow you to see more detailed data. For example, the "Show all devices" link in the Devices section will show whether each device has macros or add-ins, what Office version and build it's running, what update channel it is on, and so on.

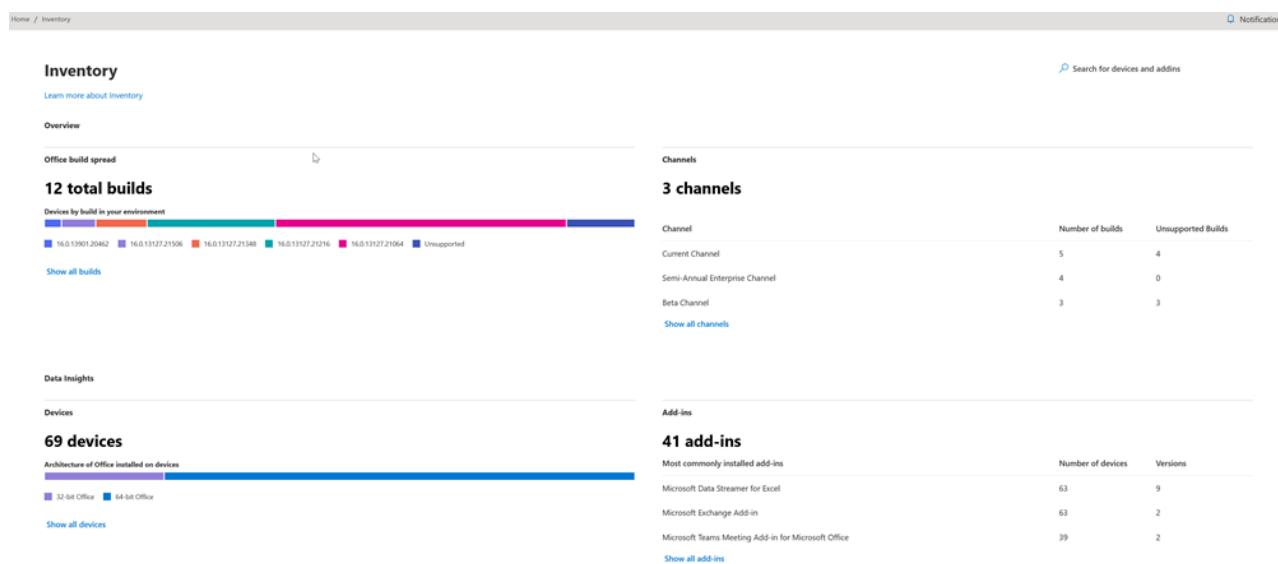


Figure 14-1: An example application inventory

Managing the Outlook Client Family

Outlook is still the most common desktop email client used to access both on-premises and cloud Exchange mailboxes. It's also arguably the most important of the clients, and it's fair to say it has the broadest set of management features (in part because those management features are spread across several parts of the service). Microsoft is trying to create a unified user experience and identity for Outlook across multiple platforms, which can lead to some confusion when discussing "Outlook" in books like this. (In fact, they go so far as to [say that](#) "One of the Outlook design principles is to make Outlook feel native to your preferred operating environment"). Despite that confusion, we'll tackle managing the Outlook client family as a single topic. The family currently includes several members:

- Desktop Outlook, available for both macOS and Windows. There are [some differences in the functionality](#) between the two clients, and of course, there are differences between different versions, but in general, you can consider the two as equivalent. Both OS platform versions support multiple Exchange Online accounts in a single client session; both can work online or offline, and both offer extensive caching features. In this chapter, when you see a reference to "Classic Outlook," that refers specifically to the Win32 version of Outlook. Starting with Office version 2407, the Win32 version of Outlook became "Classic Outlook" and its icons, window titles, and so on say "Outlook (classic)" to reflect the name change. Microsoft has committed to support Outlook classic until 2029.
- Classic Outlook for Windows will eventually be replaced by what has been called "New Outlook" and, before that, "One Outlook" or "Monarch". New Outlook is an ambitious effort to replace the Windows, web, and macOS clients with a single unified codebase. It's currently available only for Windows, though Microsoft has promised it will cross platforms. In this chapter, when you see a reference to "Outlook" with no "classic" in front of it, this is the version we're talking about.
- Outlook Web App (OWA) is the webmail interface for Exchange Online, providing users access to their mailbox, calendar, contacts, and tasks, as well as a launch pad for other services such as the Office Online apps, OneDrive for Business, SharePoint sites, Delve, and Stream. Although Microsoft officially refers to "Outlook on the web," this is a clunky name, so we won't use it, especially as most documentation for the product still refers to "OWA".

- Outlook mobile for iOS and Android is Microsoft's first-party mobile client for Exchange Online. It adapts the Outlook user experience to the smaller screens and touch-based interface of mobile phones and tablets, and it includes some mobile-only features such as Play My Emails (a voice-based system that will read your emails to you and let you respond via a connected Bluetooth or wired headset). As with the macOS-vs-Windows split, you'll find that features come to the Android and iOS versions of Outlook at different speeds. (In August 2022, Microsoft started rolling out an "[Outlook Lite](#)" version intended for older Android devices that don't have either enough horsepower or a recent-enough OS to run the full version.)
- A [sidebar app for Edge](#); when enabled, this puts a slimmed-down version of OWA into a panel on the right side of your browser window, alongside whatever content is in the primary content region.

Real-world: Classic Outlook performs best when you configure it to use cached mode to connect to Exchange Online. In this configuration, you can decide how much of the server copy of the mailbox Outlook should keep locally on the user's computer for faster access. The local cache is known as the OST file and is on the hard drive of the user's computer in a default folder path within their local profile. You can use a slider control in the Outlook account settings to manage how much of the mailbox Outlook synchronizes to the OST file so that you can balance the availability of data and storage consumption. For instance, many users find that keeping the last year's email in the OST is the right balance. Outlook for Mac uses a similar approach to cache mailbox contents on the local drive; it uses a file very similar in concept to the OST file, but with a different structure. Unfortunately, there's no equivalent of the Outlook for Windows slider control, so you can't regulate how much email is synchronized with the client. This is a long-standing, and popular, feature request that Microsoft will hopefully get to sometime soon.

Features become available for the main flavors of Outlook at different times and in an unpredictable order. For example, Microsoft first developed and released "dark mode" for OWA, then rolled it out to macOS users, then to Classic Outlook customers who were on the old Monthly Channel (Targeted)... after which the Outlook mobile team released their dark mode implementation. While there are certainly exceptions, it's fair to say that *most* new features come to OWA first. The individual versions of Outlook have a pretty high degree of independence for feature releases; in general, it seems that new features that require changes to the back-end services in the substrate usually appear first in OWA but that the mobile and desktop versions freely introduce UI-only changes on a more frequent schedule. Overall, the principle Microsoft's trying to apply is that the user experience for its multiplatform applications should be as consistent as possible whilst still fitting into the design language of the host platform—but those underlying implementation choices are to be minimized in favor of giving users a consistent *Microsoft-centric* experience on whatever device they're using. Common UI elements, affordances, color schemes, and so on are the vehicle Microsoft uses to deliver this consistency—if you look at the UI of OWA on Edge, classic Outlook, Outlook for macOS, the new Outlook, and Outlook on iOS side-by-side, you'll notice the consistency.

When it comes to managing Outlook, it's important to differentiate between managing settings on the client (such as whether certain features are enabled or disabled on the client) versus managing them at the tenant level versus managing them at the mailbox or protocol level. For example, you might (and probably should) disable IMAP4 and POP3 in your tenant but that wouldn't necessarily stop an individual user from connecting Outlook using those protocols to another mailbox in another tenant (or another service). Several of the newest features added to Outlook in late 2020, for example, are integrations with Cortana-powered services for things such as word suggestions. You may be able to control those features at the tenant level but there is no separate policy or setting that allows you to control the features' availability in Outlook itself.

Classic Outlook for Windows

The C2R version of Outlook for Windows is almost always delivered as part of a Microsoft 365 Apps installation. There are several ways to manage its behavior:

- Policies defined in an Office administrative template and distributed via Group Policy to domain-joined clients.
- Policies defined by the Office Client Policy Service and distributed when the client connects to the service.
- Local customizations made through the Windows registry.
- Local customizations made directly through the Outlook settings interface. These changes typically apply to the user's profile and thus only impact the specific user for whom the customizations are applied.

For the most part, the first three of these management techniques have an identical effect. Which one you use will depend on the infrastructure you deploy. User-specific customizations are a bit tricky, though, because they are usually chosen by the user herself, and users can be *very* protective of their customizations.

Outlook for macOS

Microsoft has long shipped a version of the Outlook client for macOS. It's never quite had feature parity with the Windows version, though, even though the promise of a single unified client looms. More so than the other Office desktop applications, Outlook for macOS takes advantage of macOS features, including summary desktop widgets, [support for focus profiles](#), integration with the native OS search mechanism, and so on.

Outlook is also available through Apple's macOS App Store. [Users can use Outlook for macOS without buying an Office 365 license](#)—the client's freely available for use with Microsoft accounts, Office 365, iCloud, Google, Yahoo! Mail (remember them?), and IMAP accounts. This is an interesting strategic move since it seems to be an attempt to shift users away from the provided macOS mail and calendar clients even if they aren't subscribing to the full Office suite. It remains to be seen how well this will work.

New Outlook / One Outlook / Monarch

We already have a single Outlook client for macOS, Linux, and Windows—it's called OWA. But, for a variety of reasons, not every user wants to, or can, use a web-based client for their everyday work. Microsoft has recognized this, but at the same time they have the quite reasonable desire to consolidate on the smallest possible number of unique client versions. First announced in late 2020, and first released in preview in May 2022, "One Outlook" is intended to satisfy both users who want a desktop client and Microsoft's desire for consolidation. Now users on Current Channel for Windows or the Semi-Annual Channel who have supported account types (currently Office 365, Outlook.com, Gmail, iCloud, Yahoo, or IMAP accounts) will see a toggle in the upper right of the main Outlook window labeled 'Try the new Outlook'; flipping that toggle will switch them to what Microsoft is now officially calling "the new Outlook."

Before we proceed, it's important to understand Microsoft's plans for releasing New Outlook. These plans have evolved over time as users have given very clear feedback about their attachment to Classic Outlook, and on the deficiencies in New Outlook.

For consumer users who aren't using Classic Outlook, New Outlook has already [replaced the Windows 11 Mail, Calendar, and People clients](#). New Windows 11 devices ship with Monarch as part of the base OS. On December 31, 2024, Microsoft will remove the Mail & Calendar applications from the Microsoft Store. In addition, Microsoft has already added Monarch to the Windows Store and made it visible in the Windows Search interface. That means that Office 365 users have two additional ways to discover and use Monarch.

For business users (that is, users who have an Office 365 license that includes access to Classic Outlook), Microsoft is planning four phases of deployment for New Outlook:

- Opt in: during this phase, individual users may opt in to using New Outlook. Each classic Outlook user sees the “Try the new Outlook” toggle on the top right side of the Outlook window. If users need features or workflows that are not available yet in the new Outlook, or just don’t like it, they can toggle back to classic Outlook for Windows. There have been some reports of problems with profile corruption from frequent switching. Each time a user toggles back to classic Outlook, Microsoft will ask them to give feedback on their experience with New Outlook.
- General availability: this isn’t a phase per se; it’s a milestone. When New Outlook officially went GA on 1 August 2024, it became fully supported as part of the Office 365 suite, meaning that enterprise customers will be able to get the same levels of support they do for other Office 365 applications. Microsoft will continue developing and releasing features after GA, which is a good thing—as of the GA date there were a fairly large number of significant features in the Classic client that aren’t in New Outlook.
- Opt out: sometime after GA, the opt-out phase will start. [Microsoft says](#) that they’ll start the opt-out phase “once a period for feature capability development and quality assessment has passed.” At minimum, Microsoft has promised a 12-month period between the announcement of when the opt out period will start and its actual enforcement, so you’ll have time to prepare. Tenant administrators will be able to opt in to the opt out phase to give their users an earlier transition if they wish. Once the opt out phase begins, users will automatically be switched to New Outlook. They will still be able to switch back to Classic Outlook.
- Cutover: in this phase, users will no longer have access to Classic Outlook, although it will remain supported “until at least 2029” according to Microsoft. This phase will also be announced at least 12 months in advance, and administrators will be able to enter this stage early if they choose to do so.

The new Outlook for Windows [allows users to add their personal Gmail or Outlook.com accounts](#) to their Outlook profiles. Some organizations block personal email accounts on work devices, but it’s apparently not possible to do this with the new client just yet. Microsoft’s plan seems to be to allow you to use any number of Microsoft 365, Outlook.com, and Gmail accounts together, if you have at least one account that has an Exchange Online license that supports desktop Outlook. Microsoft’s [licensing documentation](#) says that “the primary account [*i.e. the first account you add during setup*] will now also be used for determining the license that applies when adding additional secondary accounts.

Finally, keep in mind that the new client’s features are still evolving, and will be for some time to come. For example, in September 2024 Microsoft started rolling out a change that allows users to submit diagnostic logs when reporting a problem to Microsoft support (see MC869930). There is still a large functionality gap between Monarch and Outlook classic.

The earlier discussion about WebView2 is important for Monarch because some parts of its functionality are enabled by a technology known as OPX (“OWA Powered Experiences”). Just as desktop Outlook embeds the OWA room finder in a separate subpane instead of duplicating its functionality, OPX allows Monarch to consume features originally developed for OWA. That’s one big reason for the list of things that Monarch supports or doesn’t—it’s easier for Microsoft to plug in OWA features using OPX, so those features, in general, were the first ones delivered.

Blocking New Outlook

For now, you have three ways to control user access to New Outlook. First, you can disable the ability for users to switch themselves to New Outlook with a [registry key](#), through GPO, or through the Cloud Policy service

(look for the “Hide the “Try the new Outlook” toggle in Outlook” policy setting). If you don’t block this setting, your users may switch themselves to Monarch at any time. Be prepared for questions about differences in appearance and features when they do.

Second, you can block users who already have New Outlook from accessing their mailboxes with it by using the `Set-CASMailbox` cmdlet. If you do this, be aware that this does not stop users from toggling to the new experience, it just prevents the new client from connecting to the target mailbox. Here’s an example of disabling access for the user Kim Akers:

```
Set-CASMailbox -Identity Kim.Akers-OneWinNativeOutlookEnabled $False
```

Finally, OWA mailbox policies (described in the next section) also support the `OneWinNativeOutlookEnabled` flag, so you can use them as described below to enable or disable access to the new client. Whether you use `Set-CASMailbox` or OWA policies depends on how you currently enforce mailbox access policies today.

Forcing Migration to New Outlook

[Microsoft offers a policy that allows administrators to force user migration](#) from classic Outlook to new Outlook. The migration process has three steps:

1. Users see a “Try the new Outlook” toggle and a pop-up callout with a button labeled “Try it.” If they use the toggle or the “Try it” button, they get switched to the new Outlook.
2. If they ignore the toggle and pop-up, the next time they run Outlook, they get an infobar message that reads “Your organization recommends using the new Outlook for Windows. If you skip this now, you’ll be taken to the new experience the next time you start Outlook.”
3. If the user *still* doesn’t take the bait, the next time they launch classic Outlook, they’ll get a modal dialog with two buttons: “Switch now” and “Switch next time.” Users can continue to click “Switch next time” each time they launch Outlook.

As an administrator, you can start this process by using the Cloud Policy service to enable the “Admin-Controlled Migration to New Outlook” policy setting and assigning it the “enabled” value. (It’s also available as a GPO or via the `HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Options\GeneralDoNewOutlookAutoMigration` registry key. If you previously hid the “Try the new Outlook” toggle as described above, changing this policy setting will have no effect.

In addition to this policy, Microsoft provides a companion setting (“Interval between new Outlook migration attempts” in Cloud Policy or GPO) that supports numeric values from 0 to 99000. If the value is 0, once a user has declined the switch in step 3 above, it will not be tried again. If the value is 1, once the user reaches step 3, they will be re-prompted to switch each time Outlook launches; this is the default behavior. If the value is from 2 to 99000, then the process will start over at step 1 after that many days has elapsed. That is, if you set this policy to a value of 10, after a user reaches step 3, they will be left alone for 10 days, at which point they will return to step 1.

Moving Settings to New Outlook

When users first switch to New Outlook, they will be shown a dialog labeled “Let’s make Outlook familiar” featuring a prominent button labeled **Import Settings**. Clicking this button instructs Outlook to migrate a few dozen settings from classic Outlook to both New Outlook and Outlook on the web. Settings migrated include the position of the reading pane, whether to use dark mode, the display language, and the meeting hours set in the calendar. If you skip the settings migration, you can perform it later by selecting **Settings > Accounts > Email accounts**, clicking the **Manage** link next to your email account, and choose **Get Started** to cause the welcome dialog to reappear.

In addition to migrating settings from Outlook classic, users may also need help migrating add-ins. Many Outlook users rely on [add-ins built with the Component Object Model \(COM\) interface](#). COM has long been supported in Win32 applications but can't be used with new Outlook. Microsoft has also supported a similar add-in mechanism known as web add-ins for several years. Users who switch to New Outlook and have COM add-ins installed via the "import settings" option described above will have some COM add-ins replaced by compatible versions. [This article has a list](#) of which add-ins will be automatically switched.

Managing Outlook Web App

When Microsoft first shipped Outlook Web Access, it was primitive compared to desktop Outlook, and yet still revolutionary. It was the first mass-market enterprise product to use the technologies we now call AJAX (asynchronous JavaScript and XML). For several releases, OWA's feature set lagged Windows Outlook, but as time passed, we eventually reached a turning point where new features started to be delivered first into on-premises OWA before reaching the desktop rich clients, and now that trend has accelerated so that on-premises Exchange is basically in maintenance mode with very few new features being released. New client features are more likely to appear first in Outlook Web App in Exchange Online than in desktop Outlook, and it's become very clear that we will see few if any new features in the on-prem version of OWA.

The modern OWA user experience rivals that of the full Outlook client. In fact, for many users, OWA provides all the functionality they need, with the convenience that it can be used from anywhere that has an Internet connection without having to first install client software. A good way to start an argument is to ask a room full of heavy email users whether they prefer OWA or desktop Outlook—you'll probably hear some vigorous opinions pros and cons.

OWA Browser Compatibility

Outlook Web App works with all the browsers Microsoft 365 supports: the latest versions of Microsoft Edge, Firefox, and Chrome on Windows, Safari on macOS, and Firefox or Chrome on Linux. You may see some minor differences in your client as the OWA interface evolves rapidly.

With the pace of changes and new features appearing across the service, maintaining updates to web browser clients is important for customers. If you experience some unexpected behavior of OWA when running a supported combination of web browser and operating system, you should check for recent updates to the browser. You can find the latest guidance on [OWA web browser compatibility](#) on the Office Support website.

Managing Mailbox Settings

Over time, Outlook and Exchange have accumulated many mailbox-level settings to provide fine control over things like whether week numbers are displayed in the calendar view or whether read receipts should be sent. Normally, users will configure these settings themselves, but in some cases, you may want to standardize them; for example, as part of user onboarding, you might want to preload a signature into every newly created mailbox. [Set-MailboxMessageConfiguration](#) controls mailbox settings such as signatures and the use of read receipts; [Set-MailboxCalendarConfiguration](#) covers how the calendar looks and how reminders are managed; [Set-MailboxRegionalConfiguration](#) controls regional settings such as the date and time formats, and [Set-MailboxSpellingConfiguration](#) governs the default spelling checker configuration and language. These cmdlets are covered in more detail in the Exchange Online chapter.

Managing Features with Outlook Web App Mailbox Policies

Outlook Web App mailbox policies provide administrators with control over which OWA features are available to individual mailboxes. Examples of the features controlled by OWA mailbox policies include inbox rules, calendar access, mobile device controls, and social network integration. Although an OWA mailbox policy

controls access to these features for OWA, it does not disable them on the mailbox itself. For example, a mailbox user prevented from accessing their calendar due to an OWA mailbox policy can still access their calendar using Outlook or a mobile device.

You'll find OWA mailbox policies, including this default, in the **Roles** section of the Exchange admin center (if you don't see them, type "policies" into the search bar at the top of the EAC to find them). There's a default policy in every tenant that enables all features for OWA. After opening a policy, you can disable or enable features like autosignatures and inbox rules by checking or unchecking boxes. Although convenient to manage the set of features published to users through the EAC, it's important to realize that the EAC surfaces some, but not all, of the possible configuration options for OWA mailbox policies. In this example, the *Get-OWAMailboxPolicy* cmdlet is used to display the name of the OWA mailbox policy, as well as a setting that controls whether the LinkedIn contact sync is enabled within OWA.

```
Get-OwaMailboxPolicy | Select Name, LinkedIn*
```

Name	:	OwaMailboxPolicy-Default
LinkedInEnabled	:	True

Most organizations only need a single, default OWA mailbox policy to which they make one or two changes to suit organizational needs. Alternatively, you can create multiple OWA mailbox policies and assign them to different mailbox users to limit access to some features. For example, you might want to create an OWA mailbox policy that turns off Calendar access for temporary employees or people working on an assembly line, along with another OWA mailbox policy that allows Calendar access for other users. After configuring a new OWA mailbox policy it needs to be assigned to mailbox users by running the *Set-CASMailbox* cmdlet.

The OWA mailbox policy that is assigned to a mailbox user can be viewed and changed in the Microsoft 365 admin center by selecting a user, then switching to the **Mailbox** pivot of the user details view. You can also retrieve the OWA mailbox policy that is assigned to a mailbox user by running the *Get-CASMailbox* cmdlet.

```
Get-CASMailbox Kim.Akers | Format-List OwaMailboxPolicy
```

OwaMailboxPolicy	:	OwaMailboxPolicy-Default
------------------	---	--------------------------

To change the OWA mailbox policy assigned to a user, you can use the *Set-CASMailbox* cmdlet, or you can open the user in the **Mailboxes** section of the EAC, then click the **Manage email apps settings** link.

```
Get-OwaMailboxPolicy | Format-List name
```

Name:	Limited Access OWA Users
Name:	OwaMailboxPolicy-Default

```
Set-CASMailbox Kim.Akers -OwaMailboxPolicy "Limited Access OWA Users"
```

The next time the user refreshes their session or logs on to OWA the new policy is applied. To revert the mailbox user to the default OWA mailbox policy, run the *Set-CASMailbox* cmdlet again.

```
Set-CASMailbox Kim.Akers -OwaMailboxPolicy (Get-OwaMailboxPolicy | Where-Object {$_ . IsDefault}) . Name
```

An OWA mailbox policy is not mandatory for mailboxes (the default policy is applied if one is not specified), so you can also remove policies entirely from the mailbox using *Set-CASMailbox*.

```
Set-CASMailbox Kim.Akers -OwaMailboxPolicy $Null
```

Customizing the OWA URL

The OWA URL for all Exchange Online customers is the same, <https://outlook.office.com>. There are some variations of that URL that will also work thanks to redirections that Microsoft has in place. For example, <http://outlook.office365.com> will redirect from HTTP to HTTPS and from the root of the domain to the /OWA virtual directory.

Although this is a simple URL some organizations would prefer a custom URL that includes their domain name, which may be easier for their end-users to remember. This can be achieved with a simple DNS CNAME record in the organization's public DNS zone. For example, a CNAME of *webmail* in the DNS zone for *office365itpros.com* with a target of *outlook.office365.com*, will redirect anyone browsing to <http://webmail.office365itpros.com> to <http://outlook.office365.com>, where Microsoft's redirection to /owa takes care of the rest.

Aside from the branding and ease of remembering, this is also a good strategy for retaining the same OWA URL that you may have previously used for on-premises Exchange, by simply changing it to a CNAME that resolves to the Exchange Online OWA URL instead. This avoids issues with your end-users still having web browser bookmarks for the on-premises OWA URL. However, this technique should not be used for Hybrid deployments.

Outlook for iOS and Android

For many years, Microsoft pursued a terrifically successful strategy of licensing Exchange ActiveSync (EAS) as widely as possible to third parties to enable their devices to connect to Exchange. EAS proved stable and both the cloud and on-premises versions of Exchange include basic security and management capabilities for mobile devices. The strategy of licensing ActiveSync to all and sundry worked in terms of making EAS the de facto protocol for Exchange mobile connectivity. The downside was that Microsoft ceded control over the user experience to the device vendors. Companies like Apple and Samsung incorporated EAS into the mail apps running on their devices while exerting absolute control over which features the clients expose to end-users. Exchange ActiveSync was always intended to do two different things: synchronize mail items between the device and a mailbox and provide mobile device management (including remote device wipe, PIN enforcement, and so on).

Despite the popularity of EAS, there was never a real advantage for device vendors to implement *all* the functionality in the EAS protocol, instead of just whatever subset they felt was useful. A good-enough job that allowed a user to connect to Exchange and access their mailbox was sufficient; there was no pressing reason for Apple, Samsung, Google, and so on to extend their mail apps to offer more functionality to Exchange users than they do when the apps connect to Gmail, for instance. Some vendors grudgingly added support for a subset of EAS device management features. The native mail app is "good enough" if you can use it to process messages, meetings, tasks, and contacts. This attitude has existed for years and has resulted in situations like the famous series of bugs in the Apple iOS mail and calendar apps that caused excessive transaction log growth on Exchange servers or calendar appointment "hijacking". The net result is that EAS is now the lowest common denominator protocol for mobile devices to connect to Exchange. The need to do better and to have control over functionality available through mobile clients drove Microsoft to come up with a new two-pronged strategy: first, they bought a company called Accompli and rebranded their clients as Outlook Mobile for iOS and Android, then they invested in improving device management by building mobile device management tools into Microsoft 365 and then releasing Microsoft Intune.

Licensing Outlook for iOS and Android: Not all plans include a license for the Outlook mobile clients. [Microsoft's FAQ](#) makes it clear that you need a suitable commercial license. "Suitable" really means that

the license grants access to a desktop version of Outlook; Business Basic, Business Standard, and Enterprise E3 or E5 all count, as do the corresponding versions of those plans for Education or Government. Exchange Online plans or the kiosk (front-line worker) plans may not include a license; these lower license tiers allow the use of Outlook on devices with screens smaller than 10.1". Users who only have on-premises Exchange mailboxes with no service licenses aren't permitted to use the client at all. However, Microsoft does not enforce these licensing restrictions, so users can violate the license terms without realizing it.

Microsoft has kept up a rather astonishing cadence for feature improvements in the mobile versions of Outlook. The client is regularly updated every two weeks, with minor features and bug fixes appearing in each release and larger, more complex features arriving as soon as they're ready.

Feature support varies between platform and license. For example, dark mode is available on Android and iOS for both commercial and consumer customers. Support for sensitivity labels and shared mailboxes, on the other hand, are only available to commercial customers, and delegate access is available only to commercial customers whose mailboxes are in the service. As it's impossible to roll out new features to more than 100 million clients worldwide simultaneously, Microsoft uses a random selection process to decide who picks up new features first. Features for both commercial and consumer users go to a random selection of people, which means that it's possible to have some people within a tenant see a feature and some not. Microsoft releases commercial-only features on a tenant-wide basis. Successive waves of releases move the roll-out to 100% status over a period that can take some weeks to complete.

Another unique point about the Android and iOS Outlook clients: their support lifecycle is necessarily quite different from their desktop cousins. Microsoft typically supports two versions of iOS: whatever the latest major release is, and its immediate predecessor. The rapid adoption of iOS versions means that this n-1 support policy won't generally be a problem for most enterprises, as users will self-update their devices to get the latest shiny goodness, but you should remain aware of it.

Using Classic Outlook for Windows in a Virtualized Desktop Environment

In virtual desktop environments, such as Citrix XenApp or XenDesktop, where multiple users log onto published applications or desktops hosted on a farm of servers, some issues exist with the classic Windows Outlook client when it runs in cached mode:

- The OST files for multiple users accumulate on the hard drive of the server and can quickly consume all the available disk space.
- If a user logs on to a new session on a different server than their last session, the OST file may need to go through a major resynchronization, or even recreate its copy of the mailbox from scratch, which causes both a poor user experience as well as a server performance issue that can affect all other users on the same server.

Similarly, in virtual desktop environments that use non-persistent storage, Outlook needs to rebuild the OST file from scratch each time a user opens Outlook to start a new session.

Microsoft has somewhat belatedly realized that customers want to use Office 365 in environments that are built around virtualized desktops, and they have been making steady improvements to support those environments. As an administrator, you can tweak Outlook sync settings using the [Office Group Policy administrative templates](#) (ADMX files) to improve the sync experience in these environments:

- **Sync Settings** – this setting allows you to specify the amount of data (by age) that Outlook should cache in the OST file. For example, you could set this to 1 month for users logging on to the virtual desktop environment and then set it to 12 months for users who typically work from the same desktop or laptop each day. Users who frequently work offline in remote locations may even prefer *all* their email to be cached always.
- **Fast Access** – this setting allows Outlook to connect to Exchange Online in online mode while building the OST file at the same time, and then switches to cached mode when there is enough data available.
- **Cache File** – this setting can be used to specify a network location for storing the OST file so that it can be stored on persistent storage and accessed from any virtual desktop that the user is logging on to. Microsoft has [published guidance](#) and some specific requirements covering this configuration scenario.

There are also third-party solutions, such as [Liquidware's ProfileUnity](#) or [FsLogix Office Container](#), that can help Outlook cached mode perform well in VDI environments. (Technically, FsLogix isn't a third-party solution since it comes from Microsoft but, as it must be deployed separately from Office, I'll call it that).

Real World: Microsoft offers several interfaces that developers can use to extend the various Outlook clients. For the most part, there are three categories of plugins: those which work only in Windows Outlook, those which work only in Mac Outlook, and those which are written using the Office extension APIs and can be loaded in both versions of desktop Outlook, OWA, and even Outlook Mobile. For example, the familiar button that allows you to make a meeting into a Teams meeting with a single click is an "add-in" (the preferred term for desktop-native extensions to Outlook), while the FindTime tool is written with the Office APIs and can thus be used in multiple clients once it's enabled for the user.

Supporting Outlook Cloud Settings

As part of its steady output of new features, Microsoft occasionally delivers something from the long backlog of features that have been requested for years and years. One example: the ability to synchronize signatures between different machines, something that people have been requesting for nearly two decades! Signature synchronization was the first element of the plan to synchronize most Outlook settings through the cloud, a worthy goal. However, signature sync has been delayed multiple times. For now, sync covers a subset of Outlook settings (the settings found in the Advanced, Calendar, Ease of Access, General, Groups, Mail, People, Search, and Tasks tabs), and settings are only synchronized for Outlook on Windows.

By default, this feature is enabled in your tenant, and you can't turn it off at the tenant level; you'll need to use a Group Policy template to disable it. Users can [control the setting themselves](#), though.

Managing Client Access and Protocols

Managing which clients can use mailboxes, and what protocols they can use to do so, is not so common a task as it was in the days before the cloud, but you may still find that you need to apply some restrictions to block old clients, protocols you don't want on your network, and generally tailor connections to meet your security needs. Microsoft 365 can do this in multiple ways, including applying conditional access settings (as described in the Identities chapter), using mobile application management (MAM) to control what mobile applications can do (the devices chapter), or controlling the protocols and client access on the service side.

Basic Authentication and Office Desktop Applications

Starting in August 2023, if you have version 2308 or later of the desktop Office applications, they will no longer support basic authentication. This change has no impact on clients that connect to Microsoft 365, since none of the service components still use basic authentication, but if you have a hybrid environment with older on-premises servers, you may notice that you can no longer access file shares, web pages, or on-premises SharePoint systems that are configured to use basic authentication.

Managing Application Idle Timeout Periods

Since its introduction as part of Exchange 5.5, OWA has had an idle timeout feature that allows administrators to sign out users after a specified period of inactivity. SharePoint Online has a similar feature, and of course, Entra ID token expiration and revocation may force users to log in again at any time even if they've been active. Microsoft has an [idle session timeout feature](#) that covers a selected set of Microsoft 365 web apps (OWA, OneDrive for Business, SharePoint, Office.com, Microsoft365.com, the Office web apps, and the Microsoft 365 admin center). Once you configure the idle session timeout feature in the **Security & privacy** tab of the **Org settings** item in the Microsoft 365 Admin center, the timeout you specify will take effect in all supported apps and supersedes the timeout values set for OWA and SharePoint Online.

Managing Mailbox Client Protocols

A set of connectivity protocols is available to allow clients to connect to Exchange Online. By default, Exchange Online mailboxes can use all protocols and features, which include:

- **Mail Application Programming Interface (MAPI)** - Outlook clients use MAPI to connect to mailboxes. Older Outlook clients are still able to connect using RPC over HTTP, but Outlook 2010 and newer clients running the latest service packs and updates connect using MAPI over HTTP. RPC over HTTP is an unsupported protocol from October 31, 2017.
- **HTTPS:** the OWA webmail client for Exchange Online connects via the HTTPS protocol.
- **Exchange ActiveSync** - Most mobile devices and applications that connect to Exchange Online do so via the Exchange ActiveSync (EAS) protocol.
- **POP3/IMAP4** - although these are now outdated protocols that do not support the advanced features found in most email clients, some users still use POP or IMAP to connect to mailboxes, and IMAP is also commonly used by external applications that need to ingest email items from mailboxes.
- **Exchange Web Services (EWS)** - EWS is the API for application access to Exchange mailbox resources, commonly used for integrating external applications. EWS is also used by Outlook to retrieve free/busy, out-of-office, and calendar sharing information.
- **SMTP** - Outlook can perform all its functions using MAPI, but POP and IMAP are access-only protocols. IMAP and POP clients need to use SMTP to send emails. SMTP is also used by external applications to send emails.
- **Microsoft Graph/REST API** - The Microsoft 365 APIs allow applications to access data such as email messages, contacts, calendars, and files. There are separate APIs for the various services (like Outlook and Teams), as well as the Microsoft Graph API.

You can manage mailbox client protocols through the Microsoft 365 admin center, the EAC, or PowerShell. Different capabilities exist through each interface, which we will explore in this section. First, the Microsoft 365 admin center includes an "Email Apps" section for user properties. Select a user, and then click the **Manage email apps** link in the **Mail** pivot and you'll see a list of available protocols. Enabling or disabling access to a client protocol is merely a matter of checking the boxes accordingly.

To change the client protocols available to a user through the EAC, go to the **mailboxes** section under **Recipients**, open the properties of any mailbox, then click the **Manage email apps settings** link. You'll see a toggle for each of the supported client types.

To view the status of each client protocol for a mailbox user via PowerShell, use the `Get-CASMailbox` cmdlet.

```
Get-CASMailbox -Identity Kim.Akers | Select *enabled
```

```
ActiveSyncEnabled      : True
OWAEnabled             : True
OWAforDevicesEnabled   : True
ECPEnabled              : True
PopEnabled              : False
PopMessageDeleteEnabled : False
ImapEnabled              : False
MAPIEnabled             : True
MapiHttpEnabled          : True
UniversalOutlookEnabled : True
OutlookMobileEnabled     : True
MacOutlookEnabled        : True
EwsEnabled               : True
OneWinNativeOutlookEnabled : False
```

To disable a client protocol in PowerShell, you could use the `Set-CASMailbox` cmdlet. For example, to disable access to the Monarch client for a mailbox, run the following command:

```
Set-CASMailbox -Identity Kim.Akers -OneWinNativeOutlookEnabled $False
```

You can repeat the same steps for each protocol. If you have a combination of enabled/disabled protocols you want to apply to mailboxes by default, then you will need to develop a custom script to apply those changes as part of your mailbox provisioning process. You may be able to avoid some of this tedium now that Microsoft has given us the [Set-CASMailboxPlan cmdlet](#). This cmdlet allows you to set up a template for protocol access, then apply the template automatically to newly created mailboxes. By default, you get four CAS mailbox plans in the service; you cannot create, rename, or remove them. The plan applied when a mailbox is created depends on the license assigned to the mailbox: Exchange Online Kiosk plans get the ExchangeOnlineDeskless plan, Exchange Online P1 gets ExchangeOnline, and Exchange Online P2 gets ExchangeOnlineEnterprise (which means that E3 and E5 subscribers get it too). Microsoft 365 Business Basic subscriptions get ExchangeOnlineEssentials. Suppose you wanted newly created mailboxes for your enterprise users to have IMAP and POP disabled—you could easily do this by running the following cmdlet:

```
Set-CASMailboxPlan -Identity ExchangeOnlineEnterprise -POP3Enabled $False -IMAPEnabled $false
```

Note: There are two protocols in the `Get/Set-CASMailbox` cmdlets that you can probably ignore for now. *MapiHttpEnabled* is only applicable to on-premises Exchange organizations, so changing it in a cloud environment will do nothing. The second, *UniversalOutlookEnabled*, controls whether the Mail app for Windows 10/11 (sometimes called “Universal Outlook” in news articles and blog posts) is enabled.

Managing Exchange Web Services

The Exchange Web Services (EWS) API was originally introduced with Exchange 2007 as a replacement for WebDAV and, at the time, the planned successor to MAPI. MAPI lives on, but so does EWS. Applications can use EWS to retrieve information from Exchange Online services or to interact with data in Exchange Online mailboxes. For example, an EWS application can retrieve information about calendar items for room mailboxes to determine which items might have an organizer who no longer works for the company.

Since 2018, Microsoft has steadily been [moving away from EWS](#) as the preferred API for programmatic access to Exchange Online data, in favor of Microsoft Graph. This change has no impact on on-premises Exchange servers. However, for those who are using EWS to talk to Exchange Online, this change means that:

- EWS will not receive future feature updates.
- Microsoft has decommissioned basic authentication for EWS and exclusively uses [OAuth 2.0](#). Microsoft deprecated basic authentication fully in October 2022.
- EWS will remain supported in production for Exchange Online environments if you use OAuth 2.0.
- Microsoft deprecated 25 EWS APIs ([listed here](#)) on March 31, 2022.
- Microsoft originally planned to start blocking the registration of new EWS applications in January 2023. That meant that migration vendors, as well as vendors that create client applications that leverage EWS, wouldn't be able to register new instances of their applications—which would pose a problem for vendors whose applications depend on capabilities that aren't yet available in Graph. Microsoft has deferred this plan for now, with no set date for revisiting it.
- Microsoft announced in September 2023 that they will [completely deprecate EWS on October 1, 2026](#) by blocking EWS access for all non-Microsoft applications.

There are many EWS features not present in Graph; if you use them, you're stuck with using EWS for now. The impending end of the protocol is making line-of-business app developers and third-party ISVs very nervous. Microsoft has not done a very good job of delivering parity, or even showing their plans for getting there, so this deprecation is a worrisome development if you have applications that use EWS (here's a Microsoft page [mapping EWS to Graph APIs](#)).

There are lots of clients that still use EWS today. For example, the Windows Outlook client uses EWS for calendar free/busy information, Out of Office settings, calendar sharing, and other features such as MailTips. Other applications (including the macOS Mail application) use it for access to mailbox data as well. As with the other protocols used to access Exchange Online, there are controls available for administrators to use for a variety of scenarios. EWS controls can be managed at the mailbox level or the organization level. The EWS settings for a mailbox are retrieved by running the *Get-CASMailbox* cmdlet, and the organization level settings are retrieved by running the *Get-OrganizationConfig* cmdlet.

Using the EWS Application Allow or Block List

Because EWS was the preferred protocol for mailbox access, naturally an ecosystem of third-party tools sprung up that used EWS to access mailbox data. For example, the Fantastical calendaring application for macOS and iOS uses EWS to access your calendar when you install it, and LinkedIn for years had an option to synchronize your mail contacts to their service using EWS. Thankfully, Microsoft has provided tools for controlling these applications without having to block *all* EWS traffic.

Disabling the entire EWS protocol because of one unapproved example of application access would deny your organization the many good things that EWS allows. Fortunately, we can be selective in what we block or allow for EWS by configuring an EWS application access policy. The EWS application access policy can be configured on a per-mailbox basis or configured for the entire organization. It's important to know that this blocking mechanism depends on the User-Agent header sent by the client to the service, which is easily spoofed. Don't rely on this mechanism alone to protect critical data.

Real World: If your tenant has "K" (Kiosk) or Office 365 F3 licenses, the EWS allow/block controls for your tenant will not work at the organization level. For non-Kiosk mailboxes, apply the allow/block controls on a per-mailbox basis. For the mailboxes themselves, direct EWS application access to the mailboxes is not permitted anyway.

Suppose you wanted to block access to an application whose User-Agent string had a value of "LinkedInEWS." This would require two separate calls to the *Set-OrganizationConfig* cmdlet. First, set the *EWSApplicationAccessPolicy* to enforce the block list.

Set-OrganizationConfig -EwsApplicationAccessPolicy EnforceBlockList

Unless and until you do this, the EWS block list won't be used at all. Next, add the target user agent to the EWS block list.

Set-OrganizationConfig -EwsBlockList @{add='LinkedInEWS'}

The EWS block list is a multi-value attribute so it should be managed using add/remove methods to avoid overwriting existing values when you are making modifications. For example, to add the Outlook mobile user agent to the block list you'd run this command:

```
Set-OrganizationConfig -EwsBlockList @{add='Outlook-iOS/*','Outlook-Android/*'}
Get-OrganizationConfig | Format-List ewsblocklist
EwsBlockList: {Outlook-iOS/*, Outlook-Android/*, LinkedInEWS*}
```

Similarly, to remove an entry you run this command.

```
Set-OrganizationConfig -EwsBlockList @{remove="LinkedInEWS"}
Get-OrganizationConfig | Format-List ewsblocklist
EwsBlockList: {Outlook-iOS/*, Outlook-Android/* }
```

Unlike ActiveSync device access rules, the strings used for EWS block and allow lists can use wildcards for partial matches. However, unlike ActiveSync controls there is no quarantine action available, only allow or block.

If you only wanted to block access for an application on a single mailbox, you'd follow the same process, except that you'd use the *Set-CASMailbox* cmdlet instead of *Set-OrganizationConfig*. Enforcing a block list will permit any EWS application that is not in the block list to connect. A more restrictive approach is to enforce an allow list instead, which requires that any EWS applications be listed in the allow list before they can connect.

Set-OrganizationConfig -EwsApplicationAccessPolicy EnforceAllowList

Enforcing a block or allow list for EWS has no impact on the Entourage, Outlook for Mac, or Microsoft Outlook applications. These applications are controlled with different EWS settings which are discussed next.

Blocking/Allowing Mac Clients

Organizations that standardize on Windows may want to block Mac clients from various parts of their network. In addition, organizations that allow Macs may still want to control how clients connect. For example, an organization that supports BYOD may wish to require users to connect only through Outlook Web App or Outlook Mobile.

Even though some versions of the Mac Outlook client use EWS, Microsoft provides a separate way to prevent only Microsoft's Mac clients from connecting to the service. The Mac clients are allowed by default and can be blocked using *Set-CASMailbox* or *Set-OrganizationConfig*. For example, to block Mac Outlook for a mailbox user you would run the following command.

Set-CASMailbox Kim.Akers -MacOutlookEnabled \$False

Apple's Mail and Calendar clients use EWS, and you can block their access by specifying their user agent strings using the EWS block list described in the preceding section. Note that the *EwsAllowEntourage* flag to these cmdlets only affects the ancient, and long-deprecated, Microsoft Entourage client for macOS. It doesn't affect any other client.

Blocking/Allowing Outlook EWS Access

You can also block Windows Outlook's access to EWS. This will break free/busy information, Out of Office, and calendar sharing. Blocking Outlook is a rare requirement and typically only applies to organizations that want to limit specific users from being able to share calendars or see the availability of other users.

The *Set-CASMailbox* or *Set-OrganizationConfig* cmdlets are used to apply the block. For example, to block EWS access by Outlook for a mailbox user you would run the following command.

```
Set-CASMailbox Kim.Akers -EwsAllowOutlook $False
```

Other Uses for EWS

Exchange Web Services is used by many organizations for custom application development, such as creating integrations between Exchange Online and their in-house line of business applications. It was also the API used for integration between Exchange Online and other Microsoft services such as Skype for Business and SharePoint Online. EWS applications can send and receive email messages, manage calendar items, and a whole lot more.

Many third-party migration tools use EWS to access Exchange Online mailboxes. In addition, several "cloud backup" products use EWS as the access protocol to extract mailbox data from Exchange Online to copy to cloud storage and so meet the needs of many organizations who would like to make use of cloud systems but are concerned about backup and recovery.

Managing Teams Clients

The Teams desktop app is available for:

- **Windows:** 32-bit versions are available for Windows 8.1 or later; a native 64-bit ARM version is available for ARM on Windows. You can also install Teams on Windows Server 2012 R2 or later. Teams requires .NET Framework 4.5 or later.
- **macOS:** There are native versions of Teams for macOS 10.11.0 or later, on both Intel and Apple Silicon processors, packaged as a single universal binary.
- **Linux:** Microsoft retired its desktop Linux client in December 2022 and replaced it with the progressive web app (PWA) version.

The progressive web app (PWA) version of Teams, available for Edge and Chrome on macOS and Windows, has the same functionality as the web client, with the exception that (because it's a PWA) you can pin it to the taskbar or dock, create a desktop shortcut to it, or have it automatically start when the user logs in.

Classic Teams vs New Teams

Microsoft is still attempting to convince the world to move from the previous version of Teams to what they first called "the New Teams." In this book, when we say "Teams," we mean the current version; the older version will be labelled as "classic Teams" when it's necessary to refer to it. Microsoft has already removed the "new" label from the current Teams application icons, branding, and documentation. On Windows 10 and macOS machines, the older client is now labelled "Microsoft Teams classic"; on Windows 11 computers, the app is called "Microsoft Teams classic (work or school)."

Classic Teams was written using a portable framework known as [Electron](#). It performed sluggishly on most machines, was difficult to centrally deploy, and used a unique update mechanism that was separate from the rest of Office.

The new version, sometimes nicknamed “Teams 2.1” or “T2.1”, was [released in public preview in late March 2023](#) and was released to [general availability in October 2023](#). This version launches up to two times faster, contains many performance and resource usage improvements, provides a unified experience like the unified inbox in Outlook, and can now be installed and managed through Intune. There are also several other welcome and important security improvements:

- The new Teams is packaged as a set of MSIX packages and installed with the [App Installer](#) service.
- Using App Installer means that the Teams app can be installed by an unprivileged user but without putting it in the user’s Windows profile.
- Microsoft has rewritten the entire web layer for the Teams client, adding more protection against cross-site scripting attacks, including using [Trusted Types](#) to allow the web layer to validate more of the data that it gets from the client, and vice versa.
- For macOS clients, the classic and new Teams clients can run side-by-side and be managed separately through MDM, because they have different bundles (new Teams has a bundle ID of `com.microsoft.teams2`).

Many users and organizations have already voluntarily switched over to the new Teams client thanks to the expedient of Microsoft including a toggle labeled “Try the new Teams” in the classic client for several months. However, Microsoft is now taking a somewhat firmer stance on upgrades because they’ve set a timeline for retirement of the classic Teams client. They have defined five states for Teams users in worldwide tenants; these states are set in the Teams Update Management policy either in the Teams admin center or by using the `Set-CsTeamsUpdateManagementPolicy` cmdlet:

- When the policy is set to “Not enabled,” users won’t see the “Try the new Teams” toggle and they can’t switch away from the classic client.
- The “Classic Teams as default” policy shows users the switching toggle, but defaults to leaving users in the classic client. This policy was previously named “Users can choose.”
- By default, the upgrade policy is set to “Microsoft controlled,” meaning that Microsoft will choose when to switch your users over. Microsoft-controlled tenants are currently having their users automatically switched to the new Teams client. If you choose this value for your update policy, you can’t control which users are switched or when the switching happens.
- The “New Teams as default” policy value allows users to toggle between Classic and New Teams, but the default is for users to get the New Teams experience.
- The “New Teams only” policy is a one-time cutover—when you enable it, users will be switched to the new Teams client. They can’t switch back via the toggle, and when an individual user switches that starts a timer that will remove the classic Teams client after 14 days. This grace period allows you to change users to a different policy if necessary.

These policies give you a degree of control over what Teams experience users get, at least until the client support lifecycle kicks in. As of July 1, 2024, the classic version of Teams is officially at end of support.

Microsoft says that means they will “no longer provide updates or new features for the client, nor will we help resolve support issues with the classic Teams client.” This date applies to all tenants in the commercial and educational clouds; US Government cloud customers and certain Teams and Surface Hub devices will reach end of support later. The classic client will reach end of availability on July 1, 2025; after that time, it won’t work with the service at all.

In addition to these deadlines, per the notice posted in MC794736, Microsoft blocks older versions of the classic Teams client from connecting once they are determined to be too old. Starting in August 2024, versions of Teams for Windows older than 1.6.00.18681, or macOS clients older than version 1.6.00.35956, will display a page telling users that they must upgrade to the new Teams client.

Microsoft automatically removes the classic Teams app when, in their words, "a period of time" has passed since the client's upgraded to the new Teams app.

There are separate, and evolving, timelines for users in GCC, GCC High, and US DoD clouds. See [Microsoft's documentation](#) for the latest.

Bulk Deployments of the New Teams Client

You can upgrade your Classic Teams clients in bulk, at least on Windows machines, instead of waiting for the policy-based system to apply the update. You do this by [using the teamsbootstrapper.exe tool](#). The basic procedure is straightforward: you use your preferred automated deployment tool to deploy the bootstrap utility. When it runs, it downloads the MSIX package of the current version of the Teams client and installs it for all users on the computer, then updates the registry to integrate the new installation with other existing Office applications.

Teams Desktop, Mobile, and Web Clients

In most cases, the browser client is functionally equivalent to the desktop client, but as evident in the hints dropped when you use Teams with a browser, Microsoft prefers the desktop client. The new Teams client is now fully supported for Firefox, Safari, and Linux (in addition to its existing support for Chrome and Edge). With this change, Microsoft has also started referring to "Teams for Web" as a consistent product name.

Mobile Teams apps are available for [Apple iOS](#) and [Android](#). Platform-specific technology is used (Swift for iOS and Java for Android) to create the user interfaces. Underneath, the mobile clients share the same basic functionality as their browser and desktop counterparts, including the ability to create and manage teams (membership and channels). As you'd expect, mobile clients are easier to use and more responsive than the other clients in some areas and less functional in others. For example, the mobile client often switches to a different tenant faster than the desktop or browser client do, but it is easier to compose a complex post with the desktop or browser client.

As detailed in Table 14-2, the Teams desktop and browser clients support limited offline capability to read and send personal chats and channel conversations. Almost every other piece of functionality needs an internet connection to work unless an app is designed to work offline. In some cases, like the calendar or documents, other tools are available to maintain local copies of data that permit offline activity.

Feature	Offline capability
Personal and group chat messages	Cached copies of messages are available offline for pinned and recent chats. Messages can be composed and queued for delivery locally when the network connection resumes. Messages are sent if a connection becomes available within 24 hours. If the delay is longer, the attempt to send the message will fail and Teams prompts the user to retry.
Channel messages	Cached copies of messages are available offline for pinned channels and channels recently accessed by the user, going back about 90 days. Messages for hidden channels are unavailable. Sending channel messages when offline works similarly to chat messages.

Calendar app	Cached copies of calendar events can be viewed. You can't schedule, initiate, or join meetings using Teams when offline. You can use Outlook to work with your calendar when offline.
Files	Both channel folders (SharePoint Online) and personal files in (OneDrive for Business) are unavailable offline. Files can be synchronized to the local drive with the OneDrive for sync client and accessed offline.
Tasks	None. You can use Outlook or the To Do app to work with personal tasks (but not tasks in Planner) when offline.
Wiki	None.
Lists	None.
Whiteboard	None. This may change now that Microsoft has moved Whiteboard storage to OneDrive for Business.
Viva Engage communities	None.
People card	None.
Third-party apps	Depends on the offline capability of the app.
Switch tenant	Not possible—when you go offline, you're stuck in the tenant you're currently in until you regain network access.
Manage team	None.
Calls	None unless the location deploys a Survivable Branch Appliance (SBA).

Table 14-2: Teams offline capabilities

From a practical perspective, no matter what client you're using, the internet connection must be reasonably capable in terms of both latency and bandwidth. Even though Teams clients cache data for faster access, the high latency, and low bandwidth often available in airplane Wi-Fi services can make using Teams an excruciating experience. To help assess the impact of Teams usage on a network, the Teams admin center includes a network planner to help figure out what network capacity is needed. Your mileage will vary depending on how people use Teams and the clients used. Remember that although Teams usage increases over time, the usage of other applications like email might decrease to offset the extra network demand. In terms of security, Teams supports the same multi-factor authentication methods as other Microsoft 365 applications do.

Managing Teams Updates via Channels

Like Windows and the rest of Office, Teams supports multiple release channels so that you can selectively provide early access to pre-production features. Three channels are available:

- **Beta Preview Channel:** The earliest that non-Microsoft users can access new Teams features. Microsoft uses rings to describe the release of new functionality from the development group (ring 1) to general availability (ring 4). This channel was Ring 1.5.
- **Private Preview Channel:** Access to more developed forms of new Teams features. Microsoft previously called this Ring 3.
- **Public Preview Channel:** Tenants can enable public preview for selected users via an update policy to allow those users to have early access to new features. This channel layers pre-release functionality on top of the general availability build (Ring 4). In May 2023, Microsoft announced Teams support for targeted release, meaning that tenants choosing targeted release use Teams Preview (for the entire tenant or the accounts configured for targeted release).

Collectively, the three pre-release channels are known as Teams Insider. Restricted access to the Beta Preview and Private Preview channels is available to companies participating in Microsoft's Technology Adoption Program (TAP). Features released to the TAP are under Non-Disclosure Agreements (NDA).

Clients configured to use the Current Channel (Preview) release of Microsoft 365 Apps for enterprise automatically use the Teams Public Preview channel unless the Teams update management policy assigned to their account disables the link between Office preview and Teams (the link is on by default). To disable the link, update the policy in the Teams admin center or use the `Set-CsTeamsUpdateManagementPolicy` cmdlet (in the Teams module). For example, this command disables the link for any account assigned the default update management policy:

```
Set-CsTeamsUpdateManagementPolicy -Identity Global -AllowPublicPreview Disabled
```

The `AllowPublicPreview` setting can be:

- **Enabled:** Enabled allows users to switch the Teams desktop client from the production version into preview mode manually.
- **Disabled:** Disabled hides the option to switch to preview mode
- **Forced:** Users assigned an update policy with this setting don't get the chance to opt-in to use the preview version and don't see the option to switch between preview and production.
- **FollowOfficePreview:** Accounts configured to use the Current Channel (Preview) of the Microsoft 365 apps for enterprise will also use Teams Preview.

When a Teams desktop or browser client runs in preview mode, it displays **EA** for "early access" (the indicator used to be P) beside the upper right-hand quadrant of the user profile photo in the menu bar.

Teams Client Release Notes

Like most of Microsoft 365, Teams is developing rapidly. Microsoft publishes monthly [release notes for Teams](#) online to give formal guidance about the introduction of new features. The release notes don't cover every new feature released for Teams, but they are a useful resource.

Teams Desktop Client Updates

Microsoft automatically deploys the Teams client as part of the Microsoft 365 Apps installation for users who have Microsoft 365 Business or Enterprise subscriptions. You can also bulk-deploy the new client using the `teamsbootstrapper.exe` utility described earlier in the chapter.

Once installed, the Teams Windows client is self-updating, using MSIX as its update mechanism. Users typically do not have to exit the client before an update proceeds.

Anything that prevents MSIX packages from being installed (such as the presence of the [registry keys described here](#))

On macOS, the Teams client install their updates using the Microsoft AutoUpdate tool described earlier in the chapter. to download feature updates for both production and Insider rings, except for versions of the apps downloaded through the Mac App Store.

Microsoft usually releases Teams update packages on a two-week schedule. This schedule could vary if a problem discovered in a build is important enough to warrant an immediate fix, in which case Microsoft will release a new package. When signed into their home tenant, Teams desktop clients perform a check every few hours to detect new updates, and, if found, the client downloads and applies the update in the background when the workstation is idle.

Several reasons can affect the ability of the Teams client to download updates, including:

- Antivirus software blocks the Teams update executable or the download of the update packages.
- Network infrastructure to specific locations is not capable of supporting software downloads.
- People only use Teams desktop client for calls and/or meetings. To ensure performance, Teams does not check for updates during these activities, and if the user closes Teams after their meeting finishes, the client will never download and apply updates.
- The files for the Teams client are in a non-standard path. In this situation, users must update the client manually.

The fact that the Teams client self-updates is challenging for some organizations who like to control the software users have on their workstations. However, Teams is more aligned with the app model found on mobile devices than traditional software distribution channels and the aim is to deliver the best and most functional experience to users. For this reason, if you want to know what Teams delivers in client updates, you need to keep a close eye on the [release notes published by Microsoft](#).

New Features and Enablement Flags

When Teams ships a new feature, it uses a two-phase process to enable the functionality. First, updated software rolls out to backend services and for download to desktop, browser, and mobile clients (as appropriate). To allow Microsoft to enable features separately from software updates, they use configuration flags to turn features on or off. Features don't become available to users until Microsoft sets the relevant flags.

Clients can receive software updates with the feature flags set off. When Microsoft testing and validation with early adaptors show that the feature is stable, Microsoft enables the flag to "*light up*" the feature. This process happens progressively as tranches of clients are enabled. Given the distributed nature of Office 365, the process of enabling a new feature can take some time. To ensure continual validation against a cross-section of workstation configurations and usage patterns, Microsoft does not organize users into tenants. Instead, tranches include users selected from multiple tenants and multiple countries. All of this means that some users within an organization may see a new feature before others.

Mandatory Updates

Teams supports [Microsoft's Modern Lifecycle Policy](#), which requires users to run a recent version of software to maintain access to services. Once the Teams desktop client is more than a month behind the current release, the client displays a banner to advise that a software update is necessary. The banner includes a link to start an update. If the user doesn't perform a software update, Teams continues to prompt the user to update until the software is more than three months behind the released version. At this point, Teams displays a blocking page to give the user the choice to update the software now, looking for help from their IT administrator (to help with the update or apply a manual update), or to continue accessing Teams via the browser client.

New installations of the Teams client can deploy software more than three months old. In this situation, a 28-day grace period begins during which the user can continue to use the old software while Teams attempts to update the client in the background. At the end of the grace period, the user cannot use Teams, and an IT administrator must update the device.

What Version of the Teams Desktop Client is on a Workstation?

To learn what version of Teams is running on a workstation, open the Settings app and select About Teams. The version number and the last updated timestamp is displayed there.

Teams and VDI

VDI, or Virtual Desktop Infrastructure, is a virtualization technology that allows desktop systems to be hosted on centralized servers. In late June 2024, Microsoft began rolling out Teams service updates that provide a significantly changed architecture to support VDI use of the new Teams client. The centerpiece of the new architecture is an improved version of a component known as "vdibridge," plus a new media engine. Both components are optimized to run in Citrix or Azure Virtual Desktop environments.

Microsoft notes in MC799210 that Teams VDI deployments may be affected by the automatic Teams update process described earlier in the chapter, resulting in problems when the old Teams client is automatically removed. This problem occurs most often because the organization manually chose to install the Outlook meeting add-in for Teams in the same directory as the classic Teams client. If your organization did this, the Message Center post contains instructions on how to install the new Teams client into an alternate location to avoid accidentally killing the add-in.

The classic version of the Teams client is no longer supported on VDI infrastructures after October 1, 2024.

Teams Phone Application

The Teams Phone application is a special version of the Android mobile client built for device manufacturers to build [Teams-enabled devices](#). These devices allow users to call other Teams users or PSTN numbers, join a Teams meeting, and retrieve voicemail. In effect, the phone application delivers the same functionality as other mobile clients with the chat (personal and channel), files, and extensibility features removed. Only devices specifically designed to work with Teams can support the Teams Phone application.

A Few Teams Application Tips

Unlike, say, Outlook or Word, which have been around a very long time, Teams has lots of little features that aren't well understood by many users or admins. Here are a couple of things you might want to delve into within the app to help you, and your users, get the best experience.

Notifications

Teams can notify users when different events occur in chats and channels, such as being @mentioned in a conversation. These are global settings that apply across all teams and channels that appear in your teams list. Teams doesn't notify you of events in hidden teams or channels or when you mute a channel or conversation. You can choose default settings such as notifications for all activity or just mentions and replies or customize each source of notifications. You control notification behaviors through **Settings > Notifications and activity**. For each category of activity (e.g. @mentions), you can choose any of the following:

- **Off:** Don't show these kinds of events (for example, don't show reactions to messages).
- **Show in Activity:** Show events in the activity feed only.
- **Show in Activity and banner:** Teams signals events in both the activity feed and a desktop notification. You can choose between Teams built-in notifications or native operating system notifications (Windows and macOS). For example, if you opt for native notifications on Windows, Teams posts its notifications to the Windows notification center.

Separately from notification behaviors, users may choose to receive missed activity emails. These messages are for events that happen when the user does not sign into Teams. The available intervals range from "as soon as possible" to "once a day." You can disable notifications by setting the interval to "Off." Teams can also monitor the status of priority users and flag when they appear online or sign in.

Switching Between Organizations

Users might have accounts in multiple tenants, including guest accounts based on their primary tenant. The desktop and browser clients show the current organization in the upper right corner of the Teams window. To switch tenants, click the organization name and select the target organization from the list of available tenants to which the signed-in user has access. The list includes:

- Their home tenant.
- Other Microsoft 365 tenants where the signed-in user has a guest account.
- The consumer version of Teams accessed using a Microsoft Service account (MSA).

Each tenant in the list shows the user's presence status. If the user's credentials for a tenant have expired, you see a warning sign. The notification icon in the top of the Teams window shows the number of unread notifications for each tenant where the user has access, although unread item counts are not available for any organization where the credentials need renewal until the user reauthenticates. Settings are specific to an account in a tenant. If someone is a guest in another tenant, they must configure settings for Teams in that tenant if they want to see the same behavior everywhere.

If you have notifications enabled, you will see notifications from all the organizations you're signed into. This can cause some confusion if you interact with a notification from tenant B whilst you're logged into tenant A, because tapping the notification will cause the client to load the item of interest, which means now you're seeing something from tenant B. It's easy to switch back to the desired tenant at any time.

You should also be aware that there are still a few subtle (and not-so-subtle) bugs lurking around tenant switching. For example, while writing this book I often found that switching to the Office 365 for IT Pros tenant to work, then switching back to my primary work tenant would cause some chat participants in my work tenant to be labeled "Unknown User" until I signed out and signed back in.

Managing Quiet Times

Teams has multiple ways to let users know when new information has arrived from banner notifications to the activity feed to email digests. If you belong to busy teams, you might like to have some quiet time when notifications aren't delivered unless they are urgent. Desktop and browser clients obey operating system settings for notifications. For instance, on Windows 10/11 clients, the Focus Assist setting controls when applications can send notifications. One of the automatic Focus Assist rules stops notifications between 23:00 and 07:00, and if the rule is enabled, you won't see notifications for channel or personal messages during that period. Even when notifications are suppressed, they still accumulate in the activity feed.

The Teams mobile clients take a different approach and have their own Quiet Hours settings to control when during each day notifications are allowed and Quiet Days to control on what days notifications are accepted. For example, you can disable notifications entirely at the weekend and define that you only want to see notifications between 09:00 and 17:00 during the working week. These settings are specific to each tenant—so if you've signed into multiple tenants on mobile, you will have to set quiet hours in *each* tenant or you may still receive notifications from any tenant where you haven't done so.

Annoyingly, incoming calls are not governed by the notification settings. If you are signed in and available when a call arrives, you'll have to decide if you want to answer or ignore it.

Using the Command Box

The command box at the top of the Teams window gives users fast access to common Teams operations. For instance, to call someone, type `/call` in the command box and then select the person you want to talk to while the `/chat` command switches to a personal chat with the selected person. Unfortunately, the command box

limits user lookup to tenant accounts so you can't specify a federated or guest user as the target of a command such as `/call`. The command box is also a great way to update your presence with commands like `/dnd` (Do not disturb) or `/busy`.

In addition to Teams commands, if you install apps into Teams, they can become available in the command box. For example, if you install the weather app, you can type `@weather` to find out the current weather in a location, or `@news` to use the News app to look for breaking stories about a topic, or `@YouTube` to look for a video. Once you find what you need, you can copy it to the clipboard and then paste it into a conversation.

Managing OneDrive for Business Clients

The OneDrive for Business client has come a long way since its 2016 debut. The first version of the client was based on the legacy Groove.exe client, then Microsoft introduced the Next Generation Sync Client (NGSC). NGSC morphed into what is now known as OneDrive and has by now replaced the legacy client. The current client offers full sync functionality for personal OneDrive folders, OneDrive for Business libraries, and SharePoint Online document libraries (including those associated with Microsoft 365 Groups). Sync works across tenants and Active Directory domains; for example, the files used to produce this book are hosted in the Office 365 for IT Pros tenant, but I synchronize them to several Mac and Windows PCs that are joined to various (or no) other tenants.

Deploying the OneDrive Sync Client

If you've already deployed a reasonably modern version of the desktop applications to your computers (say, Office 2016 or later), then the latest OneDrive client is installed. Note that the OneDrive client has its separate update mechanism and doesn't get updates through the same channel as either Office or the host OS.

If you have domain-joined computers, you should probably also download and configure the [OneDrive Group Policy template](#) for your organization. If you plan to use Group Policy to control sync settings for end-users, you will need to modify the copy of the Group Policy ADMX file that you place in your Central Store. You can edit the file using any text editor such as Notepad or Visual Studio Code. Within the ADMX file replace any instances of the placeholder text for the tenant ID with your real tenant ID, discovered by running the `Get-MgOrganization` cmdlet. The tenant ID is the GUID string displayed after a successful connection.

```
PS C:\> Connect-MgGraph
Get-MgOrganization | Select Id

Id
--
2b9bca49-687e-4e5f-8a52-21350b719b06
```

The Group Policy template also contains a [wealth of other settings](#), including controls that allow you to restrict what tenants users may synchronize with, control what the client should do on laptops when they're on battery power, apply default bandwidth limits for upload and download, block sync traffic when the computer is idle and no one is signed into it, and block or allow the client from synchronizing personal OneDrive accounts.

Besides these Group Policy-based settings, Microsoft supports [silently configuring OneDrive using the user's credentials](#) to provide single sign-on, but this requires you to configure the `SilentAccountConfig` registry key. If you don't do that, plan on communicating to your users how to sign into their OneDrive client manually.

Managing OneDrive Sync Client Updates

Whether you install the OneDrive sync client with Microsoft 365 Apps or by using the OneDrive standalone installer, the sync client application files are installed in the **%localappdata%\Microsoft\OneDrive** folder. This means that OneDrive is installed by default as a per-user application, not as a per-computer application. It also means that OneDrive can be installed and updated by users who do not have local administrative rights on the computer. If you want to install the OneDrive client per machine, you can do so [with these instructions](#).

Microsoft releases OneDrive sync client updates through [three deployment rings](#):

- **Insiders** – this ring is an opt-in distribution channel for early adopters; releases into this ring go only to users who have enrolled in the Windows or Office Insider programs. Complete deployment of a new version into this ring takes about 3 days.
- **Production** – Once Microsoft releases a new update for this ring, updates are released to a small percentage of clients in this ring first, and the remaining clients receive the update within approximately two weeks. This is the default deployment ring for OneDrive installs, and there are no controls available for including or excluding your computers from that initial small percentage of clients that receive updates first. During the release of updates to the production ring, Microsoft uses its telemetry to measure the success of the initial rollout. If a problem is discovered, updates will be stopped while a fix is developed. The clients that received the problematic update will then be the first to receive the next update to fix the issues, and then updating will continue through the rest of the production ring.
- **Deferred** - Updates are released to the deferred ring only after they have been successfully deployed to the production ring without any major issues. The deferred ring receives updates over a 60-day window that starts after the production ring deployment window has ended. Critical updates might be released to clients early in that 60-day window, but otherwise, you can expect your clients to update any time within that period. You can use [Group Policy objects](#) to control this behavior.

The OneDrive sync client checks for newly available updates every 24 hours while it is running. To check for or apply sync updates, the client must be able to reach the *oneclient.sfx.ms* and *g.live.com* domains. If OneDrive has not been running within the last 24 hours, it will check for updates immediately the next time it starts. Windows 11 clients also have a scheduled task that will check for OneDrive updates every 24 hours regardless of whether the sync client has been running. These mechanisms are all designed to keep OneDrive updated with the latest bug fixes and feature enhancements. If you're tempted to block OneDrive from checking online for updates then you'll need to periodically check for an updated OneDrive standalone installer, download the updated application files, package them for deployment, and then manage the rollout using your enterprise software deployment tool. That's an unnecessary overhead for most organizations though. If you prefer to take a conservative approach to OneDrive updates then you can configure clients to use the enterprise ring, but you should be aware that this will slow the release of new features as well.

You can configure the update ring for OneDrive by using the [OneDrive Group Policy template](#). In **User Configuration, Administrative Templates, OneDrive**, there is a setting to *Delay updating OneDrive.exe until the second release wave*. Enabling that setting places the client in the deferred deployment ring.

Managing Microsoft Authenticator

You can make a good argument that reusable passwords are bad. Giving users individual passwords for access control can lessen security—if you require long complex passwords, users will reuse them or write them down, but if you don't, users will pick short, simple passwords that can easily be brute-forced. In the same vein, passwords that expire are bad (because users will just recycle old ones) but passwords that *don't*

expire are bad too (because once compromised a non-expiring password might be used for a long time). However, for many years, reusable user-specific passwords were less bad than the alternatives. Thankfully, we live in a world where the widespread availability of smartphones and hardware tokens has led to the increasingly broad deployment of multi-factor authentication (a topic discussed at some length in the Identities chapter). Microsoft 365 and Azure MFA support several authentication factors, including phone-based authentication, one-time codes sent via SMS, and push notifications or codes generated by a mobile application. Although Google, LastPass, and other companies make mobile authentication apps that are compatible with Microsoft MFA, Microsoft's Authenticator app is best matched with Azure and Microsoft 365 MFA.

You can use Authenticator to set up MFA for both your Microsoft account and other accounts homed in Entra ID, including accounts that are federated or synchronized from on-premises Active Directory. The MFA challenge/response process occurs after, and only if, the user presents valid credentials. Authenticator can operate in two modes: it can display a code (which changes every 60 seconds) that serves as the authentication challenge, or it can display a push notification prompt that allows you to accept or reject the authentication request. Push notifications only work with Microsoft and Entra ID accounts, but you can use the Authenticator app to generate codes for other apps, including Google's mobile apps and the LastPass and 1Password mobile password managers.

One interesting thing to note about the Authenticator app: just as new features tend to be delivered in the service first, with on-prem versions coming later if at all, new Authenticator features tend to accrue to the consumer Microsoft account side first, before (or if) they are rolled out to Entra ID. For example, code matching for passwordless login (which I'll discuss below) was first introduced for consumer Microsoft accounts before making its way to Entra ID. Some features (such as the ability for [Authenticator to show you alerts](#) when your Microsoft account password is changed) haven't made it to the Entra ID world yet, and they may never.

Authenticator Lite in Outlook

In March 2023, Microsoft quietly released a significant new feature: the ability for "companion apps" (their term) to implement a subset of MFA functionality without requiring the user to install a separate app. [As described here](#), the "Authenticator Lite" feature set, first added to Outlook Mobile, is a subset of what's in the full Authenticator app. Users can only use the Lite feature to approve MFA requests using number matching for authentication; they can't use it with SMS authentication, or with other non-Microsoft services, and it doesn't allow the use of self-service password reset. Originally you were required to [enable use of the companion app](#); on June 26, 2023 Microsoft enabled this for all tenants worldwide.

Basic MFA with Authenticator

There are several steps required to use Authenticator as an MFA client with Microsoft 365, all well-covered in the [Authenticator app documentation](#). First, of course, you must license (if necessary) and enable MFA for your tenant. Once that's done, you can enable individual users for MFA. The app is one of several available authentication methods you can enable or block for individual users, but the app is available to MFA-enabled users by default. To configure it for the user, here's what to do:

1. Download the Authenticator app itself from the Apple App Store or Google Play. If you have Microsoft Intune or another similar MDM solution deployed, you can use that solution to push the app to devices as well.
2. Click the **+ Add sign-in method** link, then choose "Authenticator app" and click **Add**.

3. When prompted, set up the app as directed on your mobile device. As you follow the dialogs, the web page will eventually display a QR code.
4. In the mobile app, use the + icon to add an account by using the device camera to take a picture of the on-screen QR code displayed in step 4.
5. You might be asked to enter a code from the app to verify that you've got it set up properly.
6. Visit <https://myprofile.microsoft.com> and make sure that "Microsoft Authenticator - notification" is selected as the default method. Until you set up the Authenticator app on one or more devices, you'll see an error message telling you that you need to set the app up.

Once the app is set up, when you log on to a service that requires MFA, you'll see a screen on your device like the one shown in Figure 14-2. This version shows the features added to the service to prevent "MFA challenge fatigue", including the app name and rough IP-based geolocation of the authentication request.

Authentication requests are presented on the phone as modal dialogs, so you must respond to them before doing anything else on the phone. The App Lock feature of Authenticator is enabled by default, meaning that you must be logged into the Authenticator app, and have it active, before it accepts an authentication request.

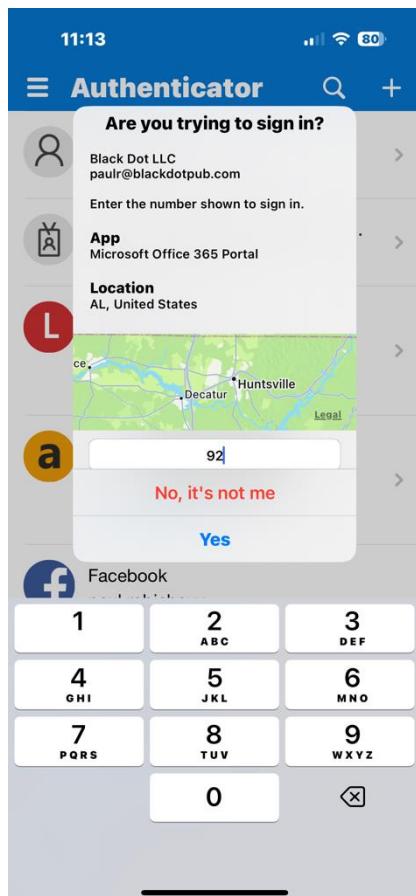


Figure 14-2: The iOS Authenticator app displays an MFA request with number matching

Using Authenticator for Passwordless Authentication

In the Identities chapter, we describe how passwordless authentication works in Entra ID. If you've enabled passwordless authentication in your tenant, you can optionally enable individual users to sign in without using a password. The way the process works is simple: when the user requests access to an app, the Microsoft authentication library will generate a two-digit challenge code and display it on screen. At the same time, the

Authenticator app will prompt the user to select the matching code from a list of 3 choices. After properly selecting the matching code, she'll be prompted to use a PIN or biometric to authenticate to the device. This approach means that no user passwords are exposed at any point, nor do they need to be stored—with no password in use, there's no way for a user to accidentally compromise it, nor for an attacker to steal it.

The [instructions to set up passwordless](#) authentication for Authenticator are reasonably detailed, but the basic steps are as follows:

1. Ensure that the [combined security information registration](#) process is enabled in your tenant.
2. Configure Entra ID to allow passwordless sign-in with the Authenticator app. This setting applies at the tenant level.
3. Each user who wants to use passwordless authentication must add the Authenticator app as an authentication method for their account.

In July 2022, Microsoft started rolling out the ability to have multiple accounts with passwordless authentication within Authenticator. Until this change hits your tenants, you'll only be able to add one passwordless account to your device.

As with all other Authenticator-based sign-in methods, if notifications don't make it to the Authenticator app the user won't be able to sign in unless they choose an alternate authentication method such as SMS.

Optimizing Microsoft 365 Client Network Access

Microsoft has published extensive guidance on [designing your enterprise network to work optimally](#) with Office 365. The primary principle they push is that you should design your network to minimize round-trip latency between the client endpoint (that is, the machine or device that the user's working on) and the "front door" service connection point that the client connects to. Traffic that reaches the front door will be carried over [Microsoft's internal network](#), which they manage with a ruthless focus on lowering round-trip latency.

To be more specific, Microsoft recommends that you consider the following when designing your network. First, you should know that Microsoft has separated Microsoft 365 service endpoints into [three categories](#): Optimize, Allow, and Default:

- **Optimize** endpoints represent roughly 75% of traffic to the service and include the *outlook.office365.com* and *sharepoint.com* name spaces. Microsoft says you should prioritize traffic to these endpoints by bypassing network inspection and proxies and ensuring the fastest possible DNS resolution for these namespaces.
- **Allow** endpoints, such as *protection.outlook.com*, are still important but are less sensitive to network latency. There are roughly 100 of these endpoints; because of this large number, many customers will choose not to do anything special with these endpoints to reduce the need for change management and control.
- **Default** endpoints have no special requirements for performance and can be treated as ordinary Internet traffic.

Second, Microsoft has some specific recommendations that you should apply to the design of your enterprise network:

- Don't use proxies, WAN accelerators, or other devices that sit between the client and the front door. Since you may very well need to do so anyway, see the section "Proxies and Network Devices" below for additional guidance.
- [Allow each office \(or client\) to connect directly to the Internet](#) instead of backhauling traffic from a remote office to a centralized data center and thence to the Internet.

- [Avoid network hairpins](#), or connections where a client's traffic exits your corporate network and then comes right back in again. Instead, you should always try to route all client traffic for Microsoft 365 endpoints directly to the Internet.

Proxies and Network Devices

Client applications and servers within your corporate network that will be connecting to Microsoft 365 will need to have access to all the appropriate endpoints. The general recommendation from Microsoft is to bypass any web proxies or other network devices that shape or rewrite traffic such as WAN accelerators, for connections to the service. That recommendation is counter to the security policies of many organizations, with the adoption of cloud services making them more likely to want to push all their internet traffic through a security or performance device.

There are good reasons for customers to want to secure their internet traffic. These days, clients on their network will be connecting to more services over HTTPS, making the traffic invisible to traditional security measures. In response, organizations implement security devices that can intercept, decrypt, and inspect HTTPS traffic to detect viruses, data leakage, and ransomware. Similarly, with so much traffic now running over internet connections, organizations try to reduce the impact on their bandwidth with WAN accelerators and traffic caching devices.

Unfortunately, such measures often result in degraded performance for clients, and in some cases, they completely break connectivity to application endpoints, causing problems such as Offline Address Book download errors, OneDrive for Business sync failure, and poor audio or video performance in Teams calls. The specifics will vary depending on the vendors involved and their ability to provide guidance and templates for properly implementing their devices into your network without impacting client traffic. If you're going to attempt to implement such measures, approach it with caution and do ample testing to ensure you don't cause problems for end-users, particularly those on BYOD devices that will require special considerations for any SSL traffic inspection you plan on doing.

There may be a happy middle ground if your chosen security devices are not fit for use with Microsoft 365, but you want to continue using them to manage other internet traffic. Bypassing security devices for clients connecting to the service is a reasonable approach but can be poorly implemented if you're not careful. The natural inclination of firewall administrators is to apply controls based on IP addresses. But as Microsoft [explains in their guidance](#), Microsoft 365 IP address ranges are a constantly moving target. To keep up, you might be making changes to firewall configurations as often as every 14 days, which is a heavy burden to carry for very little real benefit. If your device supports it, Microsoft [publishes a web service](#) that your perimeter devices can query to get updates on IP address ranges and URLs for the service. Endpoint definitions are published at the start of each calendar month and take effect 30 days after their publication.

No matter the security devices at play, NATing of outbound connections to Microsoft 365 services is also a concern; if too many clients are being NATed to the same public IP address, port exhaustion can occur, degrading performance for the clients. NATing is fully supported, but Microsoft recommends limiting the number of clients on one public IP to around 2000. This is mainly due to the number of connections a single client can have open. Outlook alone has 2-4 connections open for a basic user scenario, and more if they are also connecting to shared mailboxes, Microsoft 365 Groups, or are performing an OAB download. Once you add in other applications such as Teams or a web browser, the number of connections per client can easily be 10 or more. With a maximum of 64000 ports per public IP address, limiting NATing to 2000 clients per IP is a safe place to start. A pool of public IP addresses will be needed for NATing outbound connections if you are running a very large organization.

Real World: If you use a proxy, security, or performance device for client traffic, and you notice problems, bypassing the device is a good troubleshooting step. The goal is not to point the finger of blame at the network devices, rather it is to narrow down the likely cause of the issue. Ultimately if you choose to implement such network devices in your environment, you are better off identifying issues and working to resolve them rather than pretending they do not exist.

Split Tunnelling and VPNs

Some users may be required to connect to their corporate network through a virtual private network (VPN). This is especially common after the huge surge in telework brought on by the COVID-19 pandemic. For a lucky portion of the workforce, all the services they need are accessible directly through the Internet, but users who must use remote desktop solutions or access internal line-of-business systems are probably stuck with VPNs. The problem with combining VPN access and Office 365 is that the default VPN configuration will probably send all the user's network traffic from her computer over the VPN to the VPN endpoint on the corporate network, where it will be routed onwards. Traffic that's bound for the Internet (whether that's Office 365, Netflix, or something else) will thus have to traverse the VPN and then be sent onwards, with return traffic taking the same path. Microsoft calls this behavior "forced tunneling."

The solution to the performance problems caused by forced tunneling is to allow Microsoft 365 traffic to go straight to the Internet, a configuration known as *split tunneling*. When you [enable split tunneling on the VPN connection](#), traffic to select destinations is allowed to go directly to the Internet. Microsoft's guidance on how to enable split tunneling lists a set of "Optimize" endpoints that you should allow traffic interchange with over the Internet. The specifics of how you implement this are up to the specific VPN solution you use.

Checking Office Client Network Connectivity

Microsoft offers basic network connectivity monitoring in the Microsoft 365 admin center. This monitoring uses telemetry sent by the OneDrive for Business client on Windows computers to assess several aspects of your connectivity, including whether user traffic from a particular location is going to the optimal service front door location and whether there are excessive backhauls. As an example of the real-world problems this testing can catch, an early version of the connectivity tester identified that some traffic from a facility in Slovakia was being (incorrectly!) routed to Macomb, Michigan, more than 7,200 kilometers away. The unnecessary extra routing caused some additional delay for some types of traffic, but not enough delay to be routinely noticeable.

Chapter 15: Managing Devices

Brian Desmond

As workers access more and more data from mobile devices and security risks for corporate data increase, the management of mobile devices becomes an increasingly important factor in daily operations. Organizations have a choice of solutions for mobile device management (MDM) and mobile application management (MAM). Each of these solutions offers different features, strengths, and weaknesses.

Let's start with a quick definition to separate MDM and MAM. MDM refers to controlling the entire device, whereas MAM is concerned only with controlling the behavior of specific applications and the associated data on the device. This may seem like an obvious distinction, but there are some subtle points to it. For example, is it better to enforce a requirement to use a PIN on the entire device, or just on applications that contain corporate data? Your security team might prefer the former, but your users might prefer the latter.

Some of the considerations that come into play when planning for a mobility strategy include:

- The devices and operating systems within scope.
- Who owns the target devices (bring your own device (BYOD) versus corporate).
- The applications running on the devices (Microsoft, other vendors, and custom apps).

Some organizations can take a unified approach to mobility management, while others need to apply different policies and configurations to deal with different sets of use cases. Specific compliance requirements are also important, as some organizations fall under strict government or industry regulations.

At a high level, there are three solutions that you can choose from in Microsoft 365:

- Exchange ActiveSync.
- Microsoft 365 Basic Mobility and Security (BMS).
- Microsoft Intune.

In addition to Microsoft solutions, there is an extensive range of third-party mobility solutions provided by other vendors. Here, we focus on Microsoft Intune.

Comparing the Three Solutions

Before we dig into the details of Intune, let us take a quick look at the three options Microsoft offers. Consider this section somewhat of an executive summary to help you understand the basic capabilities and tradeoffs of each.

Exchange ActiveSync costs you nothing. It works on a very broad range of devices, and it offers basic device management functionality. It is only loosely integrated with the rest of Microsoft 365; it is very much Exchange-centric. It is not undergoing active development and it is increasingly being replaced by Microsoft's other solutions.

Microsoft 365 Basic Mobility and Security (BMS) offers a [broader set of functions](#) than Exchange ActiveSync, including the ability to secure access to documents stored in OneDrive for Business and SharePoint Online. It also gives you more control over which devices you want to allow to connect, and what they can do when they do connect. There is no additional cost for BMS if you have an enterprise or business subscription.

Microsoft Intune is a full-fledged MDM and MAM solution. It does everything ActiveSync and BMS do, plus much more. For example, Intune can also manage Windows PCs, macOS devices, Chrome OS, and Linux devices, and you can manage access to individual applications and their features even for devices that are not enrolled in Intune for MDM. This is extremely useful in environments that have BYOD policies. Intune requires you to buy licenses, through Microsoft 365, the Enterprise Mobility + Security suite, or as a standalone license. Table 15-1 summarizes the differences between the three options.

Feature	Licensing requirements	Manages data	Manages apps	Manages devices
Exchange ActiveSync	Included with Exchange Online	Exchange only (online and on-premises)	No	Limited (PIN, device encryption)
Microsoft 365 Basic Mobility and Security	Requires Office 365 enterprise or business	Yes, for most Microsoft 365 workloads	Limited	More than Exchange ActiveSync
Microsoft Intune	Requires EMS, Microsoft 365, or standalone license	Yes, including conditional access	Extensive	Extensive

Table 15-1: Choices for mobile device management

With that bit of perspective, let's dig into how you can use Microsoft Intune to manage mobile devices and apps.

Getting Started with Intune

In this chapter, we discuss how to use Microsoft Intune. More specifically, we will focus on managing Apple iOS/iPadOS and Android devices. Intune also supports Windows, Linux, and macOS devices too, but we will not discuss those capabilities. If you are just starting with Intune, there are a few tasks you will need to do to configure your tenant to work with Apple and Google services. You may also wish to configure branding to make the end-user experience more familiar to your users.

Unless we note otherwise, all the tasks discussed here are performed in the [Microsoft Intune admin center](#). Your account must be a member of the Global Administrator or Intune Administrator role to manage Intune.

Company Portal

The Company Portal application is how you enroll most devices into Intune. If you will be doing MDM or MAM on Android devices, your users must install the Company Portal app from their device's app store. Starting with iOS 15, you can choose to have users enroll using the Company Portal, or they can use [just-in-time \(JIT\) enrollment](#) via the Authenticator app. The Company Portal app is responsible for brokering Intune's MDM capabilities as well as providing a private app store, and a place to manage your device on iOS and Android. On Android, even if you choose not to use MDM, the Company Portal serves as an authentication broker. As an authentication broker, the Company Portal is responsible for enabling an integrated single sign-on experience across Microsoft's mobile apps. On iOS, Microsoft's Authenticator app serves as the authentication broker.

You can customize the Company Portal to show your organization's name, logo, colors, and other branding elements. While these items are not mandatory, they do provide a familiar look and feel to end users. To customize the app, browse to **Tenant administration > Customization** in the admin center. Microsoft documents the specific requirements for branding elements, as well as certain best practices [in their documentation](#). We recommend that you work with stakeholders in your organization such as marketing

and/or internal communications teams to select branding elements that best represent your organization. Sometimes this process can take a while, so do not leave it until the last minute.

Apple Device Enrollment

Before you can enroll your first Apple device, you must configure an important certificate in Intune. This certificate is used with the Apple Push Notification Service (APNs). The APNs does exactly what the name suggests: it lets Intune send push notifications to your devices. You can request this certificate for free from an Apple website with a few minutes of work. Once a year, you must renew the certificate. It is **extremely** important that you do not forget to renew the certificate. If you do, you must re-enroll your devices.

To setup your Apple MDM push certificate, browse to **Devices > iOS/iPadOS > iOS/iPadOS enrollment** in the admin center and click on **Apple MDM Push certificate**. The next screen takes you through the process step-by-step. Intune will provide you with a certificate signing request (CSR) in step 2 that you upload to the Apple Push Certificates Portal [linked](#) in step 3. If you have never used this portal, you must register for an Apple account first. It is very important that you do not use a personal email address for this account. Your organization's APNs certificate is permanently linked to the account you use. Instead, you should use a shared email address such as a distribution list or shared mailbox to complete the registration.

The screenshot shows the 'Certificates for Third-Party Servers' page. At the top right is a 'Sign out' button. Below it is a green 'Create a Certificate' button. The table lists two certificates:

Service	Vendor	Expiration Date*	Status	Actions
Mobile Device Management	Microsoft Corporation	Apr 27, 2022	Active	Renew Download Revoke
Mobile Device Management	Microsoft Corporation	Apr 27, 2022	Active	Renew Download Revoke

*Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.

Figure 15-1 Apple Push Certificates Portal

Click **Create a Certificate** (Figure 15-1) and upload the CSR Intune generated. You will then be able to download the APNs certificate and upload it to Intune in Step 5. In Step 4, you must enter the email address of the Apple account you registered. Click **Upload** and you will be ready to enroll iOS devices using the Company Portal app.

You can also use the Apple Configurator application or Apple's automated device enrollment program to enroll iOS devices. However, we do not cover these topics here.

If you want to allow your users to use JIT or web based enrollment on Apple devices, you must configure an enrollment type profile for those users. To do this, browse to **Devices > iOS/iPadOS > iOS/iPadOS enrollment** and click **Enrollment types**. Click **Create profile > iOS/iPadOS** on the toolbar and give your profile a name. Choose the **Web based device enrollment** enrollment type. On the Assignments tab, you can make web based enrollment available to a group of users, or you can click **Add all users** to make it available to everyone.

To use web based enrollment, users must have the Microsoft Authenticator app installed on their device. To start the enrollment process, users can browse to <https://portal.manage.microsoft.com> or they can access a Microsoft app such as Microsoft Teams that is protected by a conditional access policy requiring device compliance. You can also use other apps if you [configure the Apple single sign-on \(SSO\) extension](#), discussed later in this chapter.

Android Device Enrollment

While Apple makes device enrollment a universal process, Android offers a plethora of options for enrolling your devices. Android's enrollment options primarily revolve around Android Enterprise. With Android Enterprise, you have a choice of five MDM enrollment options:

1. **Android Enterprise personally-owned with a work profile** – use this option for BYOD devices that also need to access and store corporate data. Android separates corporate data and does not let the MDM system control personal data.
2. **Android Enterprise corporate-owned with a work profile** – use this option for devices your organization owns that you also allow end users to store/access personal data and apps from.
3. **Android Enterprise fully managed** – use this option for devices your organization owns that should be 100% controlled by Intune. Do not use this option if users are storing personal data on the device. Fully managed devices can also be automatically enrolled via zero touch enrollment.
4. **Android Enterprise dedicated** – use this for devices that serve a singular purpose such as for a walk-up kiosk. Dedicated devices are restricted to a specific set of apps that can be used on the device.
5. **Android Open-Source Project (AOSP)** – use this for devices that do not interact with Google Mobile services.

Regardless of the enrollment option(s) you choose, you will need to connect Intune to the Google Play store. To do this, browse to **Devices > Android > Android enrollment** in the admin center, and click on **Managed Google Play**. Click **Launch Google to connect now**. You will need to create a Google account or sign-in with an existing one. Much like Apple, you should not use a user-specific email address for this account. Use a distribution list or shared mailbox. Once you sign-in, supply your organization's name, agree to the terms and conditions, and click **Confirm**. Once this is complete, you are ready to begin enrolling Android devices.

Enrollment Restrictions

If you plan to use MDM to manage some (or all) of your devices, you may also be concerned with what devices can enroll. By default, any user in a tenant assigned an Intune license can enroll up-to five devices. You can alter the maximum number of enrolled devices per-user (up-to 15) or restrict users to only enroll certain operating systems (iOS or Android) or operating system versions, Android enrollment type (Enterprise or device administrator), Android device manufacturer, and/or block personally owned devices from enrolling.

To create or manage any of these restrictions, browse to **Devices > Enrollment > Device limit restrictions** or **Device platform restrictions** in the admin center. The default profiles cannot be deleted, and they apply to everyone in your tenant. You can assign alternative restrictions that take precedence by clicking **Create restriction** on the toolbar. These alternatives can either be assigned to all users in your tenant, or to specific users or groups. If, for example, you need to permit certain users to participate in a BYOD program while other users can only use corporate devices, you can create two device type restriction profiles and assign them to separate groups.

Device Categories and Enrollment Types

If you need to classify the types of devices used in the organization, device categories may be helpful. Device categories provide a list of options end users must choose from in the Company Portal when they enroll a mobile device. These can be anything you want. For example, you might create categories for departments like *Manufacturing* and *Sales* or you might categorize devices by purpose, e.g., *Point-of-Sale* and *Quality Control*. The options you choose are persisted on the device's record in Entra ID. This is helpful because you can create dynamic groups in based on a device's category (amongst other options).

Entra ID updates dynamic group membership as devices change. You can then deploy Intune configuration items like apps, profiles, and policies to these groups. If you have a set of apps that are only used by Manufacturing devices, for example, you can see how this capability can be useful. To configure device categories, browse to **Devices > Device categories** in the admin center and then click **Create device category** on the toolbar.

iOS devices can also be forced to enroll at the device or user level during enrollment. This can be pre-determined based on the group membership of the user enrolling, or the user can select the device type during enrollment. To configure this, browse to **Devices > iOS/iPadOS > iOS/iPadOS enrollment** and then click **Enrollment types**. Like device categories, you can create a dynamic group based on the device enrollment type.

Device Updates and Intune

As Apple and Google evolve the iOS and Android operating systems (OS), Microsoft also evolves their minimum supported OS versions. Generally, this does not present an issue since devices typically update automatically or make an ongoing effort to ask the end-user to perform the update. However, as devices age, they may no longer be compatible with the latest OS versions.

When you have a BYOD program, and older devices are no longer supported by Intune, it can be difficult to inform end users that they must purchase a new device to continue accessing your organization's resources. Microsoft begins communicating planned OS support changes well in advance in the [Notices](#) section of the Intune docs.

For Apple devices, Microsoft supports iOS 16 and better. For Android devices, Microsoft supports Android 10 and better. For up-to-date support information, refer to the [supported operating systems](#) documentation. Microsoft typically supports the three most recent versions of iOS and four most recent versions of Android. Android Enterprise dedicated devices, AOSP user-less devices, and Teams Room Android-based devices have separate support lifecycles. As new versions are released, Microsoft will plan to deprecate support for earlier versions. While these supportability limits apply to device enrollment, individual applications (e.g., Teams) may have different support lifecycles for iOS and Android.

Managing Apps

Regardless of whether you choose MDM, MAM, or both, chances are you will need to manage some aspect of the apps on a device. For many organizations, Intune's MAM capabilities combined with the Microsoft Office apps (and select third-party apps) provides a good balance of control over corporate data while not putting controls on a BYOD device. If you use MDM, you will likely also use MAM to manage the apps on the device, but you might also want to use Intune to install apps on the device, or provide a curated app store in the Company Portal app.

App Deployment

Intune has two app deployment options: "required" and "available". Depending on whether you are working in the context of MDM or MAM, the options for how you install apps on mobile devices varies. If a device is MDM enrolled, you can use either option. When an app is deployed as "required", it will automatically be installed on the device. You can also choose to require uninstallation of an app you have previously deployed as "required". On the other hand, "available" publishes the app in the Company Portal. End users can click on "available" apps in the Company Portal, and they will be installed on their device.

Whether you choose required or available, you need to target your app deployment to a group of users or devices. Intune uses Entra ID groups to know what users and devices to target. You can either use an existing group or create a new one. If you simply want to target an app deployment to everyone, you can choose "all devices" or "all users". Be careful if you try to mix groups containing users and devices. Intune does not try to resolve the relationship between users and their devices so you may not get the results you want. As a best practice, we recommend that you stick with assigning to users or devices, but not at the same time.

To deploy an app, browse to **Apps > All apps** in the admin center. Click **Add** on the toolbar and choose **Android store app** or **iOS store app**. In this example, we will create a deployment for Microsoft Outlook for Android. The process is very similar for iOS. You will need the URL of the application from the Google Play store which you can find by searching the store at <https://play.google.com/store/apps/>. Fill in the details for the application as shown in Figure 15-2. You can copy and paste all the details from the app's store listing.

While you do not need to provide optional details like the category or logo, they greatly enhance the user experience in the Company Portal. You can obtain the logo by saving the image in the app store listing as a PNG file and then uploading it to Intune. The category is used to help end users find apps that are available for installation in the Company Portal. There are nine built-in categories that come with Intune. You can add your own categories by browsing to **Apps > App categories** in the admin center.

The screenshot shows the 'Add App' form in the Microsoft Intune Admin Center. The top navigation bar includes 'Add App', a three-dot menu, and tabs for 'App information', 'Scope tags', 'Assignments', and 'Review + create'. The 'App information' tab is selected. The form fields are as follows:

- Name ***: Microsoft Outlook
- Description ***: Connect and coordinate your busy life with Microsoft Outlook. Stay on top of your day through a secure email and calendar app that lets you manage your
- Publisher ***: Microsoft Corporation
- Appstore URL ***: <https://play.google.com/store/apps/details?id=com.microsoft.office.outlook>
- Minimum operating system ***: Android 8.1 (Oreo)
- Category**: Productivity
- Show this as a featured app in the Company Portal**: No
- Information URL**: Enter a valid url
- Privacy URL**: Enter a valid url
- Developer**: (empty)
- Owner**: (empty)
- Notes**: (empty)
- Logo**: Change image (with a preview of the Microsoft Outlook logo)

Figure 15-2: App deployment for Microsoft Outlook for Android

Once you configure the app information, you can assign the app to users or devices. When you create an app assignment, you have several options to choose from. The assignment options are very similar across everything you will do in Intune. Fundamentally, you can assign apps to groups of users and/or devices by setting the **Group mode** to **Included**. If you need to exclude certain users or devices, you can change the

Group mode to Excluded. Make sure you do not combine groups of users and devices, or you might see unexpected results. If, for example, you include a group of users and exclude a group of devices, Intune will not filter those devices as you would expect. If you need to only include or exclude certain devices in combination with users, use a Filter. We discuss Filters later.

For apps, you have a choice of assigning the app as **Required**, **Available for enrolled devices**, or **Available with or without enrollment**. Apps assigned as required will be automatically installed on devices. Apps assigned as available will be displayed in the Company Portal app for end users to install. The choice of whether to make apps available only to enrolled devices (MDM) or with or without enrollment (MDM or MAM) gives you additional control over when users can select the app for installation.

If you are not ready to deploy the app, this step is optional. If you do list one or more groups, the deployment will begin as soon as you click **Create** and complete the wizard. Find your app under **Apps > All apps** and click the app to monitor deployment status, change the properties of the app, or modify what users or devices the app is deployed to. For iOS devices, you can also edit the assignment and configure the **Prevent iCloud app backup** setting. This prevents app data from being backed up to iCloud.

You can use the **App install status** report under **Apps > Monitor** to keep an eye on your app deployments. From here you can investigate the progress of a specific app deployment and see installation failures at-a-glance. To investigate a specific app, click on the row to go to the status dashboard for that app.

Bulk Purchased and Private Apps

Both Apple and Google support managed app procurement and the ability for app publishers to advertise private apps to select customers. Apple manages this process through the Apple Business (or School) Manager, while Google uses the managed Google Play store. With both Apple and Google, once you approve or make a bulk purchase of an app, Intune will allow you to synchronize your app library and the apps will become available for deployment using the same process as we described earlier in this section.

With Apple, you must enroll an account in Apple Business Manager. This process requires several steps and data about your organization. Apple documents this process [here](#). Once you have obtained an Apple Business Manager account, you can browse to <https://business.apple.com> to login. Next, you must connect Intune to Apple Business Manager. To do this, go to **Settings > Apps and Books**. Click the **Download** link under **My Server Tokens**.

Next, in the Microsoft Intune admin center, go to **Tenant administration > Connectors and tokens > Apple VPP Tokens** and click **Create** on the toolbar. Give the token a name, provide the Apple ID you used to login to Apple Business Manager, and upload the file you downloaded in the previous step. Intune will automatically synchronize with Apple Business Manager the first time, but you can manually synchronize by selecting the token clicking the ellipsis (...) and clicking **Sync**.

To make apps available for Intune in Apple Business Manager, you must buy licenses (even if they are free) for the app in the **Apps and Books** area of Apple Business Manager. When you buy the license, you must be sure to assign it to the location that you downloaded the server token for in the previous step. If you have multiple locations configured, you must add a token for each location to Intune. If you are attempting to work with a private app and you do not see a Custom Apps area, go to **Settings > Enrollment Information** in Apple Business Manager and configure **Custom Apps** to **Enabled**.

Once you have bought licenses for an app, synchronize the token in Intune, and you will find the apps under **Apps > iOS/iPadOS**. You can assign these apps the same way you assign any other app. Occasionally Apple updates their terms and conditions. When this happens, the sync between Intune and Apple Business

Manager will stop working until you sign-in to Apple Business Manager and accept the updated terms and conditions.

App Protection Policies

MAM is a core component of managing your organization's data on mobile devices. With MAM and Intune's app protection policies, you can apply controls to your data in apps that support MAM while leaving personal data untouched. This often creates a good balance of control versus autonomy in a BYOD program. MAM is primarily supported by Microsoft's Office applications on iOS and Android, but Microsoft publishes an SDK and an app wrapping tool that let third parties and in-house developers support MAM too. Zoom, Adobe Acrobat Reader, and Box are examples of third-party apps that support MAM.

To implement MAM, you use app protection policies. These policies define what users and the supported mobile apps can do with your organization's data. For example, you can allow copy and paste between managed apps, but, if a user tries to copy managed data from Microsoft Word to Gmail, you can block this. You can also protect access to your data in managed apps by requiring a PIN to access the app rather than requiring a device PIN. The settings and capabilities are slightly different between iOS and Android, but fundamentally, the concepts are the same.

To create an app protection policy, browse to **Apps > App protection policies** in the admin center, click **Create policy** and select **iOS/iPadOS** or **Android**. For this example, we will create an iOS policy. Once you give the policy a name, you will need to select the devices and apps that the policy applies to. On the **Apps** tab, you can either select specific apps to apply the policy to, or use curated collections maintained by Microsoft. In the Target Policy to menu, you can choose from the following options:

- **All Apps** – automatically apply the policy to all publicly available apps that support app protection. Microsoft maintains [a list in the documentation](#).
- **All Microsoft Apps** – automatically apply the policy to any Microsoft-published app that supports app protection.
- **Core Microsoft Apps** – automatically apply the policy to a small set of "core" Microsoft-published apps including the Office apps, Microsoft Teams, and Edge.
- **Selected apps** – allows you choose the specific apps the policy applies to.

If you use any of the curated collections, Microsoft will update them from time-to-time as new apps become available that support app protection.

If you want to select specific apps, configure **Target Policy to** to **Selected apps** and use the **Select public apps** link to target your policy to apps available in the app store. If there is an app that is available in the app store but not listed, or you develop an app that integrates with Intune, use the **Select custom apps** link to target the policy to the app.

Unlike app deployments, app protection policies can only be targeted to users. If you have a mixture of MAM and MDM devices, you might want to have one app protection policy for MAM-only devices that requires a PIN to access managed apps, while on MDM devices, you might require a PIN to access the device, rendering a second PIN to access managed apps unnecessary. If you need this level of control, add a **Filter** (discussed later) to the assignment.

The bulk of the MAM controls are configured on the **Data protection** screen:

- **Backup org data to iTunes and iCloud backups** – controls whether your organization's data can be backed up to Apple's iTunes/iCloud services. We generally recommend selecting **Block**.

- **Send org data to other apps** – what apps on the device can the end user transfer data between using iOS' sharing tools. We generally recommend selecting **Policy managed apps** or **Policy managed apps with Open-In/Share filtering**. These controls allow the end user to move organizational data between other MAM-managed apps, but not to unmanaged apps. If you select **Policy managed apps with OS Sharing**, end users will be able to send organizational data to apps that are deployed via MDM enrollment as well as MAM-managed apps. If you have a special case that isn't MAM-managed or MDM-deployed, you can use **Select apps to exempt** to enable sharing. For specific application links (e.g. Apple Maps), you can use the **Select universal links to exempt** setting to permit sharing data to the unmanaged application.
- **Save copies of org data** – can the user "save as" to an alternate location. The user interface (UI) for this control is confusing. It is recommended to select **Block** and then modify the **Allow user to save copies to selected services** to enable locations like OneDrive for Business and SharePoint, the device's Photo Library, Local Storage, or Box. If you block saving copies of data completely, you can also use an App Configuration policy to block caching of company data in Office applications running on Android devices by configuring [this setting](#).
- **Transfer telecommunications data to** – controls whether the user can click on a phone number in an email, for example, to dial the number. By default, **Any dialer app** lets the user use any calling application (whether the native Phone app or otherwise), but, you can restrict this if you need to.
- **Transfer messaging data to** – controls whether the user can click on a phone number in an email, for example, to send a SMS/MMS (text) message to the number. By default, **Any messaging app** lets the user use any messaging app (whether the native Messages app or otherwise), but, you can restrict this if you need to.
- **Receive data from other apps** – indicates whether managed apps can receive data from other apps. If you select the default, **All apps**, a user can transfer data from their personal email to their corporate email (for example). **Policy managed apps** allows managed apps to only receive data from other MAM-managed apps. Finally, **Any app with incoming org data** treats received data as organizational and protects it even if it does not come from a MAM-managed app. Like the **Save copies of org data** setting, if you want to choose specific data sources, you must select **Block**.
- **Restrict cut, copy, and paste between other apps** – this is an important data sharing control that determines whether an end user can copy organizational data and paste it into an unmanaged app, or vice-versa. We generally recommend selecting **Policy managed apps with paste in**. This enables full cut/copy/paste between managed apps, but also enables an end user to copy *from* an unmanaged app and paste it into a managed app.
- **Third party keyboards** – iOS supports alternative keyboards that can be installed from the iTunes Store. These keyboard apps can present a security risk since they have access to every keystroke.
- **Encryption** – enforces encryption of organizational data on the device. The downside of this is that it requires the user to have a device PIN which you may not wish to enforce.
- **Sync policy managed app data with native apps** – this is a roundabout way of saying if Outlook Mobile, for example, can add contacts to the native contacts app. There are more elaborate controls specific to Outlook Mobile that you should use if this setting is of interest.
- **Printing org data** – as the name implies, can an end-user use the native iOS printing functionality inside a managed app?
- **Restrict web content transfer with other apps** – if you want to require Microsoft Edge for browsing or to bring data into managed apps, you can use this control.
- **Org data notifications** – controls whether managed apps can create notifications on the device (or a companion device like an Apple Watch). These notifications can potentially disclose sensitive data such as in the subject of a meeting invitation.

Next, you can further restrict access to managed apps in the **Access requirements** tab by requiring the user to enter a PIN or biometric (e.g., TouchID) and/or login with their corporate credentials (the **Work or school account credentials for access** setting). Typically we find that these settings are useful if you are not using MDM. Without MDM, you cannot guarantee that users have setup security to unlock their device. By using the settings on the Access requirements tab, you can implement equivalent security controls to launch apps protected by the policy.

You may also wish to apply additional security precautions on the **Conditional launch** screen. These controls are divided into two sections: **App conditions** and **Device conditions**. App conditions control the behavior of managed apps (e.g., has the device been offline for too long, has the user entered too many invalid PINs, or what to do if their account disabled in Entra ID) and what happens (e.g., restricting access or wiping data). Device conditions inspect the status and health of the device (e.g., is the device jailbroken, is it running a minimum OS version, and/or is it at an acceptable risk level as reported by a [mobile threat defense \(MTD\) solution](#)). Like app conditions, device conditions can take actions such as blocking access to data or wiping the data entirely.

Finally, you must assign the policy to one or more groups of users on the **Assignments** tab. Once this is complete, click **Create** and complete the wizard. You can come back to the **Apps > App protection policies** screen later to monitor the status of the policy or make changes. New apps that support MAM periodically become available so you should occasionally check that you are including all the desired apps in the policy.

Once you deploy your policy, use the **App protection status** report under **Apps > Monitor** to keep track of your policy. The dashboard in this report gives you an at-a-glance view of how many users are protected by the policy, the top apps, and any errors that you should investigate. To get more detail, you can use the download links on the toolbar, such as **App protection report: iOS, Android** to export the data to a CSV file.

Email Client Configuration

Generally, we recommend choosing Outlook Mobile as the mobile email client for Exchange Online whenever possible. It provides the most complete combination of Microsoft 365 integration and administrative control. However, you may need to support the native email client on mobile devices as well. iOS in particular supports complete configuration of a profile in the native email client for MDM enrolled devices. Android devices support relatively limited pre-configuration of the Gmail and Nine for Work email apps. Outlook Mobile for iOS and Android can be pre-configured regardless of whether you use MDM or MAM.

iOS Native Mail Client

To deploy settings for the native mail client to MDM enrolled iOS devices, you will need to create an email configuration profile. To begin, browse to **Devices > Configuration profiles** in the admin center and click **Create profile**. Select **iOS/iPadOS** for the **Platform** and **Templates** for the **Profile type**, and **Email** for the **Template name** and then click **Create**. You will need to complete the following fields to configure the profile:

- **Email server** – the ActiveSync endpoint to connect to. For Office 365 in the commercial cloud, use outlook.office365.com.
- **Account name** – this is shown in the iOS mail app as the name of the email account. You could use the name of your organization, for example.
- **Username attribute from Microsoft Entra ID** – Select the user's username as in Entra ID. Generally this is the User Principal Name (UPN), but if you are connecting to an on-premises Exchange server, you might need to pick sAMAccountName, for example.

- **Email address attribute from Microsoft Entra ID** – Select the user's primary email address as stored in Entra ID. If your UPN does not match the primary email address, then you will need to select Primary SMTP Address.
- **Authentication method** – select Username and password unless you are using client certificate authentication.
- **SSL** – select Enable.
- **OAuth** – this enables modern authentication. For Office 365, and any on-premises Exchange organization using modern authentication, select Enable.
- **Exchange data to sync** – generally you will select All data, however you can filter this to a subset. You might want to combine the **Calendar only** option with Outlook Mobile to provide access to the native Calendar app while using Outlook mobile for email and contacts, for example.

The remaining choices control behavior of the native mail app and are not critical for deploying an email profile. You can also require a VPN tunnel for the email profile if your email server is not accessible over the Internet. Like deploying an app, you must target one or more groups of users or devices on the **Assignments** screen. Once this is complete, you can click **Create** to complete the wizard. You can monitor the status of your email profile deployment as well as modify settings and assignments by browsing to the profile under **Devices > Configuration profiles**.

One important thing to note is what will happen if you deploy an email profile to a device that already has a matching profile as determined by the Email server and Account name fields. Intune will not allow the profile to be installed. Instead, the end user will receive a notification that they must delete the profile that is already installed on their device. Intune will subsequently install the profile you have configured.

Outlook Mobile

You can configure Outlook Mobile much more granularly than the native email client apps. In conjunction with an app protection policy, Outlook Mobile gives you a great deal of control over how the app behaves and what end users can do with your data. To configure Outlook Mobile, browse to **Apps > App configuration policies** in the admin center and click **Add > Managed apps**. Give your policy a name and click **Select public apps**. Select **Microsoft Outlook** for iOS and/or Android and then click to go to the **Settings** screen.

Microsoft documents all the Outlook Mobile configuration settings [here](#). Most of these settings are listed in Intune under **Outlook configuration settings** and are self-explanatory. Sometimes, though, Outlook Mobile introduces new settings before Intune catches up. You can use the **General configuration settings** in Intune to set these settings. For example, if you want to prevent end-users from adding a personal email account to Outlook Mobile, add a row under General configuration settings that looks like Table 15-2.

Name	Value
IntuneMAMAllowedAccountsOnly	Enabled

Table 15-2 Outlook Mobile custom configuration settings

All the settings for Outlook Mobile are documented and can be configured like the example in Table 15-2, however most are also listed in a much more friendly manner under **Outlook configuration settings**. Before you use General configuration settings, take a minute to confirm that is the only way. The raw settings are also useful if you are using a third-party MDM solution.

App Selective Wipe

One of the benefits of MAM is the ability for Intune administrators to wipe organizational data without touching a user's personal data. This is useful when a user leaves the organization, for example. You can target a selective wipe to a specific device or all the user's devices. Once a selective wipe request is created for a user, it will remain until you delete the request.

To create a selective wipe request, browse to **Apps > App selective wipe** in the admin center. To selectively wipe organizational data on specific device, click **Create wipe request** on the toolbar. To selectively wipe organizational data on *all* a user's devices, open the **User-Level Wipe** tab and then click the **Add** hyperlink at the bottom of the list.

Select a user and/or their devices to create the request. You can open the request and monitor the progress of the wipe request for each managed app on each of their devices.

App Configuration

Some applications support managing how the application works through Intune. For example, Outlook Mobile provides this capability as discussed above. Microsoft Edge is another example. These capabilities are not specific to Microsoft, however. You might need to specify a server for a line-of-business application to connect to, or you might need to change how the application behaves so that it can correctly interact with conditional access policies.

To create an app configuration policy, browse to **Apps > App configuration policies** in the admin center and then click **Add > Managed devices** on the toolbar. Select the platform you are targeting (iOS or Android), and the app you will configure settings for. You must select an app that you have previously deployed in Intune. Next, you can choose how you enter the settings. In the **Configuration settings format** menu, **Use configuration designer** gives you a simple GUI for data entry, while **Enter XML data** is useful if the app developer has provided pre-configured settings that you can paste into Intune.

Finally, you must assign the app configuration policy to users or devices. The settings will be applied to the targeted app on any device that has the app installed.

Managing Devices

Now that we have discussed managing apps on devices, what if you want to also manage the device itself? To do this, you will use the MDM capabilities of Intune. With MDM, you have substantial control of every facet of the device, limited only by what the device's operating system lets you do. There are countless scenarios for how you deploy MDM, and thousands of settings that you can control on devices. We will not dive into all these settings or scenarios, but we will show you how to get started.

Configuration Policies

You use configuration policies to control the behavior of devices, as well as install organizational settings such as wireless networks, virtual private networks (VPNs) or PKI certificates. Configuration policies are specific to device platforms (iOS or Android) and must be configured individually for each. To create a configuration profile, browse to **Devices > Configuration** in the admin center and click **Create > New Policy** on the toolbar. You will need to select a **Platform** (e.g., iOS/iPadOS), **Profile type**, **Template** and **Template type**, or browse the **Settings catalog**. Most of the time, we expect you will use the **Device features** and/or **Device restrictions** templates. Settings catalog policies let you see every setting supported by the device platform in one searchable list.

As you explore the configuration settings available in your policy, pay attention to the notes and information tips that Intune displays. Many settings are very specific about when and how they apply. For example, some iOS settings apply to any MDM enrolled device, while others only apply to *supervised* devices that are enrolled through Apple's automated device enrollment program.

Once you have configured the policy as you desire, assign it to one or more groups of users and/or devices. You can combine groups of users and devices and even exclude certain groups. As a reminder, be very careful if you decide to combine user and device groups in your policy assignment! You may find that it does not work the way you expect. If you need to only include or exclude certain devices in combination with users, use a Filter. Like other assignments, you can come back to your configuration policy later to monitor the status of the deployment or make changes.

Device Inventory and Actions

Intune collects many data points about enrolled devices and makes it available to you in the properties of the device. You can learn about device hardware and installed apps, explore the status of configuration profile deployments, and check on app deployments. All this information is available by browsing to **Devices > All devices** in the admin center and clicking on a specific device. You can also use Intune's reporting features, which we will discuss later, to learn about this information for many devices at once.

In the same screen, you can also remotely take a limited number of useful actions on MDM enrolled devices. These actions are all accessible by. Actions you can take include:

- **Retire** – wipes managed app data and settings and removes the device from Intune. The user's personal data is retained.
- **Wipe** – removes all data from the device, resets the operating system settings, and unenrolls the device from Intune. Optionally, you can choose to preserve user data on the device.
- **Remote Lock** – returns the device to the PIN lock screen.
- **Remove Passcode** – removes the device passcode, such as in scenarios where the user has forgotten their PIN.

These actions are primarily useful when someone leaves the organization or if a device is lost or stolen. Note that some of these actions are not supported in certain Android Enterprise and AOSP configurations. From the **Devices > All devices** screen you can also perform these actions in bulk on many devices by clicking **Bulk device actions** on the toolbar. Be very careful using this tool! You could accidentally wipe many devices at once.

Storing Custom Device Properties

Intune and Entra ID track various properties of devices such as their model, operating system version, etc. You might want to keep track of information that is specific to your organization too. For example, what department does a device belong to, or is the device approved for specific uses? To do this, you can use device extension attributes. You can use device extension attributes to populate dynamic groups or in device filters that are applied to a conditional access policy.

To populate device extension attributes, you must use the Graph API. Microsoft does not currently make an editor available in the admin center. You can use the Microsoft Graph [PowerShell SDK module](#), the [Graph Explorer](#), or a custom script or program. In the example below, we use the Graph Explorer to populate `extensionAttribute1` with the value 'Finance Department'.

1. Obtain the Object ID of the device you want to update by logging in to the Entra admin center and navigating to **Devices > All devices**. From there, find the device you are planning to update, and click **Properties**.
2. Browse to the Graph Explorer at <https://developer.microsoft.com/en-us/graph/graph-explorer>.
3. Click **Sign in to Graph Explorer** on the left side of the screen.
4. If necessary, click **Modify permissions** and then click **Consent** for the *Device.ReadWrite.All* permission.
5. Configure your query with the following parameters:
 - a. **Method** – Patch
 - b. **Version** – v1.0
 - c. **URL** - <https://graph.microsoft.com/v1.0/devices/<device Object ID>>
6. Configure the body of the query with the following JSON:

```
{
  "extensionAttributes": {
    "extensionAttribute1": "Finance Department"
  }
}
```

7. Click **Run query**. A response of “No Content – 204” indicates success. You can modify Step 5 to use the Get Method to confirm the results of your update.

The equivalent command using the Microsoft Graph PowerShell SDK is:

```
$Attributes = @{
  "extensionAttributes" = @{
    "extensionAttribute1" = "Finance Department"
  }
} | ConvertTo-JSON
Update-MgDevice -DeviceId $DeviceId -BodyParameter $Attributes
```

For more information on using Device Filters or dynamic groups, refer to the Identities chapter.

Enrollment Notifications

You can configure Intune to send end users an email and/or push notification when they enroll a new device for MDM. This is a helpful security feature that lets you provide a notification of an activity that could be potentially fraudulent. To configure enrollment notifications for iOS devices, browse to **Devices > iOS/iPadOS > iOS/iPadOS enrollment** and click on **Enrollment notifications**. The same capability is available for Android devices under **Devices > Android > Android enrollment**.

To create an enrollment notification policy, click **Create notifications** on the toolbar. You will need to configure the following settings to configure the policy on the **Notification settings** screen:

- Send Push Notification – Set this setting to **On** to send a push notification to all of the user’s enrolled devices.
- Push Notification - Subject – Subject text of the push notification.
- Push Notification - Message – Body text of the push notification.
- Send Email Notification – Set this setting to **On** to send an email to the user’s mailbox.
- Email Notification - Subject – Email message subject (e.g., New Mobile Device Enrolled in Intune).
- Email Notification - Body – Email message body (e.g., **A new device has been enrolled under your account in Microsoft Intune. Contact if you did not enroll this device.**).
- Email Header - Show company logo – Set this setting to **On** to embed the logo configured in Tenant administration > Customization in the email.

- Email Footer – Show device details – Set this setting to **On** to include details about the device that was enrolled in the email. This may delay the email notification.
- Email Footer – Show company name - Set this setting to **On** to include the company name configured in Tenant administration > Customization in the email.
- Email Footer – Show contact information – Set this setting to **On** to include the contact details configured in Tenant administration > Customization in the email.
- Email Footer – Show company portal website link – Set this setting to **On** to include a link to manage the newly enrolled device in the Intune Company Portal.

You can assign the enrollment notification to all users or assign it to a specific group of users that you want to receive the notifications. This is helpful if you need to create notifications in different languages, for example.

Custom Push Notifications

Intune can send push notifications with custom text to all the iOS and Android devices enrolled by a user. This can be useful for sending emergency alerts, such as for a weather event or a security situation. Custom notifications appear on the lock screen of the phone or tablet so you should be careful not to include sensitive information. You can send notifications to individual users or to groups of users. Microsoft restricts you to sending up to 25 messages per-hour to groups, and up-to 10 messages per-hour to a specific user's devices.

To send a custom push notification, browse to **Tenant administration > Custom notifications** in the admin center. Give your notification a title (up-to 50 characters in length) and a body (up-to 500 characters in length). The title and body appear on the lock screen of the device when the notification is received. On the Assignments tab, select individual users or groups of users to send the notification to. Note that if the group includes devices, those devices will only receive the notification if the device's owner is *also included* in the group. Once you complete the wizard, Intune will immediately send the custom notification to the targeted users. It is not possible to cancel the notification or track its status.

Security by Compliance

The configuration profiles and policies you deploy with Intune can be used as signals for access control decisions in Entra ID. This integration makes Intune even more powerful and an important part of your toolkit if you are implementing a zero-trust architecture. Whether you decide to use MAM, MDM, or both, you can make powerful decisions about whether a user and their device have access to applications or data using signals from Intune.

Compliance Policies

If you use MDM, you can define policies that declare devices as compliant or non-compliant. Device compliance is determined by measuring certain settings on the device as well as risk indicators from MTD solutions. Based on the results of this evaluation, Intune sets a flag on the device's object in Entra ID that indicates if the device is compliant (or not). Subsequently, Entra ID can use this compliance flag to influence access control.

Like configuration profiles, compliance policies are created on a per-platform basis. To create a compliance policy, browse to **Devices > Compliance > Policies** in the admin center and click **Create Policy** on the toolbar. Select a **Platform** and give your policy a name. In this example, we will create a compliance policy for iOS. You'll find the settings you can choose from are relatively limited in comparison to a configuration policy,

but the settings you can choose from are typically the most important indicators of a device's security posture:

- **Email > Unable to set up email on the device** – if you set this to require, the device must have an iOS Email configuration profile deployed to it that is successfully installed. If you are not using the native email app, this setting is not useful.
- **Device Health > Jailbroken devices** – this setting lets you mark jailbroken devices as non-compliant. We typically recommend that you select **Block**.
- **Device Health > Require the device to be at or under the Device Threat Level** – if you are using a mobile threat defense solution, this integrates the risk score from the MTD into the compliance indicator.
- **Device Properties > Operating System Version** – use these settings to require minimum (or maximum) versions of the device OS for the device to be considered compliant.
- **Microsoft Defender for Endpoint** – if you are deploying Defender for Endpoint to your mobile devices, this integrates the device's risk score from Defender for Endpoint into the compliance indicator.
- **System Security > Password** – use this setting to require the device to have a PIN or passcode. We generally recommend you set this to **Require**. You can subsequently configure more specific details of the PIN such as its length or how often it must be changed.
- **System Security > Device Security** – list apps here that you want to block from mobile devices. If a listed app is installed, the device will be considered non-compliant.

Several other compliance policy settings are available for Android devices that allow you to test device integrity and block devices with side-loaded apps more granularly.

When a device is considered non-compliant you can configure what Intune should do. By default, Intune will immediately mark the device as non-compliant which may have adverse consequences for the end-user's access to organizational apps and data. You can take a more measured approach on the **Actions for noncompliance screen**:

- **Mark device noncompliant** – after how many days should Intune mark the device as noncompliant in Entra ID?
- **Send email to end user** – after how many days should Intune send an email to the end user (and optionally to others such as your helpdesk) informing them about their device?
- **Send push notification to end user** – after how many days should Intune send a push notification to the end user informing them about their device?
- **Remotely lock the noncompliant device** – after how many days should Intune lock the device, requiring the device's PIN/passcode to be entered?
- **Add device to retire list** – after how many days of noncompliance should Intune add the device to a list for an administrator to retire the device.

You might decide to first send the user an email immediately, wait three days to mark the device as non-compliant in Intune, and then add the device to the retirement list if it is still non-compliant after 90 days. On the other hand, your security requirements might not allow a non-compliant device for any period so you might decide to both send an email and mark the device as non-compliant immediately (after 0 days).

After configuring the policy, you must assign it to groups of users or devices in the same way as you have assigned other profiles or apps. If you have a single compliance policy for all iOS or Android devices, you can also assign the policy to all users or all devices in lieu of creating groups to target the policy. It is important to remember that compliance policies only *test* settings. They never configure settings on a device.

Conditional Access

Conditional access policies are an Entra ID P1 feature that let you make decisions about the who, what, when, where, and how of access to apps and data. We discuss the conditional access feature of Entra ID in detail in the Identities chapter, including various examples of how to configure policies that integrate information from Intune. A classic example is organizations that want to make sure email is only accessed from devices that are either enrolled in Intune and policy compliant, or from end-users that are using a managed app like Outlook Mobile.

You can use two indicators from Intune to achieve these goals (and we show you how in the Identities chapter). Since the compliance status of a device is reflected in Entra ID based on the results of your compliance policies, you can require a device to be compliant in your conditional access policy. Likewise, conditional access policies can determine if a user is using a managed app (e.g., Outlook Mobile) that is governed by an app protection policy. If these factors are satisfied, the conditional access policy will permit access. Otherwise, conditional access can deny access.

If you use compliance policies with conditional access, ensure that all managed devices receive a compliance policy. Intune provides a helpful report, aptly named *Devices without compliance policy*, to assist. To access this report, browse to **Reports > Device compliance**, and then open the **Reports** tab.

Enterprise Single Sign-On for iOS Devices

When you use Conditional Access to restrict access to applications from mobile devices, you might discover that device compliance does not work correctly in some apps on iOS devices. You will also notice that apps that don't use the Microsoft Authentication Library (MSAL) do not have a single sign-on (SSO) experience like when you use Microsoft Office apps. To address these problems, you can configure the Enterprise SSO extension for iOS devices.

To activate the Enterprise SSO extension, browse to **Devices > iOS/iPadOS > Configuration Profiles** and click **Create > New Policy** on the toolbar. Choose the **Templates** Profile type and then select the **Device features** template. Configure the following **Single sign-on app extension** settings:

- **SSO app extension type** – Microsoft Entra ID
- **Enable shared device mode** – Not configured. You should only configure this if you are using this capability, described [here](#).
- **App bundle IDs** – You must enter a list of applications that will be granted access to the extension. Use a tool like [Bundle Id Finder](#) to lookup the bundle ID for the apps you are white listing.
- **Additional configuration** – Configure the following settings:

Key	Type	Value
<code>browser_sso_interaction_enabled</code>	Integer	1
<code>AppPrefixAllowList</code>	String	com.apple.
<code>disable_explicit_app_prompt</code>	Integer	1

Once you have configured the profile, you can deploy it like any other configuration profile. We strongly recommend that you begin by piloting the settings with a small audience and validate the behaviour of your applications that authenticate to Microsoft Entra.

Terms of Use

Some organizations require end users to accept terms and conditions before they can enroll a device in Intune. Common examples are acceptable use policies for organization-owned devices and agreements for

how personal mobile devices can be used to access organization data. There are two ways you can accomplish this with Intune:

1. Intune terms and conditions
2. Entra ID conditional access terms of use

We recommend using Entra ID's terms of use if you have Entra ID P1 licenses. Entra ID terms of use support a much broader set of features including uploading PDFs that can have formatting and hyperlinks, multiple languages, requiring users to scroll through the entire terms document, and more.

You must first create a terms of use document in Entra ID. To do this, login to the Entra admin center and navigate to **Protection > Conditional Access > Terms of use** and click **New terms** on the toolbar. Configure the terms with the following settings:

- **Name** – a name for the terms that is useful to administrators. This value is not shown to end users.
- **Terms of use document** – upload a PDF that will be shown to end users for acceptance. You can upload additional PDFs in alternate languages. You must specify the **default language** for the first PDF you upload and provide a **Display name** that will be displayed to end users.
- **Require users to expand the terms of use** – if you select **On**, users must view the contents of the PDF before they can accept the terms.
- **Require users to consent on every device** – if you select **On**, users will be prompted to accept these terms on every device rather than just once.
- **Expire consents** – if you select **On**, users will be forced to re-accept the terms after the number of days specified in the **Duration before re-acceptance required** field.
- **Enforce with conditional access policy templates** – choose **Create conditional access policy later**.

Next, you will need to create a conditional access policy to apply the terms you created to Intune device enrollment. We cover conditional access policies in depth in the Identities chapter. The policy that you create must be configured with the following minimum settings:

- **Cloud apps or actions** – choose **Select apps** and then select the **Microsoft Intune** and **Microsoft Intune Enrollment** apps.
- **Grant** – check the box next to the name of the terms of use you created previously.

Auditing information for when users accept terms of use is accessible from the **Identity > Monitoring & health > Audit logs** area of the Entra admin center. Click the **Activity** filter below the toolbar and select **Accept Terms of Use** to filter the audit data.

Intune Management

As you plan to use Intune in your organization, you will need to determine how to operationalize management of the service. In a small organization, this may be simple, but in larger organizations, you will probably need to grant access to different teams such as your service desk or endpoint management team to manage different parts of your Intune configuration. You may also need to give management insight into how the service is being used and what your mobile device and application footprint looks like. In this section we will explore some of these requirements and how you can accomplish them with Intune.

Privileged Access and Role Based Access Control

Members of the Global administrators and Intune administrator roles in Entra ID are automatically granted full access to Intune. While these roles grant broad access, you probably will want to delegate more granular

access to administrators in your IT organization. There are several [built-in roles](#) that you can start with by browsing to **Tenant administration > Roles > All roles** in the admin center.

If your organization is more complex, you can define custom roles to meet your specific needs. Custom roles define two components: the permissions they grant and the objects (e.g., devices, policies, apps, profiles, etc.) the permission applies to. There are hundreds of individual permissions that you can explore as you create a role. The objects that the role grants access to use a capability called scope tags. We have not discussed scope tags thus far, but you may have noticed that you can set them anytime you created a policy, profile, or app.

If you do not need to segment access to individual devices or policies/profiles/apps, you can use the built-in Default scope tag. If you do need to segment access, scope tags are for you. You might want to create individual scope tags for different departments, regions or geographies, or categories of users (e.g., executives). Scope tags are assigned to devices based on group membership. You can either put devices in a group manually, or you can use dynamic groups to automatically place devices in certain groups. All other objects in Intune (e.g., configuration policies, apps, etc.) are manually assigned one or more scope tags.

To create a scope tag, browse to **Tenant administration > Roles > Scope tags** in the admin center. Click **Create** on the toolbar and give your new scope tag a name and description. You can choose anything you want – for example “Headquarters Devices” or “Executives”. If the tag will apply only to certain devices, select a group that meets your needs.

Next, when you create a custom role by browsing to **Tenant administration > Roles > All roles** in the admin center and clicking **Create**, you can choose one or more scope tags in the wizard. The permissions you select will *only* be granted to items that are tagged with the scope tag(s) you select. To apply a scope tag to almost anything in Intune, go to the Properties of that item and click **Edit** in the **Scope tags** section of what you are editing.

Multiple Administrative Approval

You can use the multiple administrative approval (MAA) capability in Intune to require changes to apps and scripts (or MAA itself) to be approved by another administrator before they become effective. This is useful for change control, as well as scenarios where you are managing high-security devices with Intune. MAA is controlled with access policies. An access policy applies to all apps or all scripts in the tenant and defines a global set of approvers.

To create an access policy, browse to **Tenant Administration > Multi Admin Approval**, open the **Access policies** tab, and then click **Create**. Give your policy a name and select a profile type of Scripts or Apps. Finally, select one or more groups that will be able to approve requests. Once the policy is created, when you go to create, edit, or assign an app or script, you will be prompted to submit the request for approval with a business justification. The change will not take effect until an administrator approves it. Note that app or script cannot have more than one change pending approval.

Approvers can review and approve pending requests by browsing to **Tenant Administration > Multi Admin Approval > My requests**. Note that Intune does not send email alerts to approvers that their action is required. Administrators will need to alert approvers that their action is required.

Complex Assignments with Filters

One of the limitations of traditional assignments in Intune is the inability to combine inclusion and exclusion groups that mix users and devices. For example, you cannot include a group of users in a specific department

but then exclude a group of devices that are personally owned. Filters allow you to create reusable rules for when an assignment should (or should not) apply to certain devices.

Filters can be used with most types of assignments, but there are a [few exceptions](#). To create a filter, browse to **Tenant administration > Filters** in the admin center and then click **Create > Managed devices** on the toolbar. Give your filter a name and select the **Platform** that it will apply to. You can either manually specify the filter in the **Rule syntax** editor or use the expression builder. For example, if you wanted to create a filter that targets only devices that are personally owned, configure the following expression:

- **Property** – deviceOwnership
- **Operator** – Equals
- **Value** – Personal

Under the **Rule syntax** editor, there is a **Preview devices** link. Clicking this link allows you to test the results of the filter in real time before you deploy it.

After creating the filter, you can apply it to an assignment for an App, Configuration Profile, Enrollment Restriction, or Compliance Policy. You will configure the **Filter mode** to **Include** or **Exclude** in the assignment and select the filter you previously created.

Simplifying Assignments

Throughout the examples described here, we assign various policies, apps, and profiles to groups. As your Intune deployment grows in scale and complexity, this can become difficult to accurately manage. To address this, Intune has a feature called *Policy Sets*. You can use policy sets to create a single assignment for any combination of apps, app configuration policies, app protection policies, configuration policies, compliance policies, device type restrictions, and more. For example, you might create a policy set for all of your users in North America and assign everything they need at once.

To create a policy set, browse to **Devices > Policy sets > Policy sets** (or **Apps > Policy sets > Policy sets**) in the admin center and click **Create** on the toolbar. Give your policy set a name and then click through the **Application management** (apps, app configuration policies, and app protection policies) and **Device management** (configuration profiles and compliance policies) tabs. Add the relevant items that you want to deploy on each tab. Finally, on the assignments tab, add the groups of users or devices that you want to include (and, optionally, exclude) from the deployment. Note, again, that you cannot combine inclusions and exclusions of users and devices in the same assignment.

Once you create the policy, all the items you selected will be deployed according to the assignment. In the future, if you need to deploy a new item such as an app or profile to the same set of users or devices, you can simply add it to the policy set without recreating potentially complicated assignment logic in yet another location.

Maintaining a Clean Admin Center

Over time, your Intune console will probably become cluttered with old devices. People get new phones all the time, but they do not call you to ask for their old device to be removed from Intune. You might remember that you can configure a compliance policy to retire non-compliant devices from Intune which will remove them from the console next time they check-in. This does not solve all the clutter, though.

Fortunately, you can configure Intune to automatically delete devices that have not checked-in for some time. To do this, browse to **Devices > Device clean-up rules** in the admin center. Set **Delete devices based on last check-in date** to **Yes**, and then set **Delete devices that haven't checked in for this many days** to a

number of days ranging from 30 to 270 days. This configuration applies to every device in Intune (except Macs managed by Jamf), and it is not possible to choose different settings for different types of devices. You will need to choose a value that makes the most sense for your organization. For example, if you have a set of tablets that are only used for special events that happen quarterly, you might configure this feature to 120 days to allow time for those tablets to be used periodically.

Reporting

The **Reports** section of the admin center contains a [set of reports](#) that highlight specific aspects of your Intune deployment. One thing you may notice when you click on a report is that it does not show any data. You must manually refresh the Intune reports before you can see any data in them. From time to time, Microsoft makes changes to the reports available here, or the contents of existing reports. The list of reports in this section is short, but, in the individual areas of the admin center, you will find a **Monitor** section with more reports. For example, if you browse to **Devices > Monitor**, you will find twenty additional reports that you can generate.

While the built-in reports are useful, the most powerful way to take advantage of the data in Intune is to access Intune's data warehouse. The data warehouse is available as an OData feed that you can integrate into any tool you want. Microsoft supplies a [sample app](#) for Power BI, shown in Figure 15-3, that is a very useful getting started tool if you have access to Power BI.

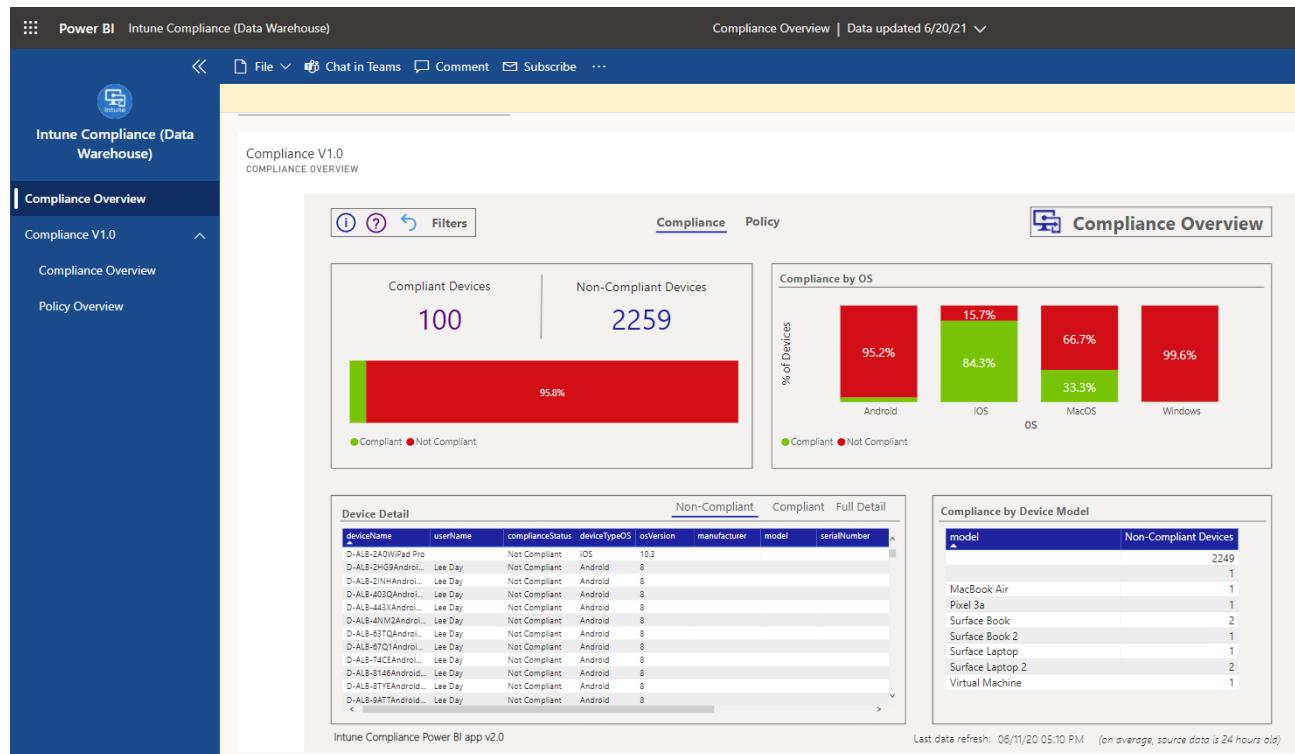


Figure 15-3 Power BI Intune data warehouse dashboard

Chapter 16: Managing Data Governance and Compliance

Tony Redmond

The Microsoft Purview suite covers a range of risk and compliance and data governance solutions available to Microsoft 365 tenants. For Information Technology, compliance is how organizations comply with established guidelines, regulations, and legislation. It can also refer to the practical measures taken by an organization to ensure compliance. Legislation varies from country to country. Well-known examples in the United States include the Sarbanes-Oxley Act (SOX 2002) and the Health Insurance Portability and Accountability Act (HIPAA – 1996). Companies working in these industries must ensure that their IT systems store and keep data in compliance with the regulations laid down in legislation. The [General Data Protection Regulation](#) (GDPR) and the California Consumer Privacy Act (CCPA) are good examples of how regulations exist to compel companies to protect personal data properly.

Microsoft began its journey to deliver compliance features in Exchange 2010. Since then, Microsoft has delivered an array of features. Although not every workload currently supports every aspect of compliance functionality, coverage is steadily spreading. The aim is to cover all workloads where users generate information that organizations might need to keep for business or regulatory purposes. Collectively, these categories give organizations a framework for “data governance.”

A data governance framework helps organizations satisfy regulations and applicable standards. Technology helps users to be compliant, but only if that technology is easy to use and unobtrusive. Experience proves that trying to implement difficult-to-use or complex compliance technology is not a recipe for success. Building compliance into applications like SharePoint Online or Teams intuitively and unobtrusively is challenging, especially as the volume, complexity, and sources of data requiring governance increase. Without good governance, organizations cannot meet compliance and regulatory requirements and expose themselves to the consequences of data leakage or external threat.

Data Governance

Originally, workloads implemented different compliance capabilities limited to the extent of the workload’s functionality. Because each took a different approach to compliance, bringing the on-premises functionality to the cloud resulted in a fragmented and disjointed situation. Some data have protection, and some do not. Some data are subject to retention policies, and some are ignorant of policies. Some data come within the scope of eDiscovery, and some are invisible to searches. And so on.

A complication is that some applications have been slow to support the compliance framework. Another arises through the introduction of new applications like Teams and Planner, which create new sets of data that might be of interest from a compliance perspective. In short, the old approach of depending on workload-specific compliance functionality was obsolete. A new cross-service architecture was necessary to handle compliance for cloud applications running inside Microsoft 365. Microsoft rolled out the new Data Governance framework in April 2017. Over the subsequent five years, Microsoft added more solutions to the framework and then renamed it as the Microsoft Purview suite in April 2022.

Depending on the business requirements that exist within an organization to preserve and protect its information, the individual compliance solutions in the Purview suite are less or more important. Fitting them

together into a coherent plan is a major task that needs input from Information Technology, Human Resources, and Legal personnel in addition to overall direction and support from senior management. As the regulatory and legal frameworks that govern compliance vary extensively from country to country and industry to industry, the treatment of the topic here is by necessity at a reasonably high level. However, it should be enough to give guidance as to what is and what is not possible.

Licensing Data Governance and Compliance Services

Many of the data governance and compliance services require premium or advanced licenses. This isn't a problem if you have the necessary licenses, but if you don't, you should remember that:

- Microsoft might enable a service for every account in the tenant. This can incur a potential licensing liability if you are not careful to restrict access to functionality to the accounts that need to use the service.
- Microsoft does not enforce licensing for many services. This might change in the future and if the accounts do not possess the correct licenses, they will lose access to a service once "targeted capabilities" are available.

Among the Purview solutions you might want to use are:

- Microsoft Purview Information Protection and Sensitivity Labels.
- Microsoft Purview eDiscovery (Premium).
- Microsoft Purview Customer Lockbox.
- Microsoft Purview Data Loss Prevention.
- Microsoft Purview Data Lifecycle Management.
- Microsoft Purview Information Barriers.
- Microsoft Purview Insider Risk Management.
- Microsoft Purview Communication Compliance.
- Microsoft Purview Records Management.
- Microsoft Purview Audit (Premium).

Other Microsoft Entra and Microsoft 365 components assist with data governance, including:

- Privileged Access Management.
- Entra ID Conditional Access Policies.
- Microsoft Defender for Cloud Apps.
- Microsoft Purview Message Encryption.
- Microsoft Purview Advanced Message Encryption.
- Microsoft Priva.

These lists are not complete and will change over time as Microsoft introduces new services and capabilities.

Some inconsistencies in Microsoft licensing deserve mention. For example, Data Loss Prevention policies for Exchange Online, SharePoint Online, and OneDrive for Business require Office 365 E3 while DLP and retention policies for Teams need Office 365 E5. Finally, make sure you know the rules for which accounts need additional licenses. For instance, anyone who is a custodian in a premium eDiscovery case because they "control" documents or messages needed by the case must have an Office 365 E5 or Microsoft 365 E5 Compliance license.

Before deciding to invest in any compliance functionality, you should consult [Microsoft's licensing guidance for security and compliance](#) to understand the features you want to use and the licenses required by the features. You can also use the [downloadable feature chart](#) to check features against license requirements.

This chapter covers three Purview solutions: Data lifecycle management (retention labels and policies), communication compliance, and information barriers. Other relevant chapters are:

- Managing eDiscovery.
- Managing Data Loss Prevention.
- Managing Information Protection.
- Managing Auditing and Reporting.

Compliance Manager

Microsoft Purview [Compliance Manager](#) is a tool to guide compliance managers through the often-confusing array of rules involved in privacy frameworks. Compliance Manager is a static tool in that it does not have the necessary features to organize the work needed to achieve compliance with complex regulations like GDPR. However, many tools are available to help tenants to organize and manage the work set down in Compliance Manager. For example, Planner tasks can track progress to completion for responsibilities assigned to those working on ensuring compliance with regulations. To gain some collaboration capabilities, including document management, the tasks in plans are accessible on SharePoint Online sites, Teams, and Groups.

Keeping Content in Place

Traditionally, when a company needed to preserve email or documents for compliance purposes, they move copies of the items to a separate archiving system. Veritas Enterprise Vault is a classic example of such an archival system. When necessary, administrators run eDiscovery or retrieval activities to find content held in the archival system. This approach was acceptable when products like Exchange and SharePoint did not have archiving capabilities. Today, the focus is on leaving data in place within its native repository and integrating compliance technology inside applications. Advantages of this approach include:

- No need exists to transfer copies of messages, documents, and other content to external systems for searching, analysis, or otherwise interrogation for legal reasons.
- Avoidance of additional costs for software and hardware by not having to use external systems. In addition, the IT infrastructure is simplified because the extra systems are unnecessary.
- It is easier to prove the "chain of custody" and show that no one can tamper with emails and documents before these items become evidence in legal cases.
- Keeping content in its native repository means that no opportunity exists to compromise content during transfer to a new repository.

Removing the need for copying files from one system to another makes it easier to meet chain of custody requirements and prove that no one could have interfered with an item to compromise its contents.

Guaranteeing the chain of custody is important when data proves facts during litigation. In-place archiving means that information stays in its original location and is protected against interference for as long as the hold persists. The data retained in place is immutable as neither administrators nor users can interfere with it after a hold is in place.

Keeping everything in place inevitably means that repositories become larger. The software therefore must be more intelligent and more capable to deal with higher volumes of data. Searches must be able to find information quickly and accurately when needed for compliance purposes. The work done by Microsoft Research to improve and make search technology smarter together with the acquisitions of FAST (otherwise known as the Search Foundation) and Equivio are examples of how Microsoft responded to the need to have better search technology. Today, Microsoft Search indexes information as soon as documents, files, messages, chats, and other items are added to repositories via user activity or bulk imports while Equivio has evolved to become Microsoft 365 Advanced eDiscovery and is capable of processing millions of messages or documents to find the desired results very quickly. Another advantage is that when you have a unified view of data such as the Microsoft 365 substrate, it is much easier to build the necessary infrastructure around that data to secure and audit its use. For instance, the audit log captures details of user activity from multiple workloads

which administrators can then search using the audit log search in the Microsoft Purview Compliance portal, Cloud App Security, or third-party solutions.

Principles of Data Governance

Microsoft 365 takes a cross-service approach to data governance based on common policies that apply across multiple workloads. This approach is obvious in the way that content searches, eDiscovery, and Data Loss Prevention work, and is rolling out for data governance in the form of retention labels, retention policies, and associated features. The Microsoft Defender and Microsoft Purview Compliance portals are important parts of that strategy because they bring together functionality designed to work across applications rather than just a single workload.

Data Governance is a policy-driven framework to control the retention and removal of content across all applications. We can break the framework down into four parts:

- **Import:** Bring information from multiple sources, including from non-Microsoft sources like Facebook and Bloomberg messaging, into Exchange Online through the Import Service or third-party products. The aim is to allow customers to gather all the information they need to manage in repositories such as archive mailboxes or SharePoint sites to replace older methods like PSTs and file servers. Once the service holds the data, it becomes possible to manage the data through the application of policies.
- **Retain:** Provide customers with the ability to state what data they need to retain for compliance purposes, for whatever period is necessary. The policies used to enforce retention must apply across all workloads (or as many as possible).
- **Delete:** It is equally important for customers to be able to remove data that they no longer need. Methods need to exist to remove information from all repositories according to policy.
- **Classify:** Some data is more important or secret than others. The framework must allow users to classify information as they work. Applications should highlight information classified by users to raise awareness of the importance of the information. The system should recognize the sensitivity of the information and potentially restrict what users can do with that content.

Of course, when a company retains data for data governance, the data should be immutable. The Office 365 Import Service is the cornerstone for “Import.” Retention policies and retention labels make sure that tenants can keep or remove information as they need and classify items to mark important data for retention. Other functionality, like Data Loss Prevention, handle the need to protect against the misuse or inadvertent disclosure of data, while sensitivity labels (applied manually or automatically) restrict access to confidential information to authorized users.

The Influence of Privacy Laws

Companies with business operations inside the European Union must follow the [General Data Protection Regulation](#) (GDPR) to safeguard how they process personal data while companies operating in California must follow the California consumer privacy act (CCPA). In both cases, heavy penalties for breaches ensure that companies must take this and similar legislation seriously. According to Microsoft, over 90% of an organization’s data stored in Exchange Online, SharePoint Online, and OneDrive for Business is in Word, Excel, PowerPoint, OneNote, and Outlook (Exchange). It is easy to imagine examples of where applications hold personal information, including:

- Annual employee reviews stored in a SharePoint or OneDrive for Business site.
- A list of applicants for a position in an Excel worksheet attached to an email message.
- Lists holding data (names, employee numbers, hire dates, social security numbers, salaries) about employees in files in SharePoint Online sites.
- Discussions about potential new hires in a Teams chat.

- Word documents holding applications for employee work visas.

Given that personal information can be found in almost any application, the work to locate the 10% of personal information stored outside Office documents is likely to take the most effort (for example, see this [guide](#)). Organizations must know what applications hold personal data and how they process personal data in compliance with legislation. Knowing where to look is only the start of the process and it might not be possible to automate many of the steps involved in responding to data subject requests.

Fortunately, the compliance features available in Microsoft 365 assist tenants to satisfy legislative requirements. These features include:

- Sensitivity labels and policies to mark and potentially protect (encrypt) documents, messages, and other objects, like Power BI reports.
- Auto-label policies to find and classify documents holding personal data. Microsoft 365 includes sensitive information definitions for many country-specific personal identity cards and passports. You can create an auto-label policy to find and label documents holding these sensitive information types. Retention processing can remove items stamped with a suitable label after a defined period, perhaps after including a manual disposition review.
- Data Loss Prevention (DLP) policies can use the same sensitive information types to stop people from sharing confidential data outside the tenant. A General Data Protection Regulation DLP template makes it easy to deploy protection for all the defined European Union sensitive information types.
- Content searches to find personal data stamped with retention labels used to mark items holding personal data.
- Alert (or advanced alert) policies to detect actions that might be privacy violations. For example, multiple downloads of documents from a SharePoint site holding HR information. You can also search the audit log to discover and report potential issues.
- The Microsoft Priva Subject Rights Request solution makes it easy to retrieve information stored in Microsoft 365 when necessary to satisfy a request to provide information held about an individual.

Microsoft publishes information about how various aspects of Microsoft 365 align with GDPR (as an example, see this post covering [SharePoint Online and OneDrive for Business](#)). Having technology available to help satisfy the regulatory requirements is helpful. However, it is only one step to achieving full compliance. Tenants still need to protect data through a mixture of user education and technology. See [this paper](#) for information comparing the terms used in GDPR with those used in U.S. eDiscovery contexts.

User Privacy and Microsoft 365 Data Processing

Many Microsoft 365 features depend on access to user data. For example:

- Mail flow transport rules examine the content of inbound and outbound messages to apply rules, including data loss prevention rules. The transport service can examine messages and attachments protected with sensitivity labels.
- Viva Insights processes email and calendar events in user mailboxes to generate its insights and recommendations.
- Machine learning running on specialized AI computers in the Microsoft cloud processes messages to create suggested replies for Outlook. The same kind of processing creates learning models to understand how people write so that editors can predict text in messages and documents.
- Communications compliance policies examine the content of emails and Teams messages to ensure that users don't violate norms like harassment and use of obscenities.
- Auto-label policies used to apply retention and sensitivity labels to messages and documents at rest can use sensitive information types or trainable classifiers to match target items. By definition, this implies that the background processes which apply the policies must scan documents and emails to find matches and apply labels.

- When it constructs responses to user prompts, Microsoft 365 Copilot can use any document or email item that the signed-in user has access to. This includes protected documents where the sensitivity label governing access for the user grants the *Extract* right.

In all cases, the data remains in user mailboxes or SharePoint Online sites and under the control of the organization. Where Microsoft performs processing in a specific manner (like building models needed to generate suggested replies), they do so on a tenant-specific basis by copying data to process it and removing it afterward using [a process designed to preserve user privacy](#). The results of the processing are stored in user mailboxes.

Using these features is not mandatory and many of them do not exist in on-premises deployments due to the computer resources necessary to process data. In effect, you could regard features like the list above as examples of the advantages gained by using cloud services. However, organizations should ensure that they are happy for user data to be processed by Microsoft to extract the information needed for these and other features and decide if they wish to restrict some processing, such as disabling the [connected experiences](#) via any Office client.

Compliance Permissions

Microsoft 365 Purview compliance functionality uses role-based access control to allow or deny access to individual features. When users access the compliance portal, Purview evaluates the permissions held by their account to decide what they can do. Microsoft Purview uses a separate set of permissions to control access to compliance functionality than those used for general administrative purposes or in Exchange Online.

Compliance permissions are grouped into roles to reflect the access needed to perform specific tasks, like Data Investigator or Compliance Data Administrator. Roles also make it easier to assign relevant permissions to users.

Compliance roles are managed through the **Permissions** section of the Microsoft Purview Compliance portal, where users holding the Organization Management role can manage the set of permissions assigned to a role or who holds a role. Some compliance roles can also be assigned by editing user accounts in the Microsoft 365 admin center. After you assign the necessary role to a user, they must sign out and back into Microsoft 365 to ensure that the new permissions are respected. Sometimes it takes a little while before the new role assignments are acknowledged. If this happens, just wait for a few minutes, and then retry.

Administrative Units

The default state of the policies generated and used by Purview solutions is that they apply organization-wide. In other words, if an administrator creates a retention policy, that policy applies to any object that comes within its scope. This scheme works well for most tenants, but in some situations, enterprises need more granular control over the management of policies. Entra ID administrative units allow granular control over:

- Retention Policies and Label Publishing Policies.
- Data Loss Prevention Policies.
- Sensitivity Label Policies.
- Communication Compliance Policies.
- Insider Risk.

Granular control works by associating members of compliance role groups with administrative units. For instance, some members of the compliance administrator role group might be allowed to work with any policy while others are limited to policies applying to members of one or more administrative units. For example, an administrator might be assigned control over administrative units containing user accounts for employees working in France and Germany. The policies managed by that administrator only apply to the

accounts in those units. Behind the scenes, the background jobs that apply policies make sure that scoping is respected and that the jobs only execute the instructions in a policy (for instance, a retention policy to remove all mailbox items after five years) against locations that match the specified administrative units. In this case, the locations are the mailboxes owned by user accounts in the France and Germany administrative units.

Using administrative units to scope Purview policies requires administrator accounts to have Microsoft 365 E5 or Microsoft 365 compliance licenses.

Optical Character Recognition

Many Microsoft Purview solutions including auto-labeling of content, communications compliance, and data loss prevention support optical character recognition (OCR) in addition to normal text recognition. OCR support is an optional pay-as-you-go Microsoft Syntex feature funded through an Azure subscription at the rate of \$1 per thousand scanned items. Supported image formats include JPEG, BMP, PNG, and PDF of up to 20 MB (Exchange Online) or 50 MB (SharePoint Online and OneDrive for Business). See [the documentation](#) for more information.

Retention Policies and Publishing Label Policies

The retention strategy for an organization usually contains a mixture of removal and retention. Organizations want to remove items after their useful lifetime or to stop the ongoing accumulation of data that has no value. On the other hand, keeping high-value content is important because these items form the collective recorded memory of the company. Documents and emails relating to policies and procedures, strategy discussions, board minutes, reports, research papers, and so on must remain available for as long as the organization needs them. Sometimes laws or regulations define the retention period, and sometimes the organization sets the period. Within Microsoft 365, retention processing operates by applying retention labels to items and retention policies to locations (mailboxes, sites, or groups). The settings in retention policies and retention labels can do the following:

- **Retain-only:** Microsoft 365 retains items in their home locations for a specified period (or forever), called the retention period. When the retention period expires, users decide how to dispose of items. The retention period can be forever.
- **Delete-only:** Microsoft 365 permanently deletes items after their age reaches a specific period (set by the creation or last modified date). Because retention is not enforced, users can delete the items beforehand.
- **Retain and Delete:** Microsoft 365 keeps items for a specified period and then deletes the items permanently after the retention period expires.

Other settings exist to enable more granular processing, but the basics of retention boil down to defining a retention period and action.

A retention label is more precise because it applies to a single item instead of to every item found in a location. For instance, a user who works on a new corporate policy will know what retention label is most appropriate for that kind of content. Retention policies apply to all the items in containers coming within the scope of the policy, such as all the documents stored on a site. A retention label always takes precedence over a policy because of its specificity. Two types of retention policies exist to satisfy the specific requirements of a tenant. A tenant can deploy both types of policies.

- **Publishing Label policies** make retention labels available to users by publishing the labels to workloads. Settings within the retention labels control what happens to content marked with the labels. Multiple publishing policies can make labels available to a user. Workloads are responsible for combining all the labels available to a user and presenting the complete set through client interfaces.

- Assigning individual retention labels to items is more precise than container-based assignment through **Retention policies** because users select and apply the labels to specific items. Retention policies allow organizations to achieve broader coverage by applying retention settings to all items stored in selected containers or locations (such as mailboxes, sites, or groups). Background processes such as the Exchange Managed Folder Assistant (MFA) process the retention settings defined in policies against the items stored in the target locations. Tenants can use retention policies to preserve or remove content for the entire organization or specific groups of up to 1,000 accounts. Typically, tenants use retention policies to ensure that a company meets the compliance requirements set out in legislation such as the Sarbanes-Oxley Act. Management of retention labels and policies is in the **Data lifecycle management** section of the Microsoft Purview Compliance portal.

It can be confusing to understand the scenarios where it's best to use retention policies and where retention labels are a better choice. Usually, tenants end up using a mixture of both to ensure broad coverage through policies and precise retention of specific items through labels. For instance, you might apply a retention policy to a mailbox or SharePoint site that mandates the removal of items after six months and then provide some retention labels for users to assign to items they wish to keep for longer periods.

Table 16-1 lists several features that you should consider when planning how and when to use retention policies and retention labels.

Feature	Retention Policy	Retention Label
<i>Workloads:</i>		
<i>Exchange Online</i>	Yes	Yes (except for items in public folders)
<i>SharePoint Online</i>	Yes	Yes
<i>OneDrive for Business</i>	Yes	Yes
<i>Viva Engage</i>	Yes	No
<i>Planner</i>	No	No
<i>Teams</i>	Yes (chats and channel messages)	No
<i>Microsoft 365 Groups</i>	Yes (group mailbox and SharePoint sites)	Yes (items in group mailbox and individual SharePoint files)
<i>Automatic application</i>	Yes	Yes (by auto-label policy, DLP, etc.)
<i>Manual application by a user</i>	No (policies can only be set and applied by administrators)	Depends on the client's UI
<i>Labels displayed in client UI</i>	Partially (by Outlook clients for email)	Depends on the client's UI
<i>Persistence</i>	Policies are location-dependent, so items move out of scope if moved out of location	Persistent within supported Microsoft 365 locations. For instance, if you move a message from one folder to another, it keeps its assigned label
<i>Mark item as a record</i>	No	Yes
<i>Event-based retention</i>	No	Yes
<i>Require manual disposition review</i>	No	Yes

<i>Microsoft 365 audit</i>	Audit records not generated for application of policies to locations	Audit records are generated when labels are applied, changed, or removed to/from items
<i>Find items subject to retention</i>	No	Via content searches (select retention label as a search condition), content explorer, and activity explorer

Table 16-1: Comparing retention policies and retention labels

In the following sections, we explore the details of how to create and manage retention labels, the policies used to publish retention labels and to auto-apply, and general retention policies. We will also examine how Exchange Online mailbox retention policies work because of the ongoing need to support hybrid environments.

Rules or Principles of Retention

The many workloads and types of data in use across Microsoft 365 create a complex environment for retention management. Multiple ways exist to mark content for retention or deletion. Therefore, a need exists for a mechanism to resolve the conflict that can occur when several policies apply to a mailbox or site, especially when Microsoft 365 retention policies remove items after retention periods expire. Microsoft applies the following four rules of retention (sometimes called the *principles of retention*) to decide how to process content. The rules work from top to bottom. Workloads use the rules as tie-breakers to set precedence when processing items if multiple policies apply.

- Retention wins over deletion:** You could call this the “keep safe” principle. In practical terms, it means that when multiple retention policies apply to content, retention wins over deletion. Take the example of where a mailbox comes under the scope of two retention policies. The first removes all messages after they are four years old. The second, perhaps applied to a subset of mailboxes belonging to senior managers, retains all messages for seven years. The solution is to move messages into the Recoverable Items structure after four years and to keep them there for three more years. Both policies are respected because items seem to be deleted after four years (users do not realize that the messages are still available) while keeping the items in the background ensures that the messages stay indexed and discoverable for the full seven years.
- Longest retention period wins:** If multiple policies specify different retention periods, items are always kept for the longest period. This principle ensures that content is kept for as long as it might be needed. If you want to deliberately remove content after a certain period, deploy a policy that explicitly removes the content after that period elapses and make sure that the location holding the content does not come within the scope of any other policy (like a default tag in an Exchange mailbox retention policy or retention policy). Note that Microsoft 365 will keep an item for longer if a user applies a label with a longer retention period to the item.
- Explicit wins over implicit:** Explicit means that a user or administrator has selected specific content for special retention. This can happen when a user applies a label with a retention action to an item in a mailbox or site, or when a location is within the scope of a “non-org wide” policy (one that only applies to some content within the tenant). The logic here is that the user or administrator has made an explicit decision about retention for a specific item (a label applied manually) or location (non-org wide policy created by the administrator). Manual application of a retention label always takes precedence over a catch-all retention policy that applies to locations, including when an auto-label policy applies retention labels automatically. This principle has long existed in Exchange retention

policies where a personal retention tag applied manually by a user always has precedence over a tag applied to a folder or a default tag applied to a mailbox.

4. **Shortest deletion wins:** Retention policies allow administrators to actively remove content after a certain period (still called the retention period). If multiple deletion policies apply with different retention periods, Microsoft 365 applies the shortest retention period and removes the content when that period expires. The logic here is that an administrator decided to remove content after a certain period. The presumption is that good reason guided this decision. It would therefore not make sense if another policy, perhaps created by another administrator, interfered with the decision to remove content after that period. Again, this is a reason to consider how the retention policies in a tenant interact with content.

Remember that holds always take precedence over deletion. If an eDiscovery case places a hold on content for a set period, Microsoft 365 cannot remove items within the scope of the hold until the hold period expires or an administrator releases the hold, even if the retention periods of policies applied to the content expire.

It often takes time and some experience in working with retention policies across different workloads to understand the effect of the retention principles and how to best deploy these principles to support the data governance strategy for the organization. Microsoft [publishes a helpful flowchart](#) to explain how retention decides to keep or remove items. It's much easier to follow and understand the steps in the flowchart after gaining some experience working with retention policies and labels.

Retention Policies

Retention policies apply retention rules to target containers (locations). The supported containers include:

- Exchange (mailboxes and cloud-based public folders). From a retention perspective, a user's primary and archive mailbox are considered a single unit.
- SharePoint Online (including files created in Viva Engage, Teams, and Groups).
- OneDrive for Business.
- Teams compliance records for chats and regular and shared channel conversations. Compliance records for chats are in personal mailboxes, while regular and shared channel compliance records for conversations in group mailboxes. Because shared channels aren't associated with a group mailbox, Microsoft 365 creates a special version called a *SubstrateGroup* mailbox to hold their compliance records.
- Teams private channel conversations.
- Conversations in Viva Engage communities and private messages between users.
- Microsoft 365 Groups (Outlook conversations in the group mailbox).

Retention labels contain settings to tell Microsoft 365 how the organization wishes to retain or remove items in a location. The basic settings are a retention action or rule, defining what should happen when a retention period expires, and a retention period, which defines when the action should occur.

The Managed Folder Assistant processes retention policies for Exchange locations:

- User and shared mailboxes (primary and archive, if enabled).
- Public folders (you can't select specific sections of the public folder hierarchy for processing).
- Microsoft 365 group mailboxes.

A separate Microsoft 365 retention assistant processes all the other workloads, including the compliance records stored in Exchange Online.

Broad and Narrow Retention

Retention policies can be broad or narrow in scope. A broad retention policy applies the same retention settings to a set of containers. Each workload has its locations: Exchange has mailboxes (user, shared, and group), SharePoint has sites, OneDrive for Business has accounts, and Teams has chats and conversations. The broadest retention policy is one that applies the same retention settings to all the locations managed by all workloads in a tenant. As described below, this is an example of an org-wide policy.

Narrow retention policies make retention labels available to workloads. Each retention label has its retention settings and a retention policy for labels can have just one label or include many labels. Publication means the process of making workloads like Exchange and SharePoint aware of the existence of the labels in a retention policy. Following publication, the workloads expose the retention labels in client interfaces so that users can then apply the labels to the selected content. The application of a retention label to a message or document is a much more precise way to keep information. As such, retention labels trump the settings applied by broad retention policies. For instance, the organization uses a broad retention policy to assign a five-year retention period to all SharePoint sites. All documents stored in a document library inherit the policy and SharePoint will keep documents until they are five years old. If a user then assigns a retention label with a ten-year retention period to a set of documents, SharePoint will keep those documents for that period.

Org-Wide and Scoped Retention Policies

Two types of retention policies exist:

- **Org wide:** The purpose of an org-wide policy is to apply a single retention policy to all supported workloads. The scope of an org-wide policy is the tenant, but the scope can be amended to exclude or include specific workloads. Currently, org-wide policies can apply to Exchange mailboxes, Exchange public folders, Groups, Viva Engage private and community messages, and documents stored in SharePoint Online sites and OneDrive for Business accounts. Separate policies handle the retention of Teams chats and channel messages and messages posted to Viva Engage communities. Policies to process Teams chat messages include the compliance records captured for Microsoft 365 Copilot interactions, such as the prompts and conversation between users and Copilot. There can be up to 10 org-wide policies in a tenant. You should use org-wide policies sparingly as it is easy to create a policy that has unintended consequences. For instance, if you create a policy to keep all content for two years and then remove the content afterward, the policy will remove everything from the tenant that is more than two years old and does not come under the control of another policy. That could lead to the removal of most content across workloads, which might not be what you want to do. Org-wide policies are “entire location” policies because they cover all the locations within the selected workloads (for example, all Exchange Online mailboxes).
- **Non-org wide:** These policies apply retention to a subset of the locations available within a tenant. The scope of these policies is set by picking specific mailboxes, sites, or groups to include in the policy or by applying a query based on keywords or sensitive information types to find the content to which the policy applies. Each workload has its restrictions for the number of locations in a non-org-wide policy. For example:
 - Exchange Online and Teams: 1,000 mailboxes (accounts).
 - Microsoft 365 Groups: 1,000 groups.
 - SharePoint Online sites and OneDrive for Business accounts: 100 of each.
 - Teams chat or channel messages: 1,000 accounts.
 - Viva Engage community or private messages: 1,000 accounts.

[This article](#) details the current limits for Microsoft 365 retention policies. If you need a policy to process more than the limit of static locations, you must split processing across multiple retention policies. This is manageable, but it can be a pain. In this situation, adaptive scopes might be a better answer.

The number of org-wide and non-org-wide policies available for deployment means that organizations can get very creative with their retention strategy. In general, it is best to simplify retention processing by limiting the number of active policies as this will help to avoid situations where the actions and retention periods of policies clash. See the *Rules of Retention* section to understand what happens when several policies apply to an item.

Getting Round Policy Limits: The limits for the target locations processed by retention label policies divide into SharePoint locations (sites and accounts) and Exchange locations (mailboxes and groups). SharePoint locations have a 100 limit while Exchange can deal with 1,000 locations. In either case, these limits are often too small for large tenants. To get around the limits, you can create multiple policies that have the same settings but different target locations. For example, if you need to apply retention settings to 500 SharePoint sites, create five examples of the same policy and include a different set of 100 target sites in each policy. With the necessary licenses, adaptive scopes (see below) allow organizations to solve the problem by creating scopes to find target locations and using the scopes in retention policies. Adaptive scopes don't have the same numeric limitations as static policies do.

Adaptive Scopes

Adaptive scopes are a way to find target locations by applying a filter (query) against the set of available locations in a tenant. In some respects, adaptive scopes work like dynamic groups or dynamic distribution lists, both of which use a query to find a set of objects. Before adaptive scopes can be used with a Purview solution, they must be created and managed through the Roles & Scopes section of the Microsoft Purview Compliance portal. Any administrative role that includes the scope manager role can manage an adaptive scope. Adaptive scopes can be used to set the scope for retention policies and communication compliance policies. They can work with Entra ID administrative units so that only objects from selected administrative units are found by an adaptive scope.

Three kinds of adaptive scope are available:

- **Users:** Filter applied against selected account properties like job title, city, state or province, department, and the Exchange custom properties. For example, an adaptive scope can find all the users located in France whose job title starts with "Manager." Mailbox states and types are also usable in filters, meaning that you can create scopes to look for inactive mailboxes (a state) or shared mailboxes (a type). Figure 16-1 shows the query builder in use to build the scope for an adaptive scope for users. You can also see the set of properties available to build the query. Adaptive scopes of this type apply retention to mailboxes and OneDrive for Business accounts.
- **SharePoint Sites:** Filter against the site URL, name, or the 100 refinable string properties (refinablestring00 to 99) available to customize the SharePoint Online search schema. For example, find all sites where the value of a custom property (represented by the RefinableString99 refiner) is "Secret." To update custom properties for a site, its administrator must write values into the site property bag. [This article](#) explains how to update the site property bag using PowerShell. Another example is to use an adaptive scope with a query to find sites with URLs starting with a certain value to find all OneDrive for Business accounts in a tenant. Adaptive scopes don't currently support the SharePoint Online sites created for Teams shared channels.
- **Microsoft 365 groups:** Filter against group properties like name, description, and Exchange custom properties.

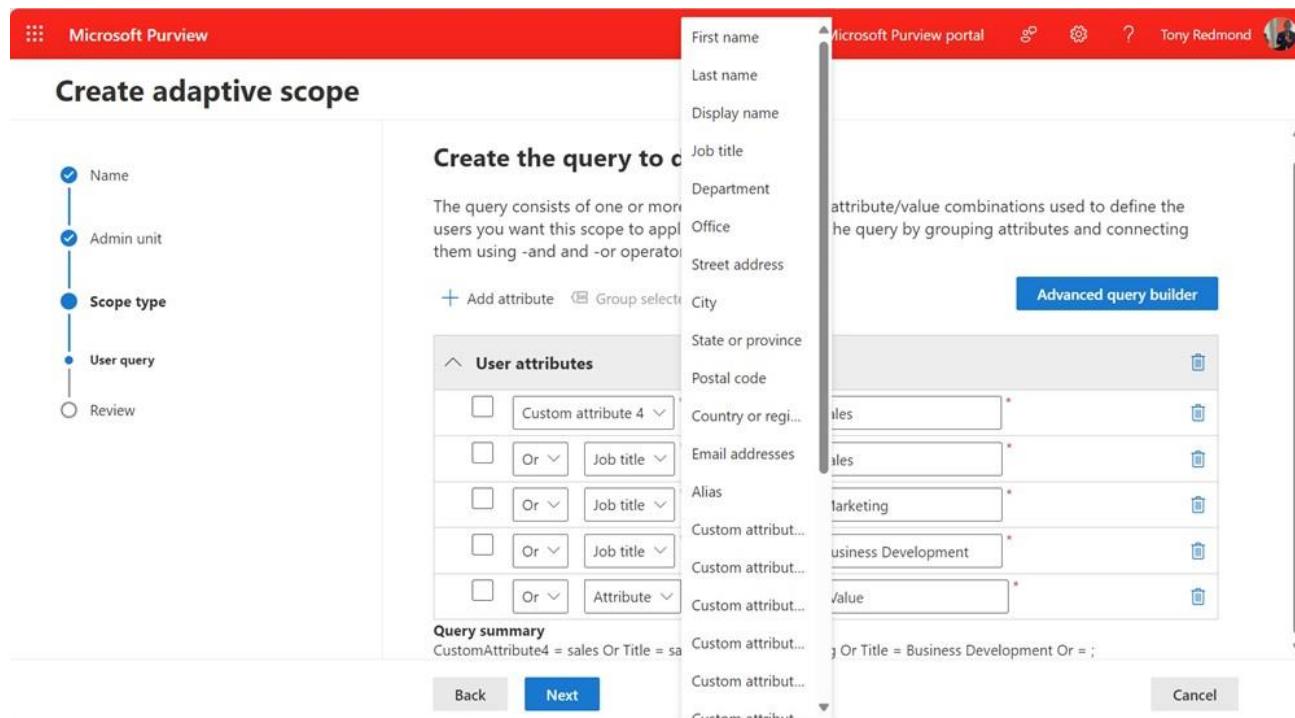


Figure 16-1: Defining an adaptive scope

The operators available to build an adaptive scope query are:

- is equal to.
- is not equal to.
- starts with.
- not starts with.

You can combine *And* or *Or* checks against properties. For instance, the query shown in Figure 16-1 contains several *Or* tests for different values in the Job title property. If the query builder can't construct the query you need, you might be able to build an advanced query in OPATH syntax (users and groups) or KeyQL (sites). For instance, an adaptive scope to find inactive mailboxes uses the OPATH query:

```
IsInactiveMailbox -eq 'True'
```

While the query to find shared mailboxes is:

```
RecipientTypeDetails -eq 'SharedMailbox'
```

The same construct supports finding user mailboxes, group mailboxes, room mailboxes, and so on and you can combine checks to find multiple mailbox types. However, although advanced queries can build user adaptive scopes using mailbox types and states and employ access to more operators (such as *like* or *notlike*) than available in the query builder, advanced queries can only use the same set of user account properties presented by the query builder. The query builder includes basic checking of the query to make sure that it will work. The check occurs when saving the adaptive scope. Microsoft has also released [a script designed to validate queries](#).

Not every mailbox property or user account property is available for use with adaptive scopes. If you find that you want to use an unsupported property as the basis for an adaptive scope, consider populating one of the custom properties with values from the property that you want to use and creating the adaptive scope based on the custom property. An [example of this approach is described in this article](#) where the adaptive scope is based on the domain name part of the mailbox primary SMTP address.

The results of adaptive scope queries are not available immediately. Instead, a background process that runs daily uses the queries in adaptive scopes to identify the set of target locations identified by the scope query. You can view the current set of locations by accessing the scope details (Figure 16-2). If you see *No data available*, it means that either the background process has not yet resolved the query, or the query doesn't find any objects.

The screenshot shows the 'Information governance' section with a 'Scope' tab selected. Under 'Individual contributor mailboxes', it displays 6 items. The table shows the following data:

Display name	Location type	State
Marc.Vigneau@office365itpros.com	User	Added
Chris.Bishop@office365itpros.com	User	Added
Oisin.Johnston@office365itpros.com	User	Added
Eoin.Redmond@office365itpros.com	User	Added
Ben.James@Office365itpros.com	User	Added
Brian.Weakliam@office365itpros.com	User	Added

The 'Details' pane on the right shows:

- Name:** Individual contributor mailboxes
- Description:** An adaptive scope to find the mailboxes belonging to individual contributors
- Type:** User
- Query summary:** CustomAttribute4 = IC Or Title = Consultant Or Title = Senior Consultant Or Title = Architect
- Last modified by:** Tony Redmond
- Last modified:** Nov 1, 2021 2:50 PM

Figure 16-2: Viewing the set of locations calculated using an adaptive scope query

A retention policy can use one or more adaptive scopes to find the locations to which it applies. Figure 16-3 shows that a retention policy uses two user adaptive scopes. Because these are user adaptive scopes, the set of workloads that the retention policy can cover doesn't include SharePoint Online. However, it does include OneDrive for Business because these accounts are personal and linked to individual users. When a workload processes a retention policy with adaptive scopes, it resolves the queries from all scopes to find the up-to-date set of locations and applies the settings in the retention policy to those locations.

Retention policies with adaptive scopes require an Office 365 E5 or Microsoft 365 E5 compliance license for every account coming within their scope. Office 365 E3 tenants can only use retention policies with static scopes, which process either all locations of a specific type (like all mailboxes or all sites) or a custom set of locations. To change the set of locations, an administrator must amend the policy manually or using PowerShell (an example of how to use PowerShell to manage the locations for a retention policy is [described in this article](#)).

Adaptive scopes work best when an organization wishes to apply retention policies based on some criteria, such as the people who work in a certain country or department, or SharePoint sites containing a certain kind of information. Because adaptive scopes depend on settings such as user account properties or custom site properties, it's easy to add new locations to policies by updating the account, mailbox, or site settings. Workloads then pick up new locations or remove locations no longer within the scope the next time they process locations to enforce retention policies.

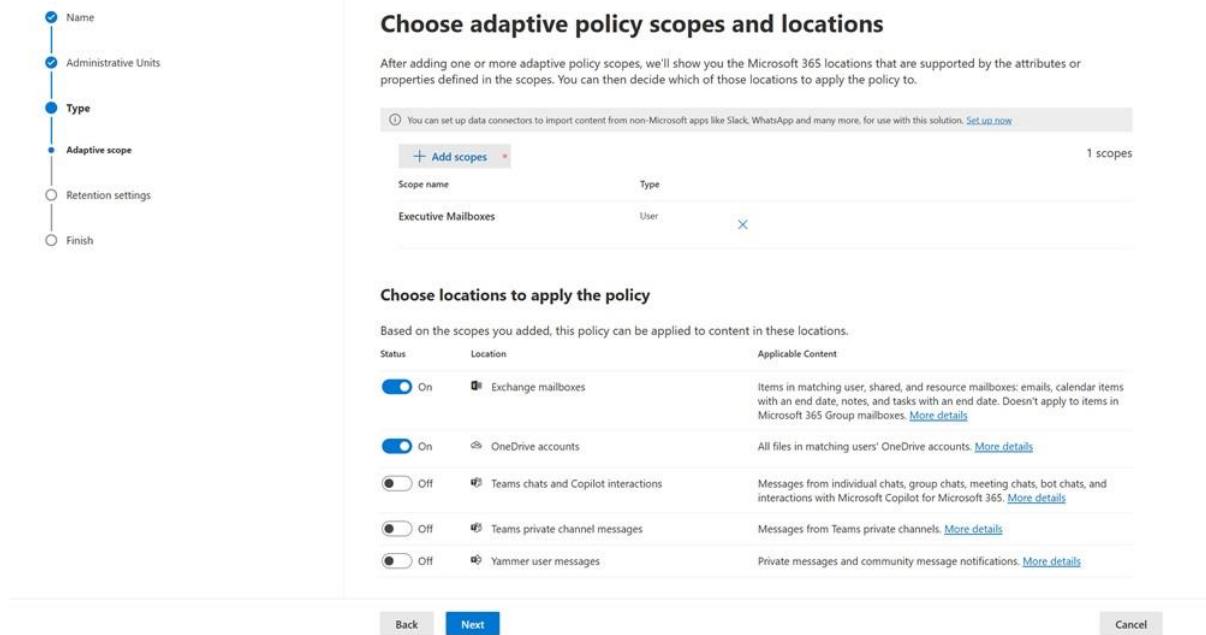


Figure 16-3: Using an adaptive scope in a retention policy

Planning a Retention Policy

Before beginning the process to create a new retention policy, it is sensible to write down the basic structure of the policy, broken down into several headings:

- **Broad or Narrow:** Do we need to apply default retention settings to some or all locations, or publish retention labels to allow users to dictate how to retain content? If the policy uses retention labels, what are those labels? Organizations often implement org-wide (broad-scope) policies to cover all workloads and all users with selective deployment of non org-wide (narrow-scope) policies to target specific workloads, users, or sensitive information types.
- **Scope:** What locations will this policy cover? If the policy targets a subset of locations within a workload (for instance, ten mailboxes or five SharePoint sites), write down those locations. If you want to exclude a subset of locations from the policy's scope, you should also note those locations. If the policy covers inactive mailboxes, this fact should be noted. If an adaptive scope will be used, some thought must be given to the query used to find the set of target locations. The scope of the policy (organization or Entra ID administrative unit) should also be noted.
- **Purpose:** Will the policy keep or remove content? If so, how long will the retention period be?
- **Records:** Is the content that comes under the scope of the policy considered to be a formal record for the company and if so, must the content be immutable? (See the sections on Preservation Locks and Records).

For the example used here, the conditions listed in Table 16-2 apply.

Heading	Policy setting
Scope	The policy applies to mailboxes and OneDrive for Business sites belonging to senior managers defined as members of the Senior Leadership Team (SLT) distribution list. It also covers the content held in the SLT group and team. The scope for targeted locations is static, not adaptive. Its management is at the organization level rather than scoped to an Entra ID administrative unit.
Purpose	The policy keeps all information in the targeted locations for ten years and then removes the content.

Type	This is a "non-org wide" policy. The group membership dictates the accounts to which the policy applies.
Lock	A preservation lock is not required.

Table 16-2: Planning a retention policy

It is bad to find yourself in a situation where you create and deploy a retention policy only to discover that the policy removes needed information. For example, it is very easy to apply an aggressive retention policy to "All Exchange mailboxes" that removes items after 30 days. This is the equivalent of a default delete tag in an Exchange retention policy to remove content after 30 days. When stamped on a mailbox, the Exchange Managed Folder Assistant (MFA) applies the "Delete and Allow Recovery" retention action to all items in the mailbox that do not have a more explicit tag. After items reach 30 days old, the MFA moves them to the Recoverable Items folder and preserves them for a further period (the deleted items retention period). When that period expires (usually 14 days), MFA permanently removes the items from the database. Exchange Online does not use backups, so you cannot recover the items at this point. Because retention policies affect the content stored in user mailboxes, it is only sensible to consider and understand exactly what will happen when a retention policy is active.

It is also possible that a retention policy will clash with an Exchange mailbox policy or another retention policy. It is a good idea to take some of the target locations and work out what policies have those locations within their scope to figure out if a clash occurs.

No Change for Retention Action or Period

A crucial factor to consider when planning the implementation of retention policies and labels is that you cannot change some of the important settings that control how the policy functions after creation. For example, you can alter the retention period for a policy, add new locations to its scope, and alter the KeyQL query to find content for the policy to apply. However, you cannot change its basic operation. For instance, you cannot change a policy that keeps content into one that simply removes content.

The logic is that users expect consistency in the processing of their data. If you can change the fundamental operation of how retention works inside a tenant, users will not know whether their data will be kept or removed or when this will happen. For this reason, it is wise to take time to chart out how retention will work across the tenant for all workloads before you create any policies. Fools rush to implement retention without thought!

Naming a Retention Policy

With our structure in mind, we can go to the **Microsoft 365** section of **Data lifecycle management** in the Microsoft Purview Compliance portal, select **Retention policies**, and then **New retention policy**. The first step is to assign a name and description (only visible to administrators) to the new policy. Some tenants insist that administrators include their name and a pointer to supporting documentation in the description of a new policy. It's more useful to include notes about what the policy does. For example:

"This is a retention label policy to publish a set of general-purpose labels to every location in the tenant."

"This policy publishes the Highly Confidential label to the Senior Leadership Team locations."

"This policy searches for content with the "Kazaa" keyword and applies the Ten Year retention label."

Administrative Units

Tenants with Office 365 E5 licenses can scope retention Policies using Entra ID administrative units. This means that Purview will apply the policy to user accounts defined by the administrative unit.

Setting the Scope for a Static Retention Policy

The simplest form of a retention policy is one that includes every available location, but quite often the need exists to focus on a select group of individuals and the data with which they work. Retention policies allow you to include or exclude subsets of locations. When you enable a retention policy for a location, you can choose the scope to be:

- **Org-wide:** Cover Exchange mailboxes, public folders, Groups, SharePoint Sites, and OneDrive for Business accounts. The policy applies to all content in all locations. As the tenant adds new locations, they come under the control of the policy.
- **Non org-wide** (choose specific locations): You can select individual mailboxes, sites, and so on. You can select everything from a workload, like all Exchange mailboxes, or you can select a subset of the locations available within a workload, such as only a few SharePoint sites. You can also exclude a selected subset from the policy. This means that the policy will not apply to the mailboxes or sites that you select.

Two special processing cases exist for retention policies. First, you can't exclude or include specific public folders, all of which are either processed by the retention policy or not. Second, you cannot mix inclusions and exclusions for a location in a policy. If you exclude some sites or mailboxes from a policy, it means that the policy applies to all other sites or mailboxes but not to those selected for exclusion.

A retention policy for Teams can only cover Teams content (chats, channel messages, or private channel messages). The same is true for policies covering Viva Engage, which process messages posted to Viva Engage communities. You cannot include another workload in a retention policy for Teams. However, you can have multiple retention policies for Teams that cover different subsets of users, or separate policies for channel messages and personal chats. Table 16-3 explains the various location types and how you input the selected locations.

Location type	Identified by
Exchange mailbox	Select All recipients to include all items stored in Exchange user mailboxes, otherwise, select the mailboxes to apply the policy. You can also input the name or alias of a distribution list or mail-enabled security group.
SharePoint site	Select All sites to include all the sites in the tenant or input the URLs for selected sites. Example: https://tenant.sharepoint.com/Projects/ .
OneDrive for Business accounts	Select All accounts to include all OneDrive accounts in the tenant or input the URLs for selected accounts. Example: https://tenant-my.sharepoint.com/personal/kim_akers_office365itpros_com/ .
Microsoft 365 Groups	Select All groups to cover all the mailboxes and sites used by Microsoft 365 groups in the tenant (but not the compliance items stored in mailboxes for Teams and Viva Engage) or the names of the selected groups.
Exchange public folders	Select All to extend the policy to cover every public folder in the hierarchy. The default is "None." You cannot select a subset of public folders.
Teams channel messages	Select All teams to cover messages posted to all channels in every team in the tenant or select the individual teams to come within the scope of the policy.
Teams chats and Microsoft 365 Copilot interactions	Select All users to include all personal chats sent by users in the tenant or select the users to come within the scope of the policy.

Teams private channel messages	Select All users to include the messages sent to private channels in all user mailboxes or select the users to come within the scope of the policy.
Viva Engage community messages	Select All communities to include all messages posted to Viva Engage communities or select the communities the policy will apply to.
Viva Engage user messages	Choose All users to include all private messages sent between Viva Engage users or select the users to which the policy will apply.

Table 16-3: Microsoft 365 workloads and locations supported by retention policies

Choosing Specific Locations

Figure 16-4 shows the user interface to add locations to a policy. Note that the default for a new retention policy is to apply the policy to all Exchange mailboxes, SharePoint Online sites, OneDrive for Business accounts, and Microsoft 365 Groups (mailboxes and sites – including those used by Teams). If you leave the target locations as the default, the new policy will apply the policy retention settings to everything in all mailboxes, sites, and OneDrive accounts across the tenant, which might not be what you want, as several organizations have discovered to their surprise.

To apply the policy to selected target locations, you must choose the individual locations. Some up-front work is often necessary to gather the information needed to specify individual locations. The easiest way to add a set of mailboxes to a retention policy with a static scope is to use a distribution list or a mail-enabled security group. Each mailbox counts against the 1,000 location limit for the policy. In addition, Microsoft 365 includes the owners of the distribution list in the mailboxes added to the set of locations (some consider the inclusion of distribution list owners as a feature; I believe it to be a bug). The population of the Exchange locations in the policy is a one-time operation and any future additions or removals to the membership of the distribution list do not synchronize with the locations in the retention policy. You must edit the policy to ensure that it continues to cover the correct individuals.

Status	Location	Applicable Content	Included	Excluded
On	Exchange mailboxes	Items in user, shared, and resource mailboxes: emails, calendar items with an end date, notes, and tasks with an end date. Doesn't apply to items in Microsoft 365 Group mailboxes. More details	All mailboxes Edit	None Edit
On	SharePoint classic and communication sites	Files in classic sites or communication sites or team sites that aren't connected to a Microsoft 365 group, and files in all document libraries (including default ones like Site Assets). More details	All sites Edit	None Edit
On	OneDrive accounts	All files in users' OneDrive accounts. More details	All user accounts Edit	None Edit
On	Microsoft 365 Group mailboxes & sites	Items in the Microsoft 365 Group mailbox, and files in the corresponding group-connected SharePoint team site. Doesn't apply to files in SharePoint classic or communication sites or SharePoint team sites that aren't connected to Microsoft 365 Groups. More details	All microsoft 365 groups Edit	None Edit
Off	Skype for Business	Skype conversations for the users you choose.		
Off	Exchange public folders	Items from all Exchange public folders in your organization.		
Off	Teams channel messages	Messages from channel conversations and channel meetings. Doesn't apply to Teams private channel messages. More details		
Off	Teams chats and Copilot interactions	Messages from individual chats, group chats, meeting chats, bot chats, and interactions with Microsoft Copilot for Microsoft 365. More details		
Off	Teams private channel messages	Messages from Teams private channels. More details		
Off	Yammer community messages	Messages from Yammer community discussions. More details		

Figure 16-4: Choosing target locations for a retention policy

While mailboxes are relatively simple to add to policies with static scopes, the same is not true for SharePoint Online and OneDrive for Business locations. This is because you must input the URLs for each location that you want to add to the policy. It can sometimes be difficult to know what the URL is for a location, so it's a

good idea to collect the URLs beforehand in a text file and cut and paste the URLs from the file into the policy. For example, you can use the `Get-SPOSite` cmdlet to output the URLs and export the information to a CSV file. It's relatively easy to automate adding SharePoint Online and OneDrive for Business locations to a retention policy with PowerShell. You can add up to a hundred individual sites in a non-org wide policy.

The processing of Teams chat and channel messages, Microsoft 365 Copilot interactions, and Viva Engage messages rely on compliance records stored in personal and group mailboxes. The rules are:

- Retention policies for chats and channel conversations cannot include any other non-Teams locations. Microsoft 365 Copilot interactions are an exception to the rule because these compliance records are captured using the same mechanism as Teams chats. Therefore, a retention policy configured for Teams chats also covers Microsoft 365 Copilot interactions.
- Retention policies for Teams private channel conversations cannot include any other location (even other Teams locations). It's important to note that retention policies for private channels operate based on individual accounts rather than teams. This is because the compliance records for private channel conversations are in user mailboxes and it's not necessarily true that all the members of a team are members of a private channel. To be sure of processing all messages for a private channel, add the mailboxes of all the members of the channel to the policy. Also, make sure that the SharePoint content for the channel comes within the scope of a separate SharePoint Online retention policy as the Teams private channel policies process only channel conversations.
- Retention policies for Viva Engage content process only Viva Engage locations.

After adding the target locations to the policy, click **Next** to continue.

Be Careful with Inclusions and Exclusions: Retention policies allow you to include or exclude specific locations. For example, you might create a policy to process a single mailbox or SharePoint site. If you edit the policy and remove the exclusion or inclusion, the target locations revert to All. This might be what you want (for example, you've tested the effect of the policy and are now happy to apply it to all locations in a chosen workload), but if it's not, it's easy to end up applying a retention policy inadvertently to all locations, which might remove items that the organization wants to keep.

Keeping or Removing Content

The final step is to define what the policy does to keep or remove content (Figure 16-5). When a retention policy removes items, it uses a "delete and allow recovery" action, to allow users to recover items later if needed from Exchange's Recoverable Items structure or the SharePoint recycle bin. In either case, we must know the length of the retention period and how to calculate the age of an item. You can keep content forever, but it is more common to set a period like seven or ten years. For mail messages, the creation date is used, but when a policy spans both documents and other items, it is best to choose the last modification date as shown here as this accommodates the fact that documents are often changed well after their creation date.

Administrators accustomed to working with Exchange mailbox retention policies see an immediate difference here. Exchange retention policies let you remove or archive items after the retention period lapses. While retention policies do not support an archive action, they let you say that you want to keep information for a set period. When the retention period lapses, you can choose to leave the content alone (in which case another policy could apply) or remove it. Alternatively, if you are more concerned about cleaning out locations to remove information that the organization no longer needs, you can instruct retention policies to remove items after they reach a certain age.

Decide if you want to retain content, delete it, or both

Retain items for a specific period
Items will be retained for the period you choose.

Retain items for a specific period

7 years

Start the retention period based on

When items were created

At the end of the retention period

Delete items automatically

Do nothing

Retain items forever
Items will be retained forever, even if users delete them.

Only delete items when they reach a certain age
Items won't be retained, but when they reach the age you choose, we'll delete them from where they're stored.

[Back](#)[Next](#)[Cancel](#)

Figure 16-5: Defining the actions a retention policy takes to process content

Immediate Evaluation: After you publish a retention policy, workloads make it active. This means that the workload processes that evaluate items know about the new policy. If you're not careful, the introduction of a new policy can have a significant effect on users. For example, let's say that you create a policy to remove items after three years and set the scope of the policy to be all OneDrive for Business accounts. After publication, the retention policy begins to evaluate items in all accounts and will remove anything more than three years old. If users aren't prepared for this clean-up to happen, the sudden removal of many items could come as a nasty surprise.

Reviewing Policy Settings

The last step is to review its settings. If all looks to be in order, click **Submit** to begin the publication process to the locations covered by the policy. You can opt to save the policy for later, meaning that the policy is in a draft state that you can complete and publish later (perhaps to add some extra locations).

It can take some time before a retention policy becomes fully effective across all locations. The assistants must process each location coming under the scope of a policy, including the compliance records stored for Teams and Viva Engage. You can check the distribution status of the policy by selecting the policy and viewing its properties. The following values are available:

- **Enabled (Success):** All locations know about the policy and are processing content as per the policy. However, the policy might still not be effective everywhere because background jobs might not have completed their processing to enable all locations.
- **Enabled (Pending):** The policy is being enabled in the target locations.
- **Enabled (Errors):** The policy is active, but some errors have occurred in its distribution.
- **Disabled (Success):** The policy is disabled and is not being applied to content. You can reenable the policy at any time.
- **Disabled (Pending):** Microsoft 365 is in the process of disabling the policy. All locations are stopping the processing of content. However, the process is incomplete.

- **Disabled (Errors):** The policy is off, but due to some errors, it might still be active in some locations. You can click the error to get more information. In many cases, the fault will disappear if you leave it alone for an hour or so.

Note that you can't disable a policy that applies a preservation lock.

The Actions Taken to Deploy Our Retention Policy

In terms of what you might have done previously with Exchange retention policies or SharePoint document deletion policies, the retention policy we just created has the following effects:

- The policy imposes a seven-year retention period on every item in the target mailboxes that do not already have an explicit mailbox retention tag (directly assigned on items or inherited from folders) or retention label. In addition, Exchange places an in-place hold on the mailboxes (both primary and archive) for seven years. During this period, Exchange preserves any item that a user removes from the mailbox in the Recoverable Items structure. The preserved items are indexed and discoverable. When an item's retention period elapses (in this case, seven years after creation), the Managed Folder Assistant applies a "Delete and Allow Recovery" action and moves the now-expired item into the Recoverable Items folder. The user can recover the item until the deleted items retention period set for the mailbox expires (usually 14 days).
- An equivalent seven-year in-place hold applies for documents and lists stored in SharePoint or OneDrive for Business sites. When users delete items, SharePoint Online captures copies of the items needed for retention in the preservation hold library for the site.
- The Exchange Online Managed Folder Assistant processes the contents of group mailboxes to apply retention policies. SharePoint Online treats the sites belonging to groups (teams) like other non-group connected sites.
- Although our policy does not cover public folders, if they were, any copies kept by policy stay in the public folder mailboxes to which they belong until the retention period expires. A process like that used to assess content removed from user mailboxes ensures that any attempt to remove held content from a public folder cannot succeed.

The Effects of Retention Policies

It's important to understand how content might come under the influence of retention settings through broad policies or the more precise application of retention labels:

- Broad retention publishing policies that define retention settings for locations (selected or org-wide defined through static or adaptive means) are invisible to users. These policies run in the background and users are unaware that retention is in force. This assignment is implicit because an item inherits the retention policy because of its location instead of having a retention label assigned by a user.
- Narrow retention publishing policies make labels available to users when they work with content in the covered locations. After publication, a user can assign one of the published retention labels to a document or mail message. This assignment is explicit because it takes a deliberate action by a user to assign the label.

Organizations can apply retention to an item in these ways:

- A user assigns a retention label to an item. This explicit assignment has the highest priority. Remember that a label used purely as a visual marker does not have a retention action or period.
- A location comes within the scope of a broad org-wide or non-org-wide policy, including policies that use advanced processing to find content. The items take the retention settings from the policy unless someone assigns a retention label to the item.
- The owner of a SharePoint site defines a default retention label for a document library. New items created in the library inherit the label. Library settings can also dictate if existing items receive the

- same label. A label inherited from a document library overrides any org-wide or non-org-wide retention policy assigned to the location.
- An auto-label policy assigns the retention label contained in the policy to items. An auto-label policy never replaces a label if a user has already assigned a label. Auto-label policies applied to Exchange Online mailboxes only process user-visible folders. For instance, an auto-label policy can't assign a label to items stored in Recoverable Items.

If their account has the appropriate permissions, users can change the retention label assigned to an item (unless the label is a regulatory record). They do not see or cannot affect the retention policy assigned to a location.

If multiple retention policies apply to an item, an explicit assignment always takes precedence over an implicit assignment. It is worth emphasizing that the presence of any type of retention affects the ability to remove a mailbox, site (including OneDrive for Business accounts), or group. Mailboxes holding retained items or under the scope of a retention policy become inactive when deleted until the retention expires. Sites and accounts cannot be removed until retention on individual documents, lists, and files lapses, and no retention policies are in effect for these locations.

SharePoint Online's Preservation Hold Library

To preserve copies of information required for retention purposes, SharePoint Online uses a special retention destination called the **Preservation Hold Library**. SharePoint Online creates the preservation hold library automatically when a site first needs to retain information about changes and deletions to files or lists. Once a site comes within the scope of a retention policy or individual items receive retention labels, user actions to remove or change content cause SharePoint to copy items to the preservation hold library. A single preservation hold library handles retention for the complete site, no matter how many document libraries and lists exist on the site.

User actions that cause SharePoint Online to capture information in the preservation hold library include:

- **Update or deletion of a document under a retention policy:** SharePoint Online captures a copy of the document. If versioning is enabled for the site (the default), SharePoint Online retains copies of all changes made to the document.
- **Deletion of labeled files (with unexpired retention periods):** Until a change deployed in November 2021, SharePoint Online stopped users from deleting labeled files and displayed a message saying that the label applied to the file blocked its removal. This behavior differed from OneDrive for Business and exposed a weakness in that members of a group could remove the label and then delete the file. With the change, both SharePoint Online and OneDrive for Business allow users to delete labeled files and capture the deletion in the preservation hold library. Users cannot remove files with a record label from either SharePoint Online or OneDrive for Business.
- **Unlocking of a retention label (record) on a file:** Users must unlock files assigned retention labels marked as a record before editing. SharePoint Online captures a copy of the file when it is unlocked.
- **Deletion of a OneNote section:** A copy of the section is captured.
- **Deletion of a OneNote notebook:** A copy of the notebook is captured.
- **Update of document metadata:** A copy of the update is captured.
- **Update or deletion of a list item:** A copy is captured in an Excel XLS. If the list item has an attachment, SharePoint Online captures the list and the attachment separately. The same happens if a user removes an attachment from a list item.

Not every change generates an update to the preservation hold library. The aim is to retain the original content before the imposition of retention controls plus the current content. When a user attempts to update or delete an item, SharePoint Online checks if this is the first action since retention for the item became active (or the policy changed). If it is, SharePoint Online captures the original content and allows the user to update

it. Any subsequent updates to the content are available in the versions that SharePoint Online captures automatically, meaning that the original content plus the complete change history are available through the data in the preservation hold library plus the online content. If a user deletes an item coming within the scope of a retention policy, SharePoint Online removes the item from the library or list and stores it in the preservation hold library until its retention period expires.

To reduce user awareness about what might be stored in the preservation hold library, SharePoint Online does not include the library in the set of resources shown in Site Contents. Site administrators can access the preservation hold library by adding */PreservationHoldLibrary* to the site URL. Because users administer their own OneDrive for Business account, they can access the preservation hold library for their account using a URL like:

https://office365itpros-my.sharepoint.com/personal/tony_redmond_office365itpros_com/preservationholdlibrary

Site administrators cannot remove or change items kept in the preservation hold library, but they can copy items from the library to retrieve a file or a previous version of a file on behalf of a user.

Using the Preservation Hold Library

Figure 16-6 shows items in a preservation hold library. SharePoint Online generates the names of the retained items by combining the original name with a GUID (and sometimes the date and time of the change) to create a unique value.

Name	Modified	Modified By
Office 365 for IT Pros 9 - June 2023_CD0ADBAF-8D35-47E0-A4A7-2F3C0...	May 22	Tony Redmond
21 Managing Reporting and Auditing_C7C1A08E-0EE6-4CA4-B65D-FB935...	May 10	Tony Redmond
13 Managing Teams_BE72E17A-B523-41FA-8107-E930C0FF1C472023-05...	May 1	Tony Redmond
_siteicon__AAEFDBA4-0843-4DCA-B8F7-27E473BBEA3A2023-05-01T20...	May 1	System Account
_siteicon__AAEFDBA4-0843-4DCA-B8F7-27E473BBEA3A2023-05-01T20...	May 1	System Account
23 Managing Tenants with PowerShell_2145A420-86CE-4796-9DC0-B2B5...	May 1	Tony Redmond
03 Managing Identities_3A6C2D08-451E-409B-A393-E0DFC88619C82023...	April 30	Tony Redmond
03 Managing Identities_79644CCE-9329-489C-9589-C593B95EF0F02023...	April 30	Tony Redmond

Figure 16-6: Items in the Preservation Hold library for a SharePoint site

When users add new items to a library, several operations happen to create the item, apply updates, add metadata, and so on. SharePoint Online captures none of these actions in the preservation hold library. However, after the initial creation, SharePoint Online monitors and captures subsequent updates to files.

Every week, a background job runs to clean out old items from the preservation hold library. The job looks for items in the library for more than 30 days and compares them against the retention settings applicable to the site to find and remove items with expired retention periods. If the file or list item is still present in its original location, the background job removes it too. SharePoint Online never deletes items directly from a preservation hold library. Instead, the background job moves items no longer needed for retention from the preservation hold library into the second stage recycle bin. Normal recycle bin processing continues from this point and SharePoint Online removes the items permanently after the 93-day period in the recycle bin expires.

Originally, SharePoint Online stored separate files for versions of deleted files. This implementation had several undesirable side-effects, the most notable of which being that the results returned by eDiscovery searches could be confusing because of the matches against multiple versions of deleted files. In mid-2022, Microsoft implemented a different approach for the Preservation Holds Library by storing single files for retained items that include previous versions in their version history. This approach is consistent with how SharePoint Online stores multiple versions of Office documents in regular document libraries.

eDiscovery searches return a single match against a deleted file and investigators can decide which version of the file they wish to use. The new behavior is not retrospective, so as you scan files in the Preservation Hold Library, you'll see that multiple entries appear for older files while newer files have a single entry.

Files in the site recycle bin and those retained in SharePoint Online because of a retention policy count against the overall storage quota for the tenant. When a retention policy is in place, the SharePoint admin center can help you understand the effect of retention through the storage metrics available through site settings (Figure 16-7). The fact that retained files occupy 21.87% of the total storage for the site underlines how much tenant quota retention can consume.

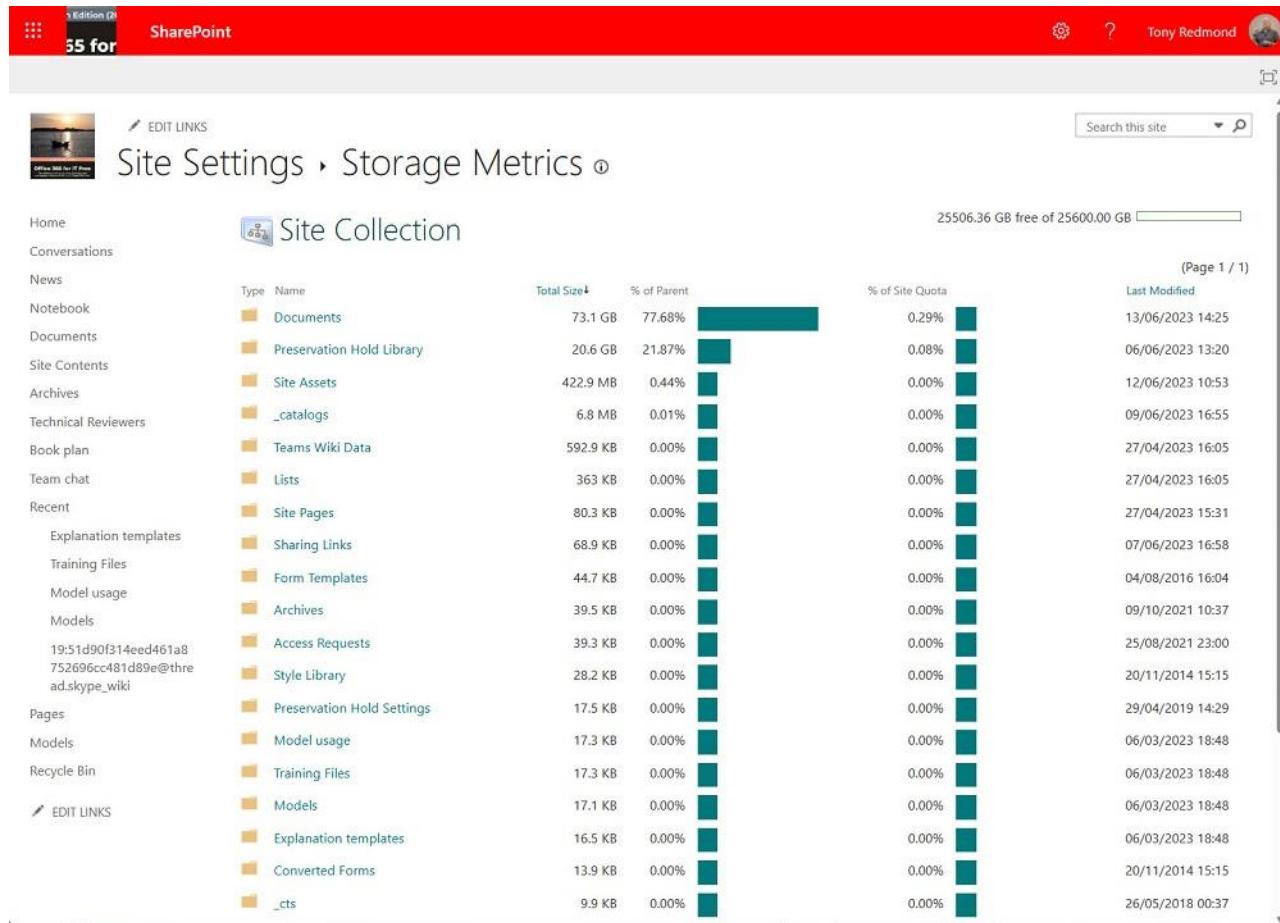


Figure 16-7: Site Settings include useful data about storage metrics

Your mileage might vary in terms of storage consumption for retained files. The number of files retained by policy differs from site to site and is highly dependent on user activity and the size of the files. If people create and save files and never edit them again, no extra versions exist and no deletions happen, so few files end up in the preservation hold library. On the other hand, if you constantly edit files stored in a library, the versions accumulate (especially through Office's Autosave feature) to consume storage. This is especially evident in libraries that store large files with frequent updates, such as the Word documents for the chapters for this book.

Purging the Preservation Hold Library After Removing a Retention Policy

When an administrator removes a retention policy from a site, a 30-day grace period starts to stop the release of the hold on the site. During the grace period, SharePoint Online preserves the items in the preservation hold library because the hold is still in place. Once the 30-day grace period elapses, the hold lapses and SharePoint Online proceeds to delete the items. Items deleted from the preservation hold library go into the second-stage recycle bin instead of an immediate purge. Items stay in the second-stage recycle bin for up to 93 days after their deletion before permanent removal. During this time, site administrators can recover items.

This mechanism gives administrators the ability to recover from the consequences of an error in removing a retention policy that results in data loss. Instead of having background processes purging content soon after the removal of a retention policy, administrators can access the preservation hold library and second-stage recycle bin to recover data during the grace period. Recovering data from these locations is a manual process that will take time and effort, but at least it's better than losing valuable documents.

Knowing That a Retention Policy Works

It can be difficult for a user to know that a retention policy is in force. It can also be difficult for an administrator to know when retention policies work as expected. Here are some ways to verify that all is well:

- For **user mailboxes**, you can check to see whether the retention tag assigned by a policy is stamped on folders and messages as expected. Clients display these tags like older Exchange Online retention tags, so if Outlook or OWA displays the tag, you know that the policy is working. Another method is to check the Purges sub-folder of Recoverable Items to see if retained items accumulate there.
- Conversations in **group mailboxes** do not display retention tags. You must check that the items in the Inbox folder are what you expect based on the retention policy in force. You can also check that the Managed Folder Assistant is processing the group mailbox and removing items.
- **Teams** and Viva Engage compliance records are in special hidden folders in group and user mailboxes. You can use the MFCMAPI utility to check these folders to ensure the expected retention of compliance data. Another (easier) method is to use the *Get-ExoMailboxFolderStatistics* cmdlet to check the number of items in the folder before the retention assistant processes it and compare it to the number of items reported afterward. For example, the command below shows that the oldest item in the folder used to hold Teams compliance items (for group mailboxes, items from all channels are in the same folder) is from 7 October 2020. You know the retention period defined in the policy, so it is easy to calculate what the date of the oldest item should be if the retention policy is working.

```
Get-ExoMailboxFolderStatistics -Identity 0365ITPros -ResultSize Unlimited -FolderScope NonIPMRoot -IncludeOldestAndNewestItems | Where-Object {$_.FolderType -eq "TeamsMessagesData"} | Format-Table Name, ItemsInFolder, NewestItemReceivedDate, OldestItemReceivedDate
```

Name	ItemsInFolder	NewestItemReceivedDate	OldestItemReceivedDate
TeamsMessagesData	15613	02/06/2023 16:10:41	7/10/2020 08:17:09

- Documents stored in **SharePoint Online** and **OneDrive for Business** sites, including the sites used by Groups, show no trace of retention because everything remains in place until user actions trigger the need for SharePoint to capture copies of documents. If a policy dictates the retention of an item, and someone attempts to remove it, SharePoint creates a copy of the item in the site's Preservation Hold library. The capture happens even if a retention label stops the user from removing an item. The site collection administrator can access the Preservation Hold Library to verify the capture of changes or deletions for files under the control of retention policies are there.
- Check the audit log to look for *FileRecycled* events logged for deletions of SharePoint Online and OneDrive for Business items because their retention period expired, and the retention action forces a deletion. Among the information captured in *FileRecycled* events is which account removes an item. In

the normal course of events, the data captured in the user property is the User Principal Name of the account. When a retention policy or label causes a deletion, the audit event captures the name of the policy or label. For example, this command searches for all *FileRecycled* events logged during the last 30 days:

```
Search-UnifiedAuditLog -Operations FileRecycled -StartDate (Get-Date).AddDays(-30) -EndDate (Get-Date).AddDays(1) -ResultSize 2000 -SessionCommand ReturnLargeSet
```

After retrieving the audit events, you can use the techniques explained in the Auditing and reporting chapter to interpret the data and generate an analysis. A review of the information reveals if retention processing deleted files. In this example, a user deleted two files and a retention policy deleted the next three files.

TimeStamp	User	File
-----	----	----
2018-11-28T15:15:22	tony.redmond@office365itpros.com	Board Meeting Agenda 12 Sept 2018.docx
2018-11-28T15:22:17	tony.redmond@office365itpros.com	Privacy Policy for Website.docx
2018-12-04T03:51:45	Preservation Lock - Mailboxes and Sites	Encoding Time.csv
2018-12-04T03:51:46	Preservation Lock - Mailboxes and Sites	TeamsNotebook(Shared).onetoc2

Retention Policy Lookup

Sometimes many different retention policies affect an individual location (user, site, or group) and it's difficult to understand what influence these policies have on the location. For example, the SharePoint admin center might inform you that a retention policy is blocking a site from deletion, and you want to find out what policies might be the block. To help understand the set of policies that apply to a location, use the **Policy Lookup** feature in the **Data lifecycle management** (Microsoft 365) section in the compliance portal. To lookup the policies for a location, enter the:

- Primary email address of a user.
- URL for a SharePoint Online site or OneDrive for Business account.
- Primary email address of a Microsoft 365 group.

The screenshot shows the Microsoft Purview Data lifecycle management interface. The top navigation bar includes links for Overview, Retention policies, Labels, Label policies, Adaptive scopes, Policy lookup (which is underlined in blue), and Import. A search bar at the top allows searching for specific users or SharePoint sites. The main content area is titled "Data lifecycle management" and displays a list of retention policies applied to the user "rene.artois@office365itpros.com". The list includes the following policies:

Policy name	Scope types	Applications	Last modified	Date created
Cloud Attachments Auto-Label Policy	OrgwideScope	OneDriveForBusiness	Nov 30, 2023 10:22 AM	Nov 30, 2023 6:52 AM
Office 365 for IT Pros Static Retention Policy	StaticScope	Exchange, OneDriveForBusin...	Feb 20, 2024 5:11 PM	Nov 10, 2022 3:38 PM
Office365ITPros.com accounts	AdaptiveScope	Exchange, OneDriveForBusin...	Feb 20, 2024 5:12 PM	Nov 10, 2022 3:25 PM
Ultra Confidential Documents	OrgwideScope	OneDriveForBusiness	Dec 24, 2021 10:41 AM	Nov 30, 2021 1:28 PM
Yammer messages	OrgwideScope	Yammer	Jun 18, 2022 3:42 PM	Nov 11, 2021 3:43 PM
Teams Private Channels	OrgwideScope	MicrosoftTeamsChannelMes...	Jul 18, 2022 4:42 PM	Jun 30, 2021 7:24 PM
Auto-Label Recordings of Teams Meetings	OrgwideScope	OneDriveForBusiness	Jun 11, 2021 10:33 AM	Jun 11, 2021 10:33 AM
Regulatory Label Policy	OrgwideScope	OneDriveForBusiness	Oct 9, 2021 1:20 PM	Nov 5, 2020 11:36 AM
Preservation Lock - Mailboxes and Sites	OrgwideScope	OneDriveForBusiness	Nov 30, 2018 6:50 PM	Nov 30, 2018 6:49 PM

Figure 16-8: Looking up the retention policies applying to a user

The response is the full set of retention policies for the selected location. These can be:

- Label publishing policies for which the location is a target. In other words, policies that make labels available for use by the user or in the site or group.
- Auto-label retention policies that process the location.
- Retention policies that include the location in their scope.

Figure 16-8 shows a typical result where a user account is subject to seven policies, one of which has an adaptive scope. The others are all org-wide policies created for different reasons, including specific policies for locations like messages in Teams channels. Two of the policies are label publishing policies (for example, the manual disposition label policy publishes labels used for manual disposition), but the only way to know this is to recognize the policy name. Disabled policies are in the list, so the need exists to check policies to understand the full coverage of retention.

The results of a retention policy lookup only include Microsoft 365 retention policies. They do not include Exchange Online mailbox retention policies or litigation holds.

Retention Policies and Inactive Mailboxes

An inactive mailbox is a mailbox kept for compliance or some other reason that belonged to a now-removed Microsoft 365 user account within the scope of a hold placed before deletion. Including a mailbox in the locations processed by a retention policy ensures that a mailbox becomes inactive if its account is removed, but only if the policy settings keep content. A policy configured to remove content does not transform a mailbox into inactive status upon deletion. This is logical because if you deploy a policy to remove content from mailboxes, it doesn't follow that you want to keep mailboxes after their accounts are deleted.

It is a good idea to have a retention policy to hold the complete contents of user mailboxes for a period after deletion. To make this work, you must add the mailboxes to the policy (up to 1,000 mailboxes can be included

in a single policy) before removing the account. Alternatively, you can use an org-wide policy that covers the content in all mailboxes. In either case, when the account is deleted, Exchange Online recognizes that one or more hold exists on the mailbox and makes the mailbox inactive. See [this page](#) for more information on how retention policies process inactive mailboxes.

Hybrid Governance

Retention policies do not apply to on-premises locations such as Exchange mailboxes, public folders, or SharePoint sites. The same issue occurs for content searches and eDiscovery cases. If you have a hybrid environment, it's a good idea to try to have the same retention policies (or as close as possible) apply in both on-premises and cloud locations and be prepared to perform eDiscovery processing on both platforms to capture all information necessary to satisfy eDiscovery searches. Unfortunately, synchronizing retention policies across on-premises and cloud environments is a manual process.

Groups, Teams, and Retention

When a group is deleted, it enters a 30-day soft-deleted state. Following this period, Entra ID permanently removes the group, and it becomes irrecoverable. Deletion of the group also removes all the linked resources associated with the group. However, if content in the group mailbox or the SharePoint site belonging to the group (or team) comes within the scope of a retention policy or retention label, the group mailbox and/or site is retained until the retention period expires. The group mailbox becomes an inactive mailbox while the SharePoint site becomes a deleted but retained site.

Retention Processing for Teams Compliance Records

When we discuss retention for Teams content, it is important to understand that retention policies process the compliance records that the Microsoft 365 substrate creates to record messages posted in channel conversations and chats. The substrate also creates compliance records for messages posted in channels by Office connectors. The compliance records are in a folder called *TeamsMessagesData* in the system part of user, group, and cloud-only mailboxes that are invisible to email clients. Retention policies do not directly process any data in the Teams message store in Azure Cosmos DB. Synchronization with Exchange apply the effects of retention to that store.

Retention policies can process all Teams accounts with a valid Office 365 license. However, a difference exists between accounts with enterprise licenses (Office 365 E3 and E5) and other licenses. Accounts with enterprise licenses can use retention periods as low as one day while the other accounts have a minimum retention period of 30 days.

When a Teams retention policy is active, the substrate retains all changes users make to Teams messages that come within the scope of the policy. If a user modifies or deletes a message in a personal chat or channel conversation, the substrate moves (for deletions) or copies the message to the *SubstrateHolds* subfolder of the Recoverable Items folder. Messages remain in *SubstrateHolds* until their retention period expires.

The retention assistant processes mailboxes covered by Teams retention policies to remove compliance records according to the criteria set in those policies. Different policy settings cover chat and channel messages. Messages in chats are "owned" by all the chat participants, so each participant has a copy of each message in their mailbox. As chats are removed from mailboxes by retention processing, the number of references to a message drop until it eventually reaches zero. At that point, Teams removes the message from its data store in Azure Cosmos DB. Only one copy of channel messages exists in the group mailbox belonging to the team. When retention processing removes the item, synchronization removes the message from the Teams data store.

MFA processes Teams compliance records in the same way that it deals with other mailbox items (for example, MFA doesn't process a mailbox holding compliance records if its size is under 10 MB). The date used to determine whether items exceed their retention period are the creation dates of compliance records in the *TeamsMessagesData* folder.

When MFA removes Teams compliance records, it first moves the messages from the *TeamsMessagesData* folder to the *SubstrateHolds* folder. Messages remain in *SubstrateHolds* for a day before MFA permanently removes the items from the mailbox. During this period, a background job removes the source items in the Teams data store in Azure Cosmos DB and later, through server-to-client synchronization, from client-side caches. The minimum period for Teams compliance policies is one day. However, depending on the load on different components across the service and how often clients connect to the Teams service, the end-to-end removal process usually takes a couple of days to complete and can take up to a week. Administrators should take great care when creating or amending the settings of Teams retention policies as an error might lead to an irrecoverable data loss like [that suffered by KPMG](#).

Retention policies do not process system messages posted to channels (for example, the addition or removal of a member). In addition, processing might not cover some older messages posted by guest or hybrid users because no matching compliance records exist.

If you want retention policies to apply to the content posted in the SharePoint document libraries used by Teams, you must include those sites in the **SharePoint** section of the retention policy. A retention policy cannot process data stored in other locations used by Teams such as third-party applications accessed through tabs or bots.

Retention policies for Teams messages cannot use the advanced features to search for content based on keyword queries or sensitive information types.

Be Careful with Short Retention Periods: The reason why Teams supports a 1-day minimum retention period is that some organizations don't like the idea of keeping chats around for any longer. Although there can be good business reasons for such a stance, it's important to understand the downside. If you configure a very short retention period for items, the intended recipient might never see some messages. For instance, a message sent on Friday might be removed before the recipient checks for new messages on Monday. Short retention periods are really to cover scenarios where messages do not need to be persistent. In most Teams scenarios, removing chats and conversations quickly can mar business effectiveness if you're not careful and users understand just how quickly items are removed.

Org-wide Policies and SharePoint Online Sites

When an org-wide retention policy covering SharePoint sites is deployed, SharePoint Online keeps deleted sites until their retention period expires. The policy spans all SharePoint sites in the tenant, including the team sites belonging to Groups and Teams as well as the hidden sites used by Teams private channels. This is expected behavior: SharePoint is told to retain deleted sites for a period and that's what it does.

If you want to permanently remove a deleted SharePoint site before the retention period expires, you must:

- Use the SharePoint Admin Center to restore the site from the Deleted sites list. If the site was connected to a group and more than 30 days have elapsed since the group was deleted, you won't be able to restore the group and reconnect the site.
- Wait a few minutes after the site restore finishes and then edit the retention policy to exclude the now-restored site from the locations covered by the policy (you can't exclude a deleted site from a retention policy because it's already deleted). The delay allows the Microsoft Purview Compliance portal to recognize that the site exists.

- Wait another little while for the amended retention policy to be effective and then delete the site from the Active sites list in the SharePoint Admin Center.
- Finally, permanently remove the site from the Deleted sites list.

Applying Retention Policies to Microsoft 365 Groups

By default, when retention policies cover Microsoft 365 groups, the same retention settings apply to content in both the mailboxes and the SharePoint sites owned by the groups. You cannot, for instance, remove conversations after a month and keep documents for a year. If you want retention policies to process either mailboxes or sites, you can update the policy with PowerShell by running the *Set-RetentionCompliancePolicy* cmdlet. For example:

To process only the contents of group mailboxes covered by the policy:

```
Set-RetentionCompliancePolicy -Identity "General Retention Policy" -Applications "Group:Exchange"
```

To process only the contents of the SharePoint team sites for groups covered by the policy:

```
Set-RetentionCompliancePolicy -Identity "General Retention Policy" -Applications "Group:SharePoint"
```

To reset the policy so that it covers both mailboxes and team sites:

```
Set-RetentionCompliancePolicy -Identity "General Retention Policy" -Applications $Null
```

The Managed Folder Assistant (MFA) processes the group mailbox to remove or keep items based on the settings in a retention policy. MFA will not process mailboxes unless they hold more than 10 MB of data, so MFA might never process some groups, even if their mailboxes hold several hundred conversation items. The information in the group team site does not count against the 10 MB threshold. You can use the *Get-ExoMailboxStatistics* cmdlet to check the current storage for a group mailbox:

```
Get-ExoMailboxStatistics -Identity Office365TenantServiceHealth | Format-Table DisplayName, TotalItemSize, ItemCount
```

DisplayName	TotalItemSize	ItemCount
Tenant Service Health	11.29 MB (11,836,393 bytes)	154

In this case, MFA will process the group mailbox. See the section about Logging the Managed Folder Assistant later to understand how to see a summary of the actions taken by the MFA to remove items from a mailbox per the settings of a retention policy.

Removing Retention Policies

To remove a retention policy, select it in the Microsoft Purview Compliance portal and take the **Delete policy** action. When you remove a retention policy, Purview notifies the affected workloads that the policy no longer exists so that they cease to implement it. Retention labels applied by automatic label policies stay in place after the removal of that policy.

The next time a background process reviews content, it might apply a new retention policy to items. The time taken to switch retention policies depends on how quickly workloads cease processing the original policy and how soon afterward the content covered by the original policy is reevaluated.

If you delete a label publishing policy, the labels published by the policy are no longer available in the locations covered by the policy. However, any labels applied when the policy remain assigned to items.

Preservation Locks

Some regulatory regimes require that after an organization implements a retention policy, administrators cannot turn the policy off or make it less restrictive. To meet this need, you can apply a preservation lock to a retention policy. After applying a preservation lock to a policy, an administrator cannot disable the policy or remove locations from the policy. The lock remains in force and active for all locations under the scope of the policy until the retention period expires. Users cannot remove or update content within the scope of the policy during this period either. The only option open to an administrator is to add locations to the policy or extend its duration.

To lock a retention policy, set its *RestrictiveRetention* property through PowerShell. For example:

```
Set-RetentionCompliancePolicy -RestrictiveRetention $True -Identity "Management Preservation Policy"
```

Microsoft can remove the preservation lock from a retention policy. If you get into a situation where you need this to happen, the tenant administrator must open a support incident and supply Microsoft with the details to justify unlocking. If Microsoft concurs, they will remove the preservation lock from the policy. Because the potential exists that Microsoft might not agree to unlock a policy, it is wise to pause and think before enabling preservation lock on a retention policy. You might need to implement such a policy to satisfy a legal or regulatory need, but in most cases, tenants do not need to lock down content in this way. In short, make sure that you need a preservation lock before turning it on for a policy. Apart from waiting for the policy to expire, there is no way back if you make a mistake and enable the lock-in error.

To discover if any policies include preservation locks and the workloads they cover, view its details through the Microsoft Purview Compliance portal or run this command:

```
Get-RetentionCompliancePolicy | Where-Object {$_._RestrictiveRetention -eq $True} | Format-Table Name, Workload
```

Note that if you move a mailbox that is subject to a preservation lock back to an on-premises Exchange server, Exchange Online keeps a copy of the mailbox to satisfy the lock. The copy held in Exchange Online is a point-in-time copy and no mechanism exists to synchronize the two copies after the mailbox moves.

Retention and Sensitivity Labels

Two forms of compliance labels exist within Office 365:

- **Retention labels:** Mark content like documents and messages that the organization wants to retain, like keeping certain documents because they hold valuable information, such as accounting records, sales records, and so on. Users apply labels to messages or documents to mark the items as a visual marker of the importance of the content or to make sure that Microsoft 365 keeps the item for a set period. Two types of retention labels exist: standard and record. Standard labels are the more common type while the major use of record labels is in the Records management solution, covered later.
- **Sensitivity labels.** Apply marking with optional protection to content. [Sensitivity labels](#) are how Microsoft has extended the functionality of the original Azure Information Protection labels as part of their Microsoft Information Protection initiative. They refer to these labels as “unified” because they bring together the work done by Azure Information Protection to make it easy for users to self-classify content by applying labels in the Office applications with the data governance framework. Applying a sensitivity label to an item can protect it through encryption or add visual indicators such as watermarks to show users the importance or sensitivity of the information. See the Information protection chapter for more information about how to define sensitivity labels and deploy them to users through sensitivity label policies.

When we refer to the two types of labels in general, we say "labels" or "Office 365 labels." Otherwise, we refer to the specific type. The information presented here covers retention labels.

Retention Label Concepts

A retention label can be passive, meaning that it serves as a marker for a certain type of content but takes no further action because it doesn't have any retention settings. Passive labels are useful to mark content that someone will need to process in the future or to find items belonging to a project. Mostly, retention labels are active, meaning that the label has a defined retention action and period. The action tells the owning workload to keep content for the period or to remove content after that period. For instance, the organization might decide to retain all documents marked with the "Confidential" label for five years and removed afterward. Auto-label policies remove the need for users to apply labels manually. The combination of manual (explicit) and auto-applied (implicit) classification gives tenants great flexibility in how they manage important content.

Items such as a document or message can only ever have one retention label (it can also have a sensitivity label). Apart from the precedence of manually-applied retention labels, the other rules are:

- Anyone with write access to content can change the label assigned to that content whether the item receives a label manually or automatically. For example, if an email has the "Confidential" label, the user can go ahead and change that label to any other available label. The exception is retention labels that mark items as formal company records. Once a user applies a record label to an item, the item can't be edited, updated, or removed until its retention period lapses (for instance, Exchange Online keeps deleted records in the Recoverable Items structure).
- Retention labels applied automatically can never overwrite labels manually applied by users.
- If multiple auto-label policies match an item, the workload uses the label belonging to the oldest policy. On the creation of a label policy, the policy receives a priority number incremented from 0 (zero) as more policies are created. Thus, the policy with the lowest number is the oldest. You can discover the priority order for policies by running the *Get-RetentionCompliancePolicy* cmdlet as shown below:

```
Get-RetentionCompliancePolicy | Where-Object {$_.Enabled -eq $true} | Sort-Object Priority | Format-Table Name, WhenChanged, Priority
```

Name	WhenChanged	Priority
Management Preservation Policy	13/04/2018 13:02:36	0
Company Confidential Policy	17/06/2023 15:52:57	1
Preserve Office 365 for IT Pros Files	01/07/2022 17:10:49	10
Senior Leadership Team (SLT) Retention Policy	20/02/2024 17:15:22	15
Office 365 for IT Pros eBook Content	06/12/2021 16:25:55	16
SharePoint Online Retention Policy	26/07/2021 20:52:24	26

You cannot change the priority order of retention policies.

Planning Retention Labels

The first thing to decide is what labels the organization needs to build out the retention strategy. Broadly speaking, you can divide retention labels into the following categories:

- **Targeted:** Retention labels needed by certain departments and used for specific purposes. For example, "Project Documentation," "Board Minutes," or "Patent Material." These labels usually keep information that is of high importance to the organization and might be published to a select group of locations.
- **Generic:** Retention labels used anywhere in the business. Often, these labels are named after the length of the retention period, as in "Keep Five Years." They might also have names that describe the

business purpose, like "Commercially Sensitive" or "Required for Audit." These labels are usually published to all locations in an org-wide policy.

- **Special-Purpose.** Retention labels that the organization creates for a specific well-defined purpose. For example, to mark and keep a set of information needed for a merger and acquisition project.

After consulting with business units (including the IT department) to gather suggestions for retention labels, you can rationalize the set to a manageable number. Each label should serve a distinct and obvious purpose definable in clear and easily understandable terms. In addition, you should be able to say where the records marked by labels are stored. For example:

"We are required to preserve financial records for five years because we can be audited during this period. We need a label to mark these records and ensure that they are retained for at least five years. Items needed for audits include messages and documents across all mailboxes and sites."

It is sensible to write down each of the retention labels that you plan to use before creating anything. It is much easier to delay the release of a label and the training of users to use the label properly than it is to launch a label into general circulation only to discover that you later need to withdraw it. Another thing to consider is how easy it is for users to decide between different retention labels when the time comes for them to apply a label. Too many labels, misleading names, or too many choices can lead to frustration and bad decisions.

Other points to consider include:

- An item can only ever have a single retention label. To change a label, you must remove the original label and replace it with another. Sometimes, you might have to remove a label from an item before you can remove the file.
- A retention label applied by a user always has the highest priority.
- If you use automatic label policies to apply labels to content found using a keyword query or because the content has sensitive data, you might find yourself in a situation where some documents come within the scope of multiple policies. A tiebreaker decides which policy to apply. The tiebreaker is the age of the policy, and the workload always complies with the oldest policy.
- Although auto-label policies cannot replace labels assigned by users, they can replace labels previously automatically assigned to items by other policies.

In summary:

- Make sure that every retention label has an obvious purpose.
- Try to have a small number of retention labels so that it is easier for users to make good choices about for how long they should keep content.
- Create retention labels and policies in priority order.
- Deploy auto-label policies after users have had a chance to apply retention labels manually.

Removing a Site: Before you can remove a SharePoint Online site, you must remove any documents that have retention labels from the site. Normally, this means that you must remove the label from the documents and then delete them.

Creating New Retention Labels

After understanding the labels necessary to implement the data governance policy, we can create them through the Data lifecycle management section of the Microsoft Purview Compliance portal. Click **Labels** and then **Create a label**. You can then start by entering the name of the label and some text to describe the purpose of the label for administrators and a separate description that is visible to users when they browse labels as they classify material.

Naming a Retention Label

The name given to a retention label is important because this is what users see when they use the label to classify a message or document. One issue for multilingual tenants is that no facility exists to translate labels. Whatever name you give to a label shows up in clients, no matter what language they use. For this reason, it is best to give labels names that are simple to understand and unambiguous in their intent as this will make it easier to communicate how to use the labels to classify information.

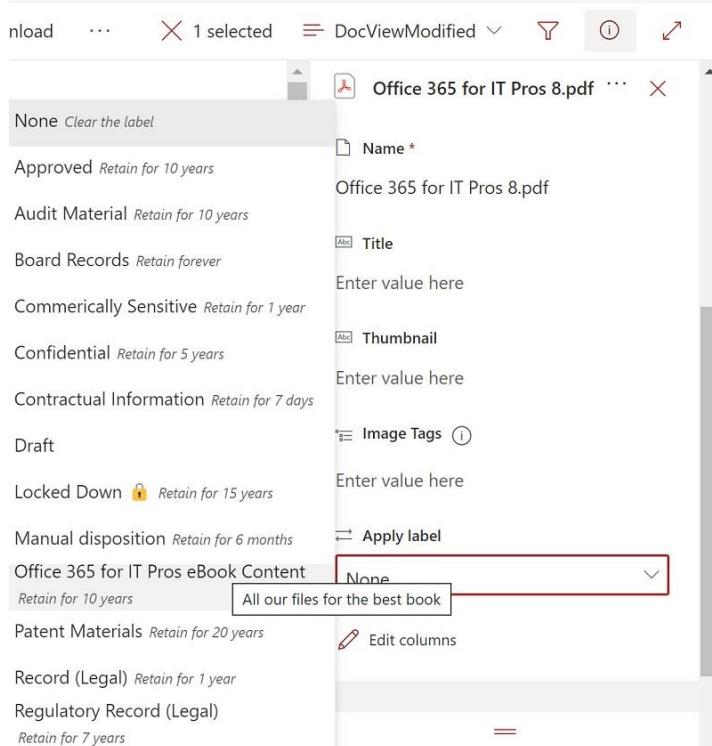


Figure 16-9: Selecting a retention label to apply to a SharePoint document

For example, if we publish a label to OneDrive for Business and SharePoint Online, people can use the label to classify a document stored on a site by amending the document properties and selecting the label. As you can see in Figure 16-9, two visual hints are available to help users understand the purpose of a label: its name and the descriptive text that appears when they hover over the label. You can also see that it's possible to include Windows emojis in the display name of retention labels to deliver a visual hint to users about a label's purpose.

Retention Actions and Periods

The next step is to define how workloads will process items with a retention label. You must choose what action the label will apply and when the action occurs. A retention label can:

- **Retain items forever or for a specific period.** The specific period is the number of days that elapse before workloads process the retention action. If instructed to keep items forever, the workload stores the items in its retention location (recoverable items folder or preservation hold library).
- **Enforce actions** after a specific period. Once the item reaches the set age (retention period), it is removed.
- **Just label** items. These labels act as visual markers for the type of information in an item (sensitivity labels with no encryption that apply watermarks, headers, and footers might be a better choice). For instance, you could create a "Draft" label to allow users to mark items that have not yet reached the point where the content is interesting or valuable enough to justify its retention. Another way of using labels without actions is as a convenient way to find information with content searches (for instance,

find all documents for "Project X"). Labels that do not have a retention action show up with a "Never" expiration date when viewed through Outlook or OWA.

If you choose to keep items for a specific period, you can choose between date-based retention or event-based retention as the baseline for the retention period. For date-based retention, you select one of the three predefined periods (5, 7, 10 years, or forever) or a custom period in years, months, and days. The GUI allows the selection of a retention period of over 100 years, but a shorter period is best. You then choose the basis for the retention period:

- The **creation date** for items: This is the default and works well for most items.
- The **last modification date** for items: This is a better retention base for documents that go through multiple review cycles before finalization.
- The date when a user or policy applies a **label** to an item.

If you use event-based retention instead of date-based retention, the retention period starts when the event occurs. Some of the standard event types are listed below. You can create additional event types to meet business needs. We cover event-based disposition in the Records Management section.

- Employee activity.
- Expiration or termination of contracts and agreements.
- Product lifetime.

The user interface presented to create a retention label depends on its settings. Figure 16-10 shows how to configure a label with a seven-year retention period based on the creation date for items. When the retention period for an item expires, the owning workload deletes the items. This means that the next time that the item goes through retention processing, its expired status causes the workload to apply its normal deletion process. For instance, a document removed from a SharePoint Online site goes into the recycle bin.

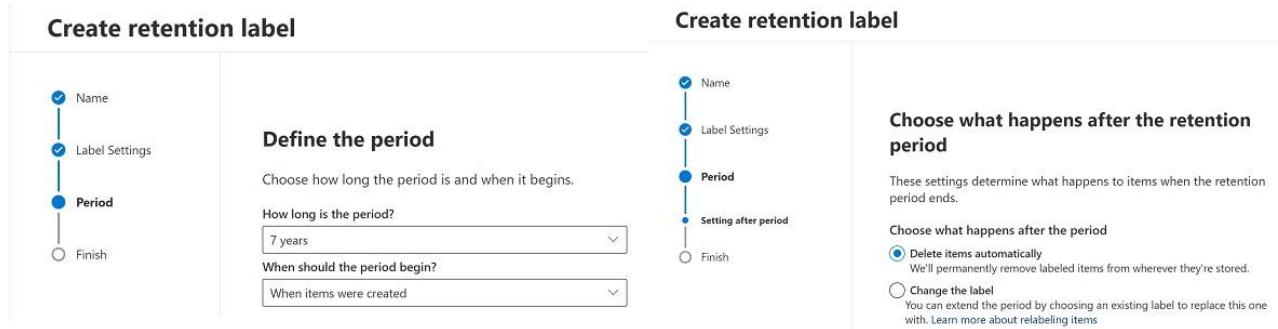


Figure 16-10: Defining retention periods and actions for a new label

Apart from deleting items after the retention period for a label ends, you can also choose to:

- Start a disposition review. When a disposition review happens, the item stays in place until a designated person reviews it to decide what to do with the item. See the later section for more information.
- Change the label. The settings for the newly applied label then control the item.
- Run a Power Automate flow. This option allows organizations to perform their own disposition processing for retained items. For instance, the flow could copy items to a new location for long term storage.
- Deactivate retention settings. The item remains in place and it's up to its owner to decide what to do with it.

The first two actions require Office 365 E5, Microsoft 365 E5, or Microsoft 365 E5 compliance licenses. This is also the case when the retention period of a label commences after an event occurs.

When all the details are complete for the new label, click **Next** to review the settings and then take the **Create label** option. Purview offers the chance to publish the new label to Microsoft 365 locations, auto-apply the label, or do nothing. The first two options create new publishing policies. Although ad-hoc publishing works in terms of bringing new labels into action quickly, we recommend that you take a more measured approach and publish or auto-apply new labels through planned policies.

One chance to get label settings right: Be careful with the settings you specify when creating a new label as you can only change the retention duration after a label is created. The logic is that allowing other changes after label creation will disrupt how the label behaves when applied to content. For example, if you change a label that keeps content for ten years and does not remove it afterward to now remove the items, users might lose information that they expect to have.

Making Retention Labels Available Through Label Publishing Policies

Retention label publishing policies make one or more retention labels available to end-users through a publication process to inform workloads about the labels and their settings. It is then up to the workload to decide how best to reveal the labels through its clients. Each label publishing policy makes one or more retention labels available to specified locations, such as Exchange Online or SharePoint Online.

To make new labels available to users, you must publish the labels through a label policy. You can publish a new label in a separate policy, but it's usually better to create policies to publish sets of labels to users. For instance, you might have a label policy called "Finance Department Labels" that includes all the labels needed by workflow processes in the finance department. The department users can apply the labels when an administrator publishes the policy to them.

A retention label can be in multiple label publishing policies. For instance, the "Confidential" label referred to above to keep content for five years could be in the policies assigned to different departments along with other labels that meet the specific needs of each department. The members of the legal department might have a policy that includes labels called "Case Review", "External Counsel", and so on while people working in Accounts might have labels for "Collections", "Audit Records", and "Tax." Being able to create label publishing policies with a mixture of generic labels and work-specific labels supports flexibility in data governance. After all, not everyone who works in an organization needs to deal with information in the same way.

Start the publication process by going to the **Labels policies** section under **Data lifecycle management (Microsoft 365)** to view the set of label policies defined in the tenant. You can then select an existing policy and edit it to add or remove labels from the policy or use the **Publish labels** or **Auto-apply a label** option to create a new label policy. The first type of policy makes the label available to workloads, the second sets the conditions for the automatic application of a label. You can select several labels and take the action to publish the set of selected labels in a single policy (bulk publish). A previous section covers Auto-application of labels.

After deciding on the set of labels to include, you decide on scoping (static or adaptive) and if the target locations are in the whole directory or limited by an administrative unit. If static, you select the locations to publish the labels to users. The options for static policies are:

- **All locations:** This means that the labels in the policy are available to all users in the following workloads. This is an org-wide policy.
 - **Exchange Online mailboxes.** Labels appear in clients in the same way as Exchange retention tags and behave like retention tags. For example, you can create a rule in Outlook desktop to apply a label to messages, such as all those that come from a specific address.
 - **SharePoint sites.** Users assign labels to classify individual documents or items inherit a label because it is the default for a document library. When a default label is defined for a document library, new Office and PDF files created or uploaded in the library inherit the label. The SharePoint sites location includes sites that are not connected to Microsoft 365 Groups.

- **OneDrive for Business accounts.** Users assign labels to classify individual documents stored in OneDrive folders.
- **Microsoft 365 Groups.** Users apply labels to conversation items in Outlook Groups. Viva Engage communities don't support the labeling of conversations. Because SharePoint supports retention labels, they can classify information in the document libraries belonging to Outlook Groups or Viva Engage communities. The Microsoft 365 Groups location includes the SharePoint Online sites owned by groups.
- **Let me choose specific locations:** For each of the supported workloads, you can opt to include or exclude certain mailboxes, sites, OneDrive for Business accounts, or groups. For mailboxes and groups, you enter the names of individual mailboxes or distribution lists you want to include or exclude. For site collections, you enter the URL in the form <https://mytenant.sharepoint.com/>. For OneDrive for Business accounts, enter the URL for the site. Figure 16-11 shows the target locations available for label publication.

Edit retention policy

Status	Location	Included	Excluded
On	Exchange mailboxes	All mailboxes Edit	None Edit
On	SharePoint classic and communication sites	All sites Edit	None Edit
On	OneDrive accounts	All user accounts Edit	None Edit
On	Microsoft 365 Group mailboxes & sites	All microsoft 365 groups Edit	None Edit

Choose where to publish labels

When published, users in your organization will be able to apply this label to items in the locations you choose.

(i) You can set up data connectors to import content from non-Microsoft apps like Slack, WhatsApp and many more, for use with this solution. [Set up now](#)

All locations. Includes content in Exchange email, Office 365 groups, OneDrive and SharePoint documents.
 Let me choose specific locations.

Back **Next** **Cancel**

Figure 16-11: Selecting locations to publish labels in a retention label policy

Scoping with Non Org-Wide Policies

Label policies with excluded or included locations are known as non-org wide policies. You can have up to 1,000 non-org wide policies in a tenant. This figure includes both retention and label policies.

When you exclude or include locations in a label policy, certain limits exist in the picker used to select target locations:

- For **Exchange**, if you don't enter anything in the search box, the picker shows the first 50 mailboxes and distribution lists in the directory. Enter a search phrase to find the mailboxes to include or exclude. The easiest way to add many mailboxes at one time to a policy is to use distribution lists. The membership of the list is expanded, and the mailboxes are added to the policy.
- For **SharePoint**, you can include or exclude up to 100 sites. These are sites, not libraries within sites. Use this location to publish labels to traditional SharePoint sites that are not connected to Groups.

- For **OneDrive for Business**, you can include or exclude up to 100 accounts by specifying the URLs for the target accounts.
- For **Microsoft 365 Groups**, the picker shows the first 100 groups in the tenant, including those hidden from Exchange clients (used by Teams). You can add up to 1,000 groups to a label policy. Labels published to Groups apply to the chosen group mailboxes and the group team sites. Use this location type to publish labels to modern team sites connected to Groups.

Workloads like Teams and Planner do not currently support retention labels, so there is no need to include them in the publication process. Teams does support retention policies.

Click **Next** after selecting all the target locations. You now name the policy and give some optional information to explain its purpose. Click **Next** to review the settings for the policy. If any issues are detected at this point (for instance, you enter a SharePoint site instead of a site collection), the policy cannot be published, and you must fix the problem before you can continue and save the policy.

When everything is ready, click **Publish labels** to begin the provisioning process that makes the policy available to the target locations. You know when the provisioning process is complete when the policy status changes from “Pending” to “Success.” Once published, the new label is available to the target workloads defined in the policy. This process can take up to one day to complete as, in some cases, clients must find out about the new labels. For example, the XML data used to inform Outlook desktop clients about retention policy settings must receive an update with details of the new label. The clients then need to download the label information before the new label appears in Outlook’s user interface. Web clients typically pick up new labels faster, but it is reasonable to expect that the entire end-to-end publication and provisioning process might take one or two days before a new or updated label is available throughout the tenant.

Comparing Retention Labels and Retention Policies

A retention policy (not a label publishing policy) applies a single retention setting to everything in a container or location (mailbox, site, group, or team). A retention label applies retention settings at the item level. Together, the combination of retention policies and retention labels gives administrators a lot of flexibility in planning a retention strategy for content. However, policies and labels support different settings, and this can be confusing at times.

Let’s summarize what retention labels and retention policies can do:

- You can apply retention actions and periods through both policies and labels. Some workloads (Teams and Viva Engage) apply the same settings to everything in the targeted containers. Others (Exchange, SharePoint, and OneDrive) support label assignment to individual items and targeted containers.
- A retention label can act purely as a visual marker. In this case, the label has no retention settings. Because it can add visual markings to documents and messages, a sensitivity label might be a better choice for this purpose.
- Both policies and labels support the ability to retain content for a set period, remove content after a set period, or retain for a period and then delete it. Both can use the created date or the last modified date as the date when the retention period begins.
- A retention label assigned explicitly to an item can override the retention period imposed by the policy assigned to a container. For instance, if a site has a retention policy that removes items after three years and an individual document in the site is assigned a retention label with a retention period of five years, SharePoint will remove all the unlabeled items on the site after three years and keep the labeled document for five years.
- After the retention period lapses, both policies and labels allow items to remain in place for the user to decide what to do with them. An analogy is government papers that have restricted access for ten

years after creation. When the ten-year period expires, the papers are not dumped. Instead, they become available for public access. This subtle differentiation is important for records management.

- Because they are more explicit, retention labels offer extra control over what happens when a retention period is over. A retention label can invoke manual disposition or use event-based retention. We'll get to these topics later.
- A retention label can classify an item as a formal record or regulatory record. Labels created for this purpose are managed through Records management – see later section.
- Labels assigned by auto-apply policies can be replaced by explicitly (user-assigned) labels. Explicitly-assigned labels can never be replaced by automatic assignments.
- Labels inherited from a container (like the default label for a SharePoint site) can be replaced by labels assigned by auto-apply policies.
- Unlike Exchange Online retention tags, neither retention policies nor retention labels support a "move to archive" action. If moving mailbox items to the archive is important, you can continue to use mailbox retention policies in conjunction with retention policies.

Figure 16-12 shows the retention settings for a retention policy (right) and retention label (left). These are old UI screens (2021), but they show the extra flexibility available in retention labels better than the current GUI. The ability to set a label to mark items as records (label classification) is only available when editing retention labels through the File Plan section of Record Management in the Microsoft Purview Compliance portal.

Define retention settings

When this label is applied to items, the content is retained and/or deleted based on the settings you choose here.

Retain items for a specific period
Labeled items will be retained for the period you choose. During the retention period, Users will be able to edit items and change or remove the label. If they delete items, we'll keep copies in a secure location. Learn more

Retention period of years months days

Start the retention period based on

+ Create new event type

At the end of the retention period
 Delete items automatically
 Trigger a disposition review
 Do nothing
Items will be left in place. You'll have to manually delete them if you want them gone.

Retain items forever
Labeled items will be retained forever, even if users delete them. Users will be able to edit items and change or remove the label. If they delete items, we'll keep copies in a secure location. Learn more

Only delete items when they reach a certain age
Labeled items won't be retained, but when they reach the age you choose, we'll delete them from where they're stored.

Decide if you want to retain content, delete it, or both

Retain items for a specific period
Items will be retained for the period you choose.

Retain items for a specific period of years months days

Start the retention period based on

At the end of the retention period
 Delete items automatically
 Do nothing
 Retain items forever
Items will be retained forever, even if users delete them.

Only delete items when they reach a certain age
Items won't be retained, but when they reach the age you choose, we'll delete them from where they're stored.

Policy

Label

Figure 16-12: Retention settings in a retention policy (right) and retention label (left)

In summary, retention labels offer more flexibility, but they must be assigned manually or through auto-label policies. The retention settings in policies are simpler, but they are easier to apply because you can deploy retention across the entire organization or for a selected set of locations with just a few policies.

Using Retention Labels

We now know how to set up, publish, and manage labels and understand the basic principles that only one label can exist on an item at any time, whether a user assigns the label to an item manually or a background process assigns the label automatically. With those thoughts in mind, we can now go ahead to discuss how to use labels within the different locations.

Using Retention Labels with Exchange Online

Exchange Online processes both old (legacy) Exchange mailbox retention policies and Microsoft 365 retention policies. To make everything work together, the Managed Folder Assistant (MFA) integrates the retention settings from Exchange Online and Microsoft 365 so that retention policies, retention labels, and Exchange retention tags work together.

Publication of a new retention label means that workload-specific mechanisms make the label available to users of an application. For Exchange Online, that mechanism is to insert the label into the set of retention tags available to a mailbox. MFA creates a unified set of retention tags and retention labels and publishes the set to user and group mailboxes (group mailboxes only see retention labels and not retention tags). MFA includes only labels with a retention action in its published set.

MFA operates a workcycle to process mailboxes at least once every seven days. Therefore, it might take up to a week before new retention labels become available to mailboxes. See the “Logging the Managed Folder Assistant” section later to understand how to extract and interpret MFA diagnostic logs for a mailbox to know when MFA last processed the mailbox.

Mailboxes must hold more than 10 MB of content before the MFA processes the mailbox to make retention labels available. This restriction exists to ensure that MFA does not waste processing cycles on unused mailboxes. When it opens a mailbox for processing, MFA makes sure that the current set of labels is known to the mailbox before it begins to check items against their retention status.

Integrating retention labels with retention tags allows OWA and Outlook desktop to handle the two kinds of tags consistently. In effect, OWA and Outlook treat labels in the same way as personal retention tags and make the labels available to users to tag individual messages or folders. Figure 16-13 shows how Outlook presents a mixture of retention tags and retention labels to the user when they want to apply a policy to a folder.

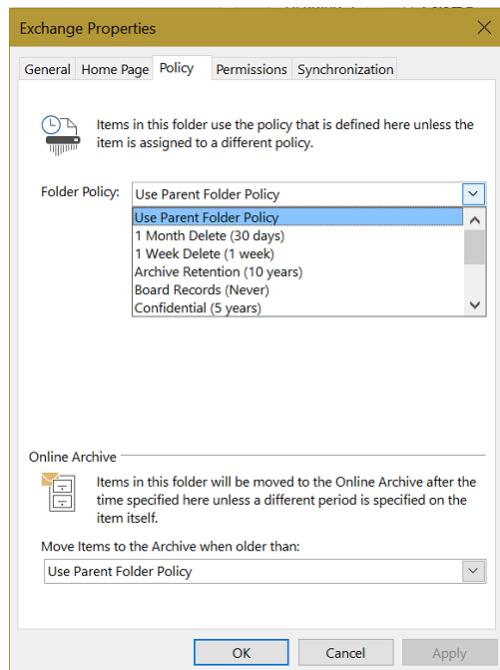


Figure 16-13: Outlook lists retention tags and labels

Because Outlook clients display retention labels alongside personal retention tags, users should not see any difference between the two types. If a user assigns a label to a folder, all items in the folder inherit that label, unless the item already has a personal tag or another retention label. Likewise, if you change a label at the

folder level, the next time MFA processes the mailbox, it updates the items in the folder with the new label unless they already have an explicit label or tag.

Because Exchange public folders do not support retention policies, they also do not support retention labels.

Integration with Exchange Retention Policies

Although OWA and Outlook present retention labels to users in the same way as they see personal retention tags from mailbox retention policies, we already know that labels function differently from retention tags.

Table 16-4 lists some of the differences between the two methods used to mark mailbox items for retention processing.

Feature	Mailbox Retention Tag	Retention Label
Remove content from mailboxes	Yes, when the retention period expires.	Yes, when the retention period expires.
Archive content from mailboxes	Yes, when the retention period expires.	No. Labels do not support an archival action.
Expiration of control	No. A retention tag stays with an item until it is removed from the mailbox.	Yes. The effect of a label ceases when it expires.
Policy-driven tagging of default folders	Yes. Retention policies can include folder tags for any of the Exchange default folders (like Inbox).	No. A retention label functions as a personal retention tag and can be applied to any other folder except default folders.
User-driven tagging of items and folders	Yes. Retention policies can include personal tags for users to stamp on non-default folders and individual items.	Yes. A label can be used in the same way as a personal tag to mark items or folders.
Policy-driven default retention	Yes. Retention policies can include default tags that apply to all items in the mailbox that are not stamped with a more explicit tag. A policy can include default tags to define removal and archival actions and you can have a specific default tag for voicemail.	No. It is possible to create an auto-label policy that applies to all items in the mailbox, but that is different from a default tag.
User-selectable tags	Yes. Users can select personal tags (through OWA options) that are not in the assigned retention policy and use them to tag items and folders.	No. Users do not have access to labels not published to their mailbox.
Target	Limited to Exchange mailbox folders, items within a conversation, individual items, or complete mailboxes.	As for retention tags, with the addition that labels can be used in other workloads.

Table 16-4: Differences between Exchange retention tags and retention labels

The last point is the most important. Retention policies and tags only cover Exchange content. OWA and Outlook desktop clients combine retention labels with the tags published through Exchange mailbox policies. Meaning users can apply labels to email items in the same way as they use retention tags. Of course, the big difference between labels and tags is that labels are available in other workloads.

Using Retention Labels with Groups

When you publish retention labels to a group, they become available in both the group mailbox and the group document library. At the time of writing, OWA is the only client that supports the application of labels to conversations in Groups. Only group owners can use labels to classify conversations as OWA hides the labels from ordinary group members.

However, all group members can assign retention labels to files and folders in the group document library and any group member can overwrite a label previously assigned by another group member, except if that label is a formal record (in which case only the site collection administrator can update the item). The reasons why labels behave differently in a group's mailbox and document library are because of the different ways that Exchange retention tags and SharePoint permissions work. An Exchange mailbox is typically under the sole control of its owner while a SharePoint site is designed to support multiple levels of shared access.

Using Retention Labels with SharePoint and OneDrive for Business

Any user in the default members group for a SharePoint site (with the Contribute permission level) can apply labels to documents, folders, or items in a list within the site. If the site belongs to a group, any of the members can apply labels because they all have equal access to the site. The owner of a OneDrive for Business account can apply labels to content within their account. When you apply a retention label to a folder, all items in the folder inherit the same label, unless some of the items in the folder already have labels. Applying a retention label to a folder holding thousands of files can take a little time to complete. A retention label inherited from a folder stays with a document even when the document moves to another folder or another site. Also, if you upload a file to replace an existing document that has a retention label, the uploaded file inherits that label.

To apply a label to an item in OneDrive for Business or SharePoint, select the document or folder and then open the Details pane. Go to the **Apply Label** section and select a label from the set published to the location. This method also works when accessing the details of SharePoint files through the Teams Files channel tab. Placing a label with a retention action on an item has some consequences:

- Depending on the Retention labels settings (available in the Records management section of the Microsoft Purview Compliance portal), users might be unable to remove a labeled item. See the section covering Record management settings.
- Users cannot edit documents marked with a label that classifies items as a formal record. They can update documents marked with labels not classified as formal records. Site administrators can remove the label or replace it with another if users need to edit the item.
- SharePoint records updates and deletions for documents in the site's Preservation Hold library.
- If a document is subject to a retention policy, users can remove it from the library, but because the document comes within the scope of a retention policy, SharePoint must keep a copy. In these instances, SharePoint Online moves the deleted document into the Preservation Hold library and keeps it there until the retention period expires.

The behavior is different for files held in OneDrive for Business because these sites are personal rather than shared and the owner of the site has the right to remove files from the site. When a user removes a file from their OneDrive for Business site, the file goes into the site recycle bin. Thereafter, when the retention period

for the recycle bin expires (93 days), a timer job examines expired items and moves copies of any item with a label into the site's Preservation Hold library.

A label is a managed property that SharePoint indexes along with other document attributes. Indexing occurs when the crawler accesses new or updated documents. It can take up to an hour before a newly-assigned label is in the index. When indexed, you can search for documents tagged with a retention label by using the *compliancetag* property. For example, you can input *compliancetag:"GDPR Personal Data"* in the SharePoint search box or a content search to find documents stamped with the *GDPR Personal Data* label.

Displaying Retention Labels Used in a Document Library

The Outlook clients include the necessary user interface to make retention tags available to users, including those published by retention policies. This is valuable because users get a clear visual understanding about how long Exchange will keep an item. Retention labels are not one of the default fields shown for SharePoint document libraries or lists. You can make the labels more obvious by customizing the view of items in the library or list to include the "Labels" and (if necessary), "Item is a record" fields. Figure 16-14 shows how information about assigned labels appears in a document library. Note that the column only displays the label name and doesn't show anything else such as the outstanding retention period. This points to the need to either include the retention period in label names or to coach users about what each retention label does.

Name	Modified	Published	Published Date	Publication	Labels	Item is a Record
Office 365 Data Governance.docx	7 hours ago	No		Petri	Formal Company Record	Yes
Bringing Compliance to Office 365 Groups.docx	Yesterday at 9:03 AM	No		Petri		No
Outlook Enhancements Continue to Disappoint On-Premises Users.docx	Yesterday at 8:40 AM	Yes	4/20/2017	Petri	Confidential	No
Turning Office 365 Off at the Weekend.docx	Yesterday at 8:40 AM	Yes	4/18/2017	Petri	Confidential	No
Office 365 New Retention Strategy.docx	Yesterday at 8:40 AM	Yes	4/11/2017	Petri	Confidential	No
Microsoft Q3 FY17 numbers and Office 365.docx	Monday at 2:30 PM	No				No
Planner Moves Forward.docx	6 days ago	Yes	4/6/2017	Petri	Confidential	No
Office 365 Adoption Content Pack is a Step in the Right Direction.docx	March 29	Yes	3/23/2017	Petri	Confidential	No
An Archive to Rule Them All.docx	March 29	Yes	3/28/2017	Petri	Confidential	No
Recovery for Office 365 Groups.docx	March 29	Yes	3/30/2017	Petri	Confidential	No
Looking forward to Engage.docx	March 27	No			Confidential	

Figure 16-14: Viewing label information in a SharePoint document library

Unlike when you update properties like a document's name or title, SharePoint does not treat applying a label as a modification. Instead, it is more of an administrative event. SharePoint, therefore, does not update the "Modified By" property with the name of the person who applies the label.

An organization might have many retention labels in active use at any time. It can be confusing for users to have to choose between multiple labels when they classify documents. In addition, some labels might be inappropriate for the content of certain sites. With these points in mind, it is sensible to consider what sites should receive a label when you publish it. Some labels are general purpose and are useful across all sites while others are better if restricted to specific sites.

Finding Items Marked with Labels in Content Searches

You can create content searches (either standalone or part of an eDiscovery case) to find content marked with specific labels. You do this by using the "ComplianceTag" keyword in searches. For example, this search finds any items stamped with the "Draft" or "Approved" labels.

(*ComplianceTag:Draft*) OR (*ComplianceTag:Approved*)

If the label name contains spaces, enclose the name in quotation marks. See the eDiscovery chapter for more information about eDiscovery searches.

Audit Records Generated for Retention Label Actions

When someone assigns, changes, or removes a retention label from a document or folder in a SharePoint Online or OneDrive for Business library or an item in a list (including a list created in the Lists app), a *ComplianceSettingChanged* audit record captures the event.

- For retention labels applied by a user or retention labels assigned because a default label exists for a document library, the *UserIds* property holds the user principal name of the account that executed the action.
- For retention labels applied by the background job for auto-label policies, the *UserIds* property holds the GUID of the background job. You will see a value like *1b1c17be-a6f8-4691-9fca-9b6ac128c9e1*.
- SharePoint Online does not generate audit events for retention labels inherited by new documents because a site has a default label. This is an acknowledged gap in Microsoft's compliance story.

If a user removes a retention label from a document or list item, SharePoint Online captures the *TagUnApplied* audit event.

Audit records captured for retention label actions in a library include the site, the document name, the user, and the name of the label. If a label previously existed for a document, the audit record captures both the original (*SourceLabel*) and new (*DestinationLabel*) classifications. For label actions involving list items, SharePoint Online writes the item number into the audit event, so you see values like:

https://office365itpros.sharepoint.com/sites/GDPRPlanningMarkII/Lists/Things%20to%20do/2_000/2

Exchange Online does not capture audit events when messages receive retention labels. This is because Exchange treats retention labels in the same way as mailbox retention tags. Exchange does not capture the assignment of mailbox retention tags as mailbox audit events.

Analyzing Retention Policy Updates

Retention policies exercise control over user information, so it's wise to keep an eye on changes made to policy settings to ensure that administrators don't make mistakes that result in inadvertent loss of data. Microsoft 365 captures audit records for additions, updates, and removals of retention policies and retention label policies. [This article](#) explains how to analyze audit events for retention policy changes to report change details. The situation is more complicated than it first appears due to the information captured in audit events for different types of retention policies.

Default Assignment of Retention Labels

If you have Office 365 E5 or Microsoft 365 E5 licenses, one solution is to classify items by using an automatic label policy to find documents using searches based on keywords or sensitive information types. This is a good way to make sure that documents with certain characteristics (like HR personnel files) are classified no matter where they are stored within SharePoint.

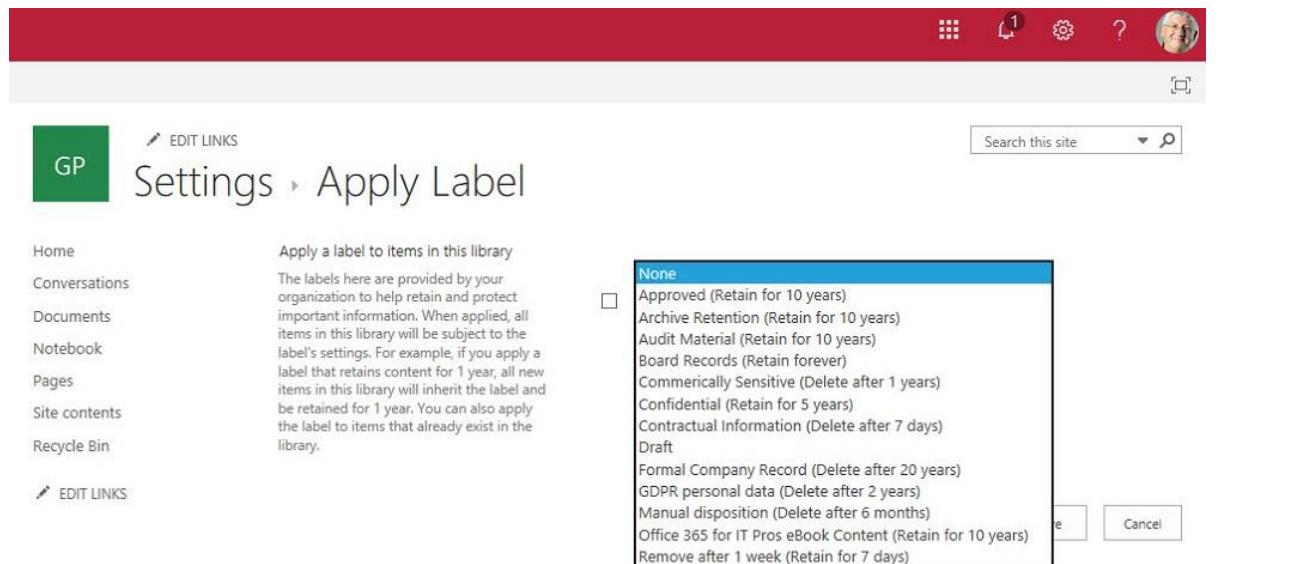


Figure 16-15: Applying a default retention label to a SharePoint library

Another method to ensure that all items in a SharePoint or OneDrive for Business list or library are assigned a retention label is to assign a default label. Microsoft considers this to be an advanced feature, so defining a default label for a document library requires an Office E5 license. Interestingly, defining a default label for documents in a sensitivity label policy only requires Office 365 E3.

To assign a default retention label, go to the settings for a library and select **Apply label to items in this list or library**, and then choose the default label from the set of available retention labels (Figure 16-15). In addition to assigning a default label to new items, you can choose to have SharePoint or OneDrive for Business apply the selected label to existing items. If you need to add default retention labels to multiple libraries, it's possible to [use PowerShell to script the assignment of a default label](#) to a SharePoint library.

OneDrive for Business Library Settings: If you want to set a default retention label for a OneDrive for Business account, you must either enter the URL for the library settings (it's the *settings.aspx* page) or use the old-style interface. Library settings are available when you expose the ribbon, select the library tab, and then library settings. You can then select a retention label as described for SharePoint above.

Applying Retention Based on Sensitivity Labels

Given that files with sensitivity labels often hold confidential information that the organization wishes to keep (or wants to remove after a set period), it makes sense to use auto-label policies to find documents with certain sensitivity labels to make sure that they have appropriate retention labels. In this example, we'll create an auto-label retention policy to assign a retention label to documents and messages protected by the Highly Confidential sensitivity label. To do this, you:

- Connect to the compliance endpoint with PowerShell by running the *Connect-IPPSSession* cmdlet.
- Find the unique identifier (GUID) for the selected sensitivity label by running the *Get-Label* cmdlet.
The *ImmutableId* property contains the GUID.

```
Get-Label | Where-Object {$_ . DisplayName -eq "Highly Confidential"} | Select-Object -ExpandProperty ImmutableId
```

```
Guid
```

```
----
```

```
9ec4cb17-1374-4016-a356-25a7de5e411d
```

- Use SharePoint search to test the KeyQL query for the auto-label policy. The search term is in the form *InformationProtectionLabelId:9ec4cb17-1374-4016-a356-25a7de5e411d* where the managed SharePoint property that holds the GUIDs of sensitivity labels (*InformationProtectionLabelId*) is combined with the GUID identifying the sensitivity label you want to search for. Run the search and open one of the documents returned by the search to check that it has the correct sensitivity label. If no documents are found, it might indicate that the GUID is incorrect or that your account has access to no documents that have this sensitivity label.
- If the search term finds the correct documents, create an auto-label retention policy that uses the same search term as the content query to find the target documents and apply a suitable retention label to keep the documents for the desired period.
- Configure the policy to find documents in the desired target locations. Remember to use Microsoft 365 Groups to cover SharePoint sites owned by groups and teams. Publish the policy when everything is complete.
- After ten days or so, check that documents with the sensitivity label have the correct retention label, remembering that if a user assigns a retention label to a document, an auto-label policy won't replace it.

The ten days mentioned above are an estimate rather than a guarantee. It can take SharePoint Online anything from seven days to two weeks for a new auto-label retention policy to become operational and start to apply retention labels.

Finding Unlabeled Files: Over time, it's possible that some files will remain unlabeled, even if you use auto-label policies and apply retention labels by default when users add them to document libraries. In this situation, you can use Microsoft Search to find unlabeled files (see [this article for an explanation](#)). Once you know what files are unlabeled, you can figure out the best method to label them.

Auto-Label Retention Policies

Publishing labels for people to apply to documents and messages is certainly one way to solve the need for data governance. The problem with this approach is that it depends on human beings to be very precise, consistent, and persistent in how they classify material. As noted in this book, we know that humans are very inventive, but they also tend to lose interest in boring technicalities after a while. On the other hand, computer systems are all about processing the same steps time after time until told to stop. Auto-label policies help organizations meet their data governance needs by finding content to retain and applying the right label to that content. Auto-label policies work alongside standard label policies. People apply the labels published to their accounts to explicitly label important or specific items while most items that need labels receive them automatically. Auto-label policies require Office 365 E5 or Microsoft 365 E5 compliance licenses for any account coming within the scope of the policies.

Take the "Business Critical" label for example. We know that we want users to use the label to classify any content that the organization needs to keep for audit purposes. We have reasonable confidence that people will classify new documents and messages, but tens of thousands of pertinent documents exist in SharePoint Online and OneDrive for Business that the business should retain. If we can build rules to tell Microsoft 365 how to find the content, an auto-label policy is the right tool for this job.

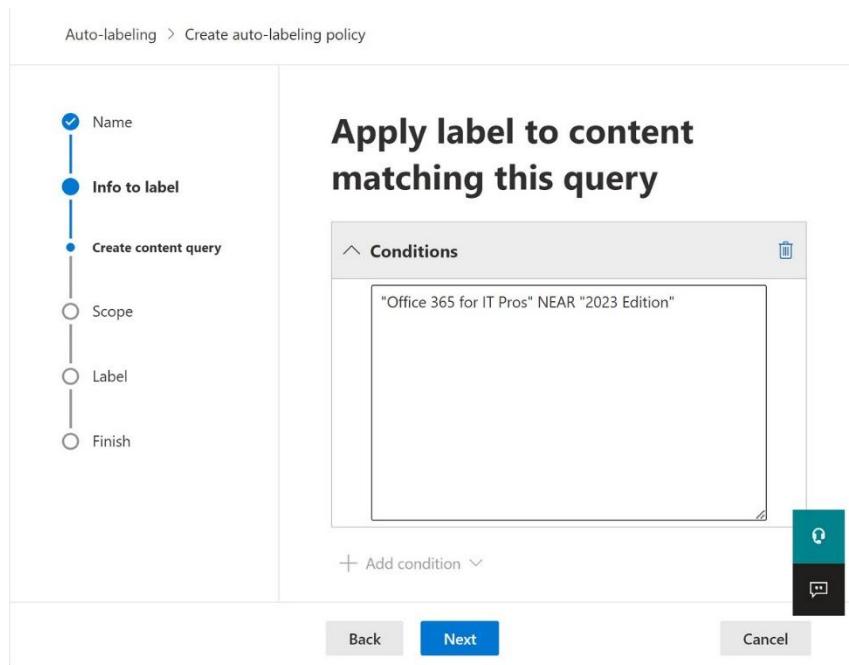


Figure 16-16: Using keyword queries to find content to keep through a retention policy

Auto-label policies use conditions to find matching items in the locations covered by the policy and assign a retention label to those items. For instance, you might want to use an auto-label policy to protect items identified with matching criteria. Among the options exist to find content for an auto-label policy are:

- **Sensitive Information:** Find items containing sensitive information types such as credit cards, bank account numbers, taxpayer identification numbers, and social security numbers. Any sensitive information type known within a tenant is usable, including custom types defined by the tenant or created using digital fingerprinting.
- **Content (KeyQL) Queries:** Find items using a content query containing keywords or search terms. Good examples of this kind of policy inaction are those used to [find and label Teams meeting recordings](#) and [apply retention labels to documents marked with sensitivity labels](#). Like content searches, the query is expressed in KeyQL syntax (this [page is helpful](#) to understand how to construct KeyQL queries). A good way of testing a query before using it in an auto-label policy is to use it with SharePoint search or a content search. Either way, by checking the items returned by the search, you'll know if the content query finds the correct items for the auto-label policy. See the eDiscovery chapter for more information about running content searches.
- **Trainable classifier:** Find items matching a classifier created by Microsoft or created by the tenant. Auto-label policies that use trainable classifiers can't process content that's more than six months old.
- **Cloud attachments and links** shared in email, Teams, Copilot, and Viva Engage (Yammer): Cloud attachments and sharing links are mechanisms to allow users to share files while leaving the files in their original repositories. If you opt to apply labels to a file shared in these ways, Microsoft 365 automatically creates a copy of the file and applies the label to it without the user being aware of this action. The policy applies only to files stored in SharePoint Online and OneDrive for Business.

To create a new auto-label policy, go to Label policies and then select auto-apply a label. After naming the new policy, you select the kind of criteria to match items against. In Figure 16-16, we see a simple query to look for one phrase close to another. You can specify as many keywords as necessary to create the best chance of matching items for retention using the same approach as for eDiscovery searches.

Content queries can filter out certain kinds of files for retention processing. For example, let's assume that you only want to assign retention labels to Word documents and PowerPoint presentations stored on specific sites. The keyword query to find documents of these types must include a reference to their file extensions.

Some search experts recommend adding a term to have SharePoint Online only search items it considers documents (*isDocument* is true). However, an argument also exists that it's sufficient to pass the desired file extensions. This content query uses both file extensions and an explicit term to limit the search to documents:

```
filetype:doc* filetype:ppt* isDocument:1
```

If you change a policy to update the keywords used in the content query, the target locations evaluate the updated content query to decide whether to keep or remove content.

Microsoft 365 publishes auto-label policies to the target workloads in a similar manner to label publishing policies. Auto-label policies work against data at rest for both SharePoint and Exchange locations. Policies detect matches against conditions when the indexer processes items, leading to the assignment of labels to matched items. When an Exchange mailbox comes within the scope of an auto-label policy, the locations include both the primary and archive mailboxes.

Figure 16-17 shows how to include a sensitive information type in a retention policy. When you choose to use sensitive information types, you select a template like the way you create a new DLP policy. In this case, we chose the U.S. Financial Data template, which imports three sensitive information types into the policy. You don't have to use all the imported sensitive information types and can remove those that aren't necessary.

When using a trainable classifier to find items to apply labels to, you can use the set of classifiers created and published by Microsoft or build a tenant-specific classifier. Classifiers are "trainable" because their creation involves a training process where artificial intelligence technology processes sets of sample documents to recognize their essential characteristics and create the classifier. In this instance, the *Customer Billing* trainable classifier is constructed by analyzing a set of 400 customer invoices. When the auto-label policy is active, each time the indexer meets a matching document (one with the same characters as learned from the sample set), Microsoft 365 applies the label to the matched item.

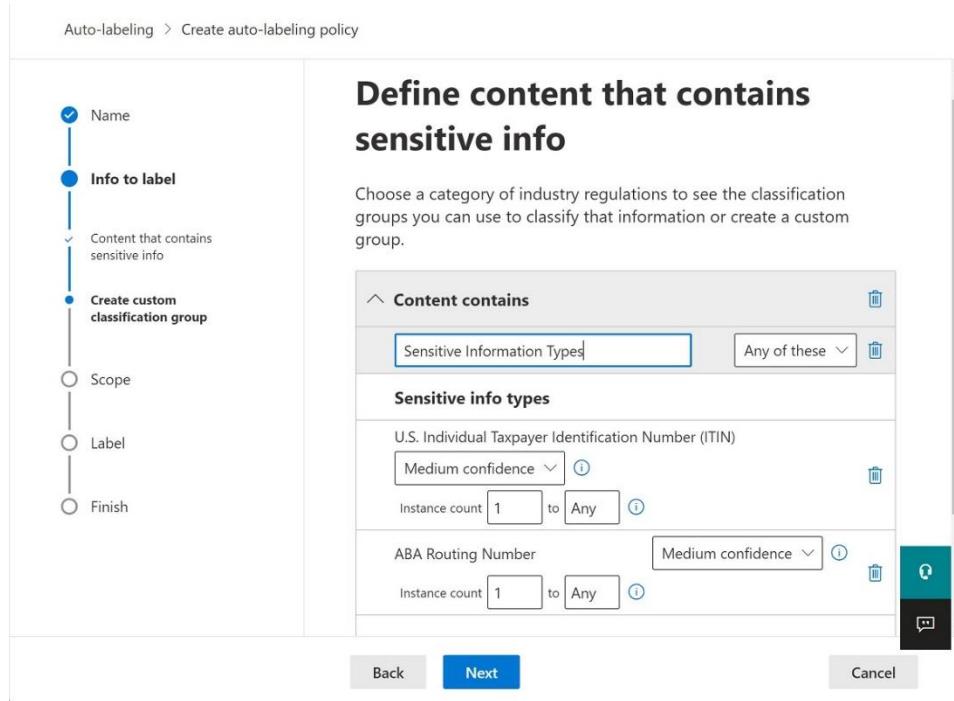


Figure 16-17: Using sensitive information types in a retention policy

After choosing the criteria to find matching items, you select an adaptive scope or select static target locations from:

- Exchange mailboxes. Note that when using sensitive data as the criterion for auto-labeling, the policy applies to all mailboxes. You cannot include or exclude individual mailboxes.

- SharePoint sites.
- OneDrive for Business accounts.
- Microsoft 365 Groups. These locations include the group-connected SharePoint Online sites, including those used by Teams. When using sensitive data, you cannot include or exclude individual groups. Also, you must include Exchange mailboxes in the policy to ensure that the policy processes the complete content for the groups.

Finally, you choose the retention label to apply. After a last check of the policy settings, submit the policy for publication to the target workloads. The Compliance portal validates the settings and if everything is OK, go ahead and publish.

Auto-applying labels are an effective way to achieve broad coverage of content that a query can find using a keyword or because the content holds some sensitive data. Later, users can review items with the label and decide whether the label is correct, or if another label is a better fit. Unlike other labels, the labels included in auto-apply policies do not show up in SharePoint, OneDrive, or Exchange as labels that users can apply manually.

Validating the Progress of Auto-Labeling

It can take up to a week before an auto-label policy becomes fully effective. Unfortunately, there's no easy way to measure the effectiveness of auto-labeling without some degree of manual checking. You can:

- Check the properties of individual items that you expect to receive labels to see if the auto-label policy has assigned a label to those items.
- Use the Activity explorer in the compliance portal to see what items have received the label applied by an auto-label policy.
- Analyze the *TagApplied* events from the audit log to track the application of the label applied by an auto-label policy. An example [script in the Office 365 for IT Pros GitHub repository](#) shows how to approach the task.

If you deploy several auto-label policies, documents can end up with labels that you think are incorrect. Apart from using bad search queries to find the items, the problem might be because more than one policy applies to documents. When this happens, the oldest policy (by creation date) wins and once a policy applies a label to an item, other policies will ignore that item because it already has a label. Because auto-labeling works in this manner, you need to be careful with the queries used to find content and with the order in which you deploy policies.

Auto-labeling of Cloudy Attachments

A “cloudy attachment” is the term used when people send a link to a file stored in SharePoint Online or OneDrive for Business instead of a separate copy of a file to each recipient. Cloudy attachments are supported for messages generated by Outlook, Teams, or Viva Engage. The idea is that recipients interact with the original content stored in SharePoint or OneDrive rather than making changes to their personal copies and then attempting to reconcile individual updates. Cloudy attachments can also result in the output generated through interactions with Microsoft 365 Copilot.

The results for Purview eDiscovery standard cases and content searches include cloudy attachment links inserted into message bodies. However, they do not include the actual content of the linked file. eDiscovery investigators can follow links to retrieve attachment contents, but this becomes an onerous task when search results include many messages containing attachment links.

An auto-labeling policy created with the content condition “*apply labels to cloud attachments and links shared in Exchange, Teams, Viva Engage and Copilot*” solves the problem by capturing copies of files shared through messaging. After creating the auto-label policy, it takes some time to become effective because it must be

deployed to all the sites covered by the policy. This process can take up to a week, depending on the number of sites to cover.

When the auto-label policy is active, a background job monitors cloudy attachments sent in messages. When it detects a cloudy attachment covered by the policy, the job captures a copy of the attachment and stores it in the *SharedVersions* folder of the Preservation Hold library of the host SharePoint Online site or OneDrive account. Because the background job works on a timer, captured files do not appear for up to an hour after cloudy attachments are sent. When it captures a file, the background job stamps it with the retention label defined in the policy. The names of the captured files are obfuscated. To see the name of the original attachment, use the version history option to retrieve its details. The compliance details option reveals the retention label assigned to the file.

Because they have no access to the Preservation Hold library, users who send messages with cloudy attachments are unaware that the captured copies have retention labels. If someone modifies the file after sharing, a new version is captured in the Preservation Hold library. The retention label applied by the policy does not have to be published to users or locations. In fact, it's probably a good idea to create a retention label reserved for use with cloudy attachment auto-labeling policies. To avoid problems with attachments that are shared multiple times, Microsoft recommends that the retention label chosen for the auto-label policy begins its retention period from the time when the policy applies the label to the copy of the shared attachment.

Unlike other auto-labeling policies which process data at rest to apply retention labels to content that already exists, auto-labeling of cloudy attachments is not retrospective. The only attachments that are captured and retained are those sent once the policy is in force.

Copies of cloudy attachments labelled by auto-label policies remain in the Preservation Hold library until their retention period lapses. At that time, the normal method of processing the retention action occurs.

Depending on how many cloudy attachments an organization generates, the preservation of captured copies might have a significant impact on the [consumption of SharePoint Online storage](#). To ensure that the current version of the original shared file is preserved, any files moved or deleted in the locations within the scope of the auto-label policy are automatically copied to the Preservation Hold library. These are temporary copies kept for one day to allow auto-label processing to happen and then removed. This form of temporary retention is unique to files within the scope of auto-labeling policies for cloudy attachments and is a simple safeguard to preserve all the copies of these files that might be needed for eDiscovery.

The existence of captured attachments means that it is possible to retrieve copies of the attachments during eDiscovery operations. Purview eDiscovery premium cases leverage this capability to allow investigators see content either at the time when it was shared or its current state.

Replacing Retention Labels Assigned by Auto-Label Policies

Auto-label policies are an effective way of applying retention labels to large quantities of items. Microsoft 365 ignores matching items in the target locations if they already have retention labels assigned manually by users (explicit assignment) or an auto-label policy. Auto-label policies ignore items that already have retention labels to avoid the potential that overwriting the existing label with another might cause data loss. The situation is different for policies that automatically apply sensitivity labels because these policies can replace existing labels, but only when the sensitivity label applied by the policy has a higher priority (higher sensitivity level) than the existing label. Retention labels don't have priority levels, so the same approach cannot be used for automatic application of retention labels to content.

Good as this logic is, it does create a problem if an organization's retention strategy changes. You can update a retention label to change its retention period, but you cannot change its retention action. For instance, if a label's retention action is to delete items when the retention period expires, you can't change the action to

leave items in place. Microsoft is aware that this lack of flexibility can cause problems for organizations forced to change their retention strategy due to government or other regulations. In the future, you might be able to alter an auto-label policy to instruct it to replace one label with another but for now, you should remember that once you apply retention labels through policy, those labels will stay assigned to items unless replaced by a label explicitly assigned by a user. If you want to change a retention label through automatic assignment, you must remove the existing label first.

Other Methods to Automatically Assign Retention Labels

Although auto-label retention policies are a good way to find and label items automatically, several other methods exist to apply retention labels to content. These include applying labels by:

- Defining a default retention label for a SharePoint Online or OneDrive for Business document library. This method requires Office 365 E5 or Microsoft 365 Compliance E5 licenses.
- Using Power Automate to assign a label to a document (here's [an example](#)).
- Applying a retention label to a Microsoft Syntex document understanding model.
- Programmatically using the [SetComplianceTag method](#).

Automatic assignment of retention labels usually requires a specific license. For example, if you define a default retention label for a document library, users accessing that library need Office 365 E5 or Microsoft 365 Compliance licenses.

Records Management

Microsoft Purview Records management is a solution managed through the section of the same name in the Microsoft Purview Compliance portal. Records management makes management of retention labels and policies easier in large organizations and includes these features:

- **File plan:** Enterprises typically use more retention labels than smaller organizations and often have retention labels created for specific purposes. A file plan gives extra flexibility in grouping and managing retention labels based on different properties, such as labels used for manual disposition. Administrators can assign a set of file plan descriptors to retention labels, such as the *authority* for the label (the intended business category requiring the use of the retention label – default values are business, legal, or regulatory). In addition, the file plan allows tenants to mark retention labels as formal company records and regulatory records.
- **Retention label policies:** The same functionality is available to create and publish labels as exists under Data lifecycle management.
- **Events:** Create the events used for event-driven disposition, such as the termination of a project.
- **Disposition:** Process items that have reached the end of their retention period and require a manual check to decide what should happen to the item (deletion, further retention, and so on).

These features all require Office 365 E5 or Microsoft 365 Compliance E5 licenses.

Records Management Settings

Three important controls for retention labels are in the Settings section of Records management:

- **Deleting content labeled for retention:** SharePoint Online used to block users from deleting labeled items while OneDrive for Business allowed them to do so. To achieve consistency across the two applications, Microsoft changed SharePoint Online to behave like OneDrive for Business, meaning that users can delete labeled items and SharePoint Online will store the items in the site's preservation hold library until their retention period expires. Some organizations prefer the previous behavior because they believe that users should not remove labeled items. If this option is set, users see an error if they attempt to remove a labeled item. To proceed, a site administrator or user with

permission must remove the label to allow deletion to happen or replace the label with one that does not have a delete action.

- **Configure record versioning:** By default, record versioning is on, meaning that users can unlock items with an assigned record label and edit their content. If off, items assigned a record label remain locked and updates are not possible after the creation of these items. In effect, record labels then act like regulatory record labels.
- **Allow editing of record properties:** Apart from its content, an item has metadata like its title and other attributes. By default, users can edit items assigned a record label to update metadata. If this control is off, users cannot update item metadata after creation.

Although the Records management solution requires Office 365 E5 or Microsoft 365 Compliance licenses, administrators can set these controls without those licenses. The controls apply to all sites in a tenant.

Record Labels

Retention policies and labels play a key role in the ability of Microsoft 365 to meet the requirements of Rule 17A-4 of the U.S. Security and Exchange Commission (SEC), stating that companies that employ brokers, dealers, and other workers in the financial industry must keep records of their electronic communications for between three and six years, depending on the type of communication. Among the requirements set out are that the records should not be amendable or erasable by an administrator.

Microsoft 365 supports two forms of record retention labels to help organizations satisfy regulatory requirements. Unlike regular retention labels, you cannot create or edit record labels through the Data lifecycle management section of the Microsoft Purview Compliance portal. Instead, these special forms of retention labels are managed in Records management. The two types of record label are:

- **Record:** After a user applies a record label to an item, only administrators can remove the label or change it for another label. Anyone with write access to an Exchange mailbox can apply a record label to an item in the mailbox. Any member of a SharePoint Online site can apply a record or regulatory label to a file or list item. Once applied, a record label stops any attempt to delete the item (if they attempt to delete a record, users are told that the operation is disabled by policy). Items with record labels stored in SharePoint Online and OneDrive for Business can have a locked or unlocked status. Users cannot update the content of a locked item, but they can update its metadata (like the title) subject to the tenant Record management settings for updating items marked as records. Any site member can unlock an item to permit editing. In addition, once an item receives a locked record label, it can only move within its host container (site, account, or mailbox). Users cannot move these items to another container. You can create record labels in an unlocked state to allow users to work with labeled items. Once the record is complete, a user can lock the item.
- **Regulatory record:** This is a stricter form of record label. Not even a tenant administrator can remove a regulatory record label after its creation, and the only changes allowed to the label settings are an increase in the retention period or publishing the label to additional locations. After applying a regulatory record label to an item, no one can remove the label or delete the item until its retention period expires. Site administrators cannot change the locked status of an item, so no one can edit an item's content. However, users can open documents in review mode and save their content as a new file.

Not every organization needs to implement the strict retention regime implied by regulatory records. For this reason, before you can create new regulatory record labels, you must expose the UI to allow the compliance portal to manage regulatory record labels. Do this by connecting a PowerShell session to the compliance endpoint and running the *Set-RegulatoryComplianceUI* cmdlet.

```
Set-RegulatoryComplianceUI -Enabled $True
```

The command is effective immediately. To disable the UI to manage record labels, run:

```
Set-RegulatoryComplianceUI -Enabled $False
```

When you create a new retention label through Records management, you can choose to make the label act as a:

- Regular retention label.
- Record label.
- Regulatory record label.

The latter two options depend on enabling the necessary GUI. You can't select an existing retention label and transform it into a record label. Just like normal retention labels, the tenant must publish record labels through a label policy to make the labels available to users. If you want to withdraw a record label from active use, you should disable the policy used to publish the label.

After assigning a record label to a document, folder, or list item, users cannot delete the item until the retention period specified in the label expires. Any site member can lock or unlock records. SharePoint indicates the locked status of records with a small padlock on the item or folder icon. You can also see the locked status in the item properties (Figure 16-18). Assuming the record management settings for the tenant allow, after unlocking a record, users can edit its content. If someone subsequently updates a record after the last unlock action, SharePoint Online captures a copy of the item (before editing) in the *Records* folder of the site Preservation Hold Library. SharePoint Online highlights the version it captures by writing **Record** into the *Comment* field in the version history. You can't unlock an item assigned a regulatory record label, meaning that you shouldn't assign these labels until after you are sure that the record contains the final content.

Someone might lock a record while another member is editing the file. When this happens, the file contains anything saved (by autosave or the last explicit save) up to the point the user executes the lock action. To generate a complete copy including the changes made since locking, the person editing the file will have to save it under a different name and then exit the edit session. After a short period, SharePoint frees the file to allow an unlock to proceed. It will then be possible to merge any differences between the versions into the file.

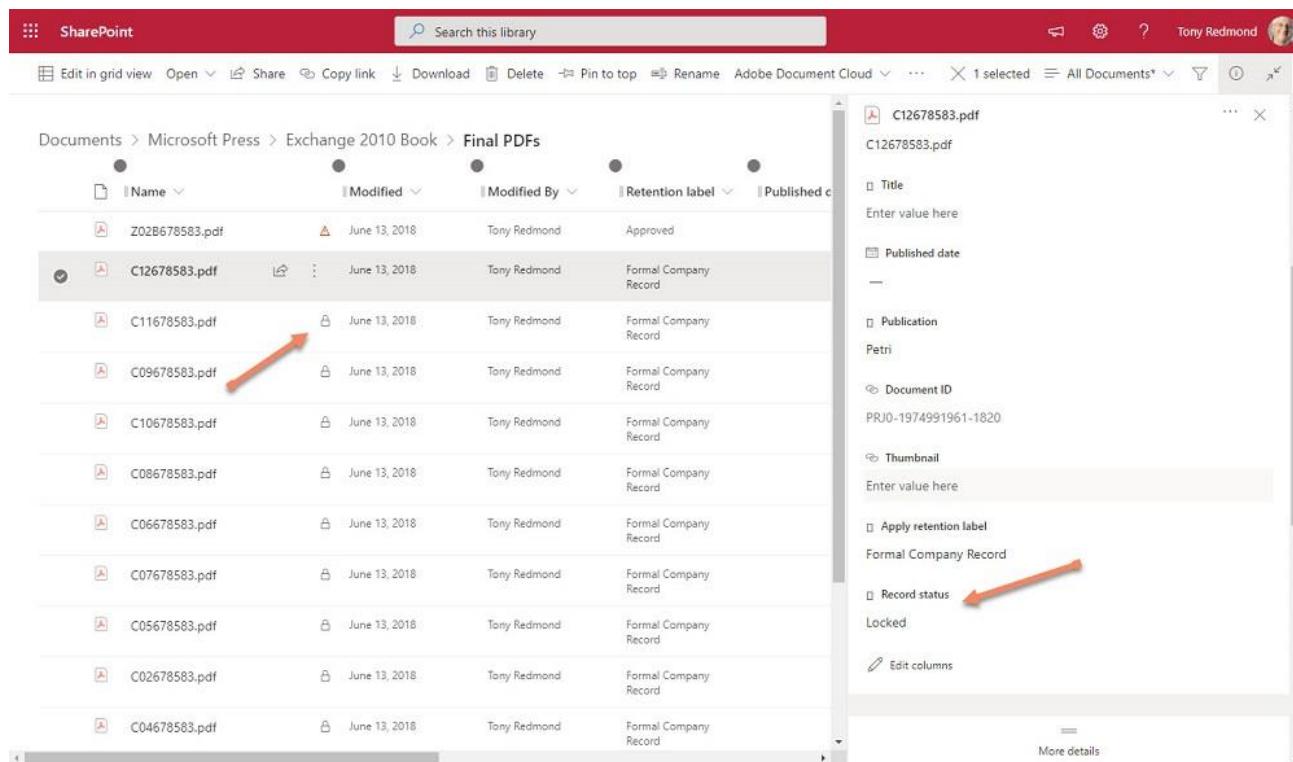


Figure 16-18: Documents in a SharePoint library marked as records

Although users need Office 365 E5 or Microsoft 365 E5 licenses to access the Records Management section in the compliance portal, any SharePoint Online or Exchange Online plan allows users to apply record labels to items. From a user perspective, after an item has a record label, it cannot:

- Permanently remove the item. If you try to remove an Exchange item labeled as a record, Exchange copies the item to the Recoverable Items structure and keeps it there until its retention period expires. If you try to remove an item marked as a record in SharePoint, the system flags an error, and the item remains unchanged. If someone tries to remove a record from a OneDrive for Business account, OneDrive for Business moves the item into the preservation hold library where it remains until its retention period expires.
- Edit a locked item. Users can unlock an item assigned a record label and edit its content, but those assigned a regulatory record label cannot.
- If the assigned label is a regulatory record label, item metadata cannot be updated.
- Change or delete the label. A site administrator can remove a record label, but no one can remove a regulatory record label.

Only users can assign record labels to items. You cannot use an auto-label policy to apply regulatory record labels to items.

The implementation of regulatory record labels within Exchange differs from that used by SharePoint Online and OneDrive for Business. Browser interfaces interact directly with the server while Exchange must support the synchronization model that enables Outlook desktop clients to work offline for extended periods. After applying a regulatory record label to a message, a certain window of time is available to change the label. The window accommodates Outlook's synchronization model and the need to update the new label status across multiple clients. After a few minutes, the window closes, and no further change is possible. Also, when you apply a record label to an Exchange folder, all the items stored in the folder automatically become records, even if the user later moves some or all the items out of the folder. When an Exchange item is tagged as a regulatory record, Outlook clients block deletion of the item. However, users can move messages tagged as records between folders in the mailbox.

Audit records for Records Management: When you apply a record label or a regulatory record label to an Exchange item, Exchange writes an *ApplyRecord* event into the audit log. This event comes from mailbox auditing, so it's not captured for the application of labels to SharePoint or OneDrive content using the browser interface. In these situations, SharePoint Online captures a *TagApplied* event, as it does for the application of any retention label. Note that SharePoint Online does not generate *TagApplied* events when new documents receive the default label assigned to a library. To find events for the assignment of record labels and regulatory record labels to documents and list items, you must search the audit log for *TagApplied* events and then examine the *AuditData* property of the events to look for those associated with record labels. See the Auditing and reporting chapter for more information about how to find data in the audit log. As [explained in this blog](#), it's also possible to use Microsoft Search to find items tagged as records in both a locked and unlocked state.

Processing Manual Dispositions

Retention labels are good for marking content for retention or removal, however, sometimes you do not want an automated process to function without supervision. For instance, you might have a label to mark documentation for customer projects. Usually, projects finish in a few months, and it is certainly safe to remove the associated documentation after five years. However, in some more complex or extended projects, you need to keep files for longer. A label that removes all documents classified as project documentation after five years would not work. The same might be true for items that the company might need for litigation or audit purposes.

As described in this [SharePoint blog from 2006](#), manual disposition is not a new idea. Microsoft 365 manual disposition allows retention labels to mark content for manual disposition from all workloads covered by data governance instead of just SharePoint. For now, Microsoft has enabled "Disposition Review" for items in SharePoint Online, OneDrive for Business, Exchange Online, and Microsoft 365 Groups. Support for other workloads might come in the future.

Manual disposition means that human intervention is necessary to check expired content to decide if the business still needs the items or if the deletion (disposition) can happen. A workflow notifies one or more expert reviewers, nominated because they have the skills needed to recognize content that the organization should retain for longer when they examine items with expired retention periods. The expert then decides to approve the removal of items or to extend their retention. Disposition can happen through a single review, or items can progress through up to five review stages with different reviewers processing items at each stage. The reviewers defined for each stage are individual accounts or mail-enabled security groups.

Background processes for each workload scan to detect expired items for manual disposition. When items await disposition, the compliance portal sends mail notifications to the reviewers defined in the retention label settings to tell them that content awaits their decision. Items remain in the awaiting disposition stage until a reviewer decides about their future. Reviewers also receive weekly reminders about items waiting for disposition. If a retention label uses multi-stage disposition, items processed in one stage pass to the next stage and so on until the last stage is complete.

Reviewers must have accounts with cloud mailboxes in the tenant. They should also be members of two compliance role groups:

- **Records management:** Members of this role group (containing the Disposition management role) have access to the disposition section of records management within the compliance portal.
- **Content explorer content viewer:** Members of this role group (containing the Data classification content viewer role) can view the content of items awaiting disposition. Members of the record management role group can see the details and history of items, but not the content.

If you wish, you can create a new role group and assign the necessary roles and members to that group. For instance, you might decide that it's a good idea not to grant access to the other features enabled for members of the Records management role group, like being able to customize the messages sent to reviewers. In this situation, you create a new role group and include only Disposition management and (optionally) the Data classification content viewer roles.

In addition to making decisions about keeping or removing items, the review process helps organizations understand whether people apply labels correctly. For instance, if you see documents stamped with inappropriate retention labels, you might ask why people use labels in error and then take steps to update procedures or change behavior.

How to Dispose of Items

When items marked with a label that triggers the manual disposition process reach the end of their retention period, background processes mark the items as being available for manual disposition. For example, when the Managed Folder Assistant processes mailboxes, it detects messages that need manual disposition and copies these items to a special hidden mailbox. Reviewers then process the items in this mailbox.

The screenshot shows the Microsoft Purview Compliance portal interface. At the top, there are navigation links: 'Records management' > 'Disposition' > 'Manual disposition'. Below this, there are two tabs: 'Pending dispositions' (selected) and 'Disposed items'. Underneath the tabs are 'Filter' and 'Reset' buttons, and a 'Filters' dropdown. A 'Source' dropdown is set to 'Exchange'. The main area displays a list of 9 selected items. The columns are 'Name' and 'Location'. The first item in the list has a checked checkbox next to it. To the right of the list is a preview pane for the selected item, which is titled 'Re: Tips from Office 365 for IT Pros'. The preview pane shows the message content: 'Every weekday, we publish a new article on the Office 365 for IT Pros website at <https://office365itpros.com/>. Recent articles have covered these topics:'. Below this is a bulleted list of links: 'Questioning Six Reasons Why Backing up Office 365 is Critical', 'Come in Internet Explorer – Your Time is Up', 'Blocking Email Forwarding from Power Automate', 'Microsoft Drops Office 365 Auditing for Sway', 'Teams Makes Background Effects Persistent Across Meetings', 'Planner Highlights Plan Changes but No Sign of Auditing Support', 'The 1-2-3 of Exchange Online Certificate Based Authentication for PowerShell', 'Analyzing Quarantined Messages with PowerShell', 'Reviewing Email Quarantined by Exchange Online Protection', 'Teams Meeting Policy Restricts Automatic Meeting Joins to Organizers', 'MailTips: Useful Guidance for Good User Email Habits', 'Customizing Privacy Controls for Microsoft Graph Insights with the Graph Explorer', 'Customizing the Office 365 Profile Card with Graph Explorer', and 'Azure AD My Sign-Ins Activity Report Now Generally Available'. At the bottom of the preview pane, a note says: 'The volume of change which happens inside Office 365 on an ongoing basis means that we have no shortage of things to write about. However, that change'. Below the preview pane are four buttons: 'Approve disposal', 'Relabel', 'Extend', and 'Add reviewers'.

Figure 16-19: A set of messages marked for manual disposition

When a reviewer decides how to dispose of an item, Exchange replicates the action taken for the item in the hidden mailbox and back to the source mailbox. The need for workloads to process items before the compliance portal recognizes them as being ready for manual disposition means that it can take a little time between the retention period for an item elapsing and that item showing up in the list of items awaiting disposition.

Those specified as reviewers in the label settings receive email notifications about items waiting for disposition. The reviewers can go to the **Disposition** section under **Records management** in the Microsoft Purview Compliance portal to see the items they should review, grouped into the items tagged with each label. Reviewers only see the items they can review while compliance administrators can see all items waiting

for review. To process the items, select a retention label and then the *Open in new window* icon to see the waiting items. In the review window, the compliance portal selects *SharePoint and OneDrive* as the source and loads the items awaiting disposition. If necessary, you can apply a filter (like a date range for item expiration) to refine the set of items shown. If email messages are awaiting disposition, you can see the messages by choosing *Exchange* in the Source filter. Figure 16-19 shows a set of messages waiting for disposition. Note that you can see messages shown in a set of SharePoint and OneDrive items. For instance, this can happen when messages are in SharePoint document libraries because someone sent them via email to a Teams channel.

After selecting an item waiting for disposition, you can:

- **Approve disposal (Delete permanently):** The organization no longer needs this content. When a reviewer approves an item for final deletion, the compliance portal releases the block on the deletion and logs the action in an *ApproveForDelete* audit record. The workload-specific jobs that remove expired items delete the items the next time they process the host location. If the item is in a document library when its retention period expires, marking it for deletion means that the item goes into the first stage Recycle Bin within 7 days of the disposition decision. On the other hand, if the item was already deleted and is in a site's Preservation Hold library, it is eligible for immediate deletion and will be removed following the normal disposal cycle. The audit log captures the actual file deletion in a *Deleted file* or *Deleted file from the second-stage recycle bin* audit record. The delay in deletion is because of the need to run background jobs to process the disposition decisions.
- **Relabel:** The organization should keep this content by applying another retention label to the item. The other label might not have a retention action or a longer retention period.
- **Extend:** Leave the original label on the item but extend the retention period to a new date after which the item goes through the review process again. This action overwrites the computed retention date for the item with the retention date selected by the reviewer. The compliance portal captures details of the extension in an *ExtendRetention* audit record. The audit record does not include the new retention date.
- **Add Reviewers:** Add other people who need to review the content to decide on its disposition. These people must have the necessary permissions to access record management.

You can also export the set of items waiting for disposition to a CSV file.

If the reviewer has access to a document's location, they can use the link to view the content. The compliance portal creates the link when the item becomes eligible for manual disposition, and if the item is subsequently deleted or moved the link is invalid. A document might be in a different folder or a preservation hold library, while a message might be in Deleted Items, Recoverable Items, or another folder. A reviewer might want to understand the full context of an item before authorizing its deletion, and if they don't have access to its location (or the link doesn't work), they must consult with the location's owners to decide on its disposition.

Items that a reviewer extends or relabels remain in their original location, or if they were moved into the Recoverable Items folder or preservation hold library, they are moved from there back to their original location.

A busy tenant can generate a heavy workload of review items if disposition review is the norm rather than an exception. For this reason, users should receive training about when they should apply labels that trigger reviews. Reviewers also need the training to understand how to deal with items awaiting their attention so that they know when they can authorize deletion or when they need to seek further guidance from the business about how to handle items.

Disposed Items and Proof of Disposal

Reviewers can see details of items that they or other reviewers previously authorized for deletion by selecting the **Disposed items** tab. This view only shows items that reviewers approved for deletion. It does not show items where the reviewer decided to apply a different label or extend the retention period. Items don't show up disposed until the underlying workload has processed the deletion. Because of the reliance on background processes, it might take a couple of days between a decision to delete an item and its appearance in the dispositions list.

Sometimes organizations need to show evidence of the removal of items. To meet this need, Office 365 retains details of all delete dispositions. You can download a CSV file containing details of these operations using the Export option under Disposed Items, using the filters to decide to download documents or messages and the time range for the download. Each line in the file notes the deletion of an item, including:

- Location.
- Title or Subject.
- Retention Label.
- The user principal name of the user who authorized the deletion.
- The timestamp when the deletion occurred.

According to Microsoft, the compliance portal can log up to one million disposal operations.

Retrieving Disposition Items with PowerShell

The *Get-ReviewItems* cmdlet in the Exchange Online management module is available to retrieve details of items awaiting or post disposition for a retention label. The advantage of the cmdlet is that it doesn't share the limitation of only being able to display 50,000 items that exists in the Purview compliance portal. In addition, organizations can report items in whatever way they choose after extraction. For more information about using the *Get-ReviewItems* cmdlet, see [this article](#).

Records Management Settings for Disposition

The settings on the Record management page allow members of the records management role group to:

- Define a mail-enabled security group for record managers allowed to see awaiting dispositions for all retention labels. Normally, a member of the records management role group sees only the dispositions assigned to them.
- Define additional text to include in the email notifications reviewers receive to let them know when items await their attention. You can't change the default text and can only add text that appears after the default text. For instance, you could add text to inform reviewers how to find company guidelines for disposition reviews.

You can also define the mail-enabled security group for record managers to see all disposition reviews using the *Enable-ComplianceTagStorage* cmdlet. Connect to the compliance endpoint and pass the email address of the security group as the parameter:

```
Enable-ComplianceTagStorage -RecordsManagementSecurityGroupEmail  
Compliance.Records.Managers@office365itpros.com
```

Allowing people to see all items waiting for disposition review is a highly permissioned capability. As such, the compliance portal doesn't support changing it through the GUI. Instead, if you need to make a change, run the *Enable-ComplianceTagStorage* cmdlet again to update the setting with the email address of a different mail-enabled security group.

The `Get-ComplianceTagStorage` cmdlet returns details of retention label (aka compliance tag) management settings. To see the email address of the group defining record managers with full access to disposition reviews, type:

```
(Get-ComplianceTagStorage).RecordsManagementSecurityGroupEmail
```

Event-based Retention

Labels normally use age-based retention periods and invoke retention actions based on the creation or last modified date of the content. Event-based retention takes a different approach and waits until a specific event occurs before starting the retention countdown for items. For instance, let's assume that you want to preserve all project documents for seven years after a project completes. The event is the project completion, which the project manager might have to sign off. The retention period begins as soon as the event occurs.

Because it depends on something happening rather than just the passing of time, event-based retention is more complex than date-based retention. Here is the general flow of what happens:

1. The administrator creates a new label and selects "an event" as the decision point for the retention period rather than the usual "date created" or "date modified" as used with other labels.
2. The administrator selects an event type (which must already exist) to associate with the label. An event is something like, the expiration of a contract or the departure of an employee, or any other common occurrence in the life of a business. A set of pre-packaged event types are available, but you can create new event types if needed.
3. After saving the label, the administrator includes it in a label policy and publishes the policy to make it available to end-users. After an hour or so, the label is available to SharePoint and OneDrive for Business. It takes a little longer for the label to appear in Exchange.
4. Users apply the label to content that they want to link with the event. For example, they might look for the set of documents belonging to a contract and apply the label to those documents.
5. When they apply the label, users also give a value to a field called "Asset ID," which is part of the standard SharePoint Online schema. A label for an event type is reusable across many different events, so a mechanism is necessary to isolate the content belonging to a specific event. The Asset ID is used to identify individual projects, tasks, or other entities. For instance, if the event deals with the departure of an employee, the Asset ID might hold the employee's number. The Asset ID must be populated correctly because this is the value used to find content associated with an event. You can find out what items are stamped for a specific event by using SharePoint search or content searches to look for the `complianceassetid` tag. For example, find items with `complianceassetid:PK1`.
6. When an event occurs, like an employee leaving or a contract reaching its end, the administrator goes to **Events** under **Records Management** in the Microsoft Purview Compliance portal and creates a new event to trigger compliance processing. They select the event type to use or choose an existing label configured for event-based retention used to classify items. To find the items for the event, they input the associated Asset ID (for SharePoint and OneDrive items in the form `complianceassetid:<value>`) and/or keywords to locate Exchange items. If other keywords are necessary to find the relevant items, they can be added at this stage (for instance, a tenant might already have assigned a different form of asset identifiers to project documentation). Finally, they select the date the event happened and save the event.
7. Background processes now start looking for content matching the event in SharePoint, OneDrive for Business, and Exchange (in effect, a content search is run). As the search finds matching items, the retention action and period specified in the label are applied to the items. Once the items are stamped, normal retention processing begins. For instance, if the label states that items should be kept for five years, the items are kept for five years after the event date. It can take up to a week before the background processes find all matching content across workloads.

Once created, you cannot update an event, so you should be sure that everything is ready to find the items relating to an event when you create it. In addition, once you associate a label with an event, you cannot change the label to associate it with a different event. For these reasons, it is important to have a good understanding of the business events that occur within the tenant and how people working in the business can use labels to aid the processing of content associated with using event-based labels. For more information about event-based retention, see the [Microsoft documentation](#).

Removing Retention Labels

Four scenarios occur for removing retention labels from a tenant:

- **A label is created, but not published.** Because the label is not in use, you can edit the label in the Microsoft Purview Compliance portal and remove it with the **Delete label** option. Alternatively, run the *Remove-ComplianceTag* cmdlet.

`Remove-ComplianceTag -Identity "Bad Label"`

- **A label is published in one or more policies but has never been assigned to items.** If you try and remove the label, you'll see an error that the label is in use. This is technically correct because the label is in a policy even though a user or policy never assigned the label to any items. To remove the label, you first remove it from all the policies it is included in (or remove a complete policy if the label is the only one in that policy). After removing the label from all policies, you can remove the label as described above.
- **A label is in active use and applied to content.** You can run a content search to find all the items that have the label (find a compliance tag equal to the label name) and remove the label from the items. This works when a label is recent and only applied to a small number of items but is unreasonable in a tenant of any size. Instead, you can follow the procedure as if the label was never assigned to any items by removing it from all policies and then removing the label in the Microsoft Purview Compliance portal or using PowerShell. The label then goes into a pending deletion state, meaning that some background processes in the different workloads must run to remove the label from items. A background timer job removes labels from SharePoint Online and OneDrive for Business documents and the process can take several hours to complete. For Exchange, the Managed Folder Assistant removes labels from mailbox items; it might take up to a week before the assistant processes a mailbox. Once the Managed Folder Assistant removes a label from an item, the item becomes a potential target for the assignment of another label by any other retention policy applying to the mailbox.
- **A label is a record.** As noted above, an item assigned a record label cannot be changed. You cannot remove any label marked as a record (even if the label has never been assigned to an item), but you can stop people from using it again by removing the label from any policies that it is in.

Removing labels is not something to do at a whim. The complexities involved in removing labels that are applied to content underline the need for planning and preparation for the deployment of labels as part of your data governance strategy. Removing labels from items can result in their deletion by background processes because their retention period has expired, so if you remove a label from content, you might need to replace those labels with different labels to ensure the retention of the items.

Data Classification Dashboard

Retention labels have existed for several years. Sensitivity labels were the next step. Over time organizations are likely to accumulate a reasonable amount of labeled material. But how does a compliance administrator know that their data governance strategy is effective, that users apply labels as intended, and that the right information is protected? Microsoft's response is the overview page of the Data classification dashboard

(Figure 16-20) in the Microsoft Purview Compliance portal. The dashboard contains some useful statistics about where and what labels are in active use:

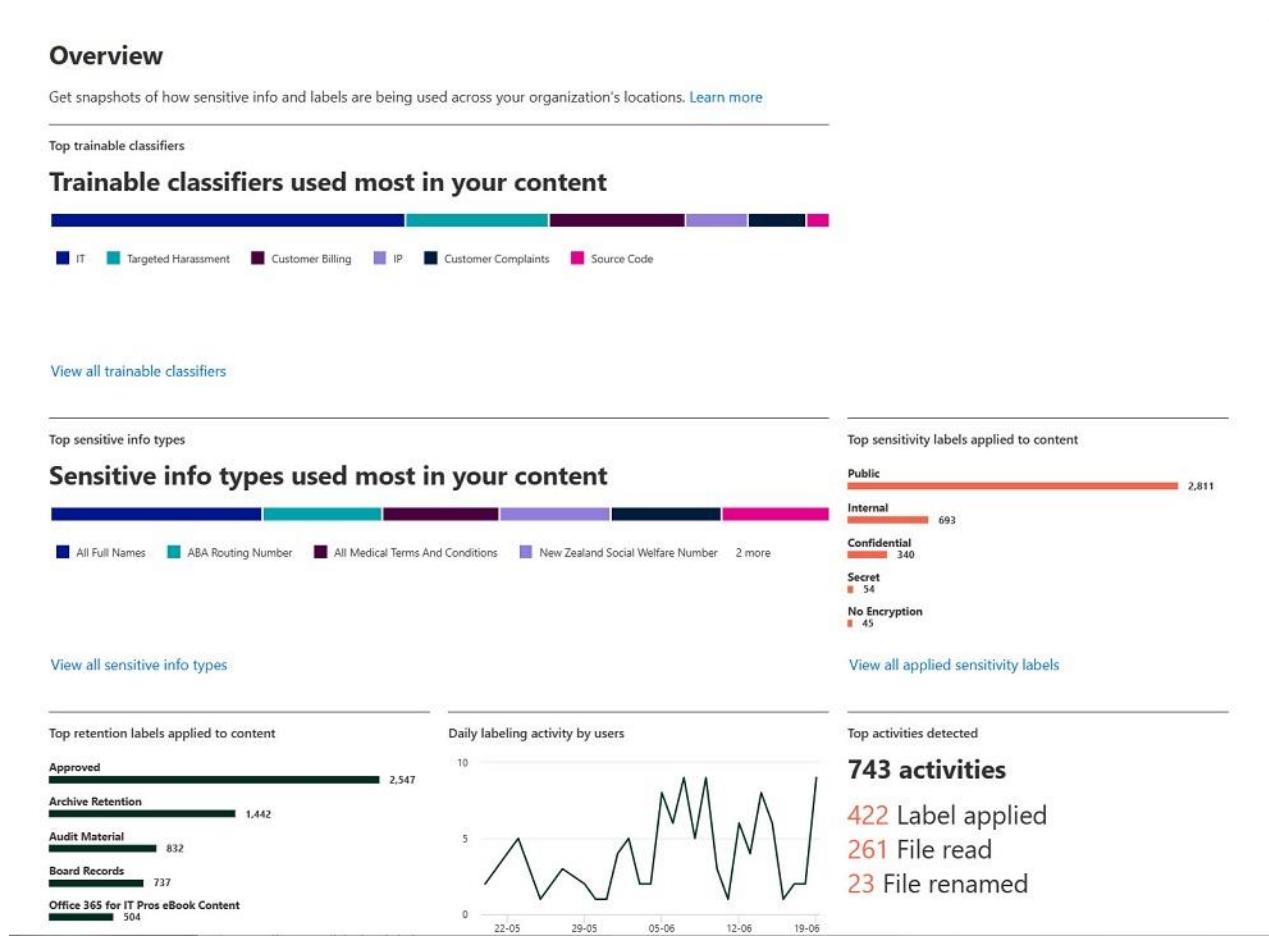


Figure 16-20: Overview page for the Data classification dashboard

Other information available in the Data classification section includes the Classifiers page, covering:

- **Trainable Classifiers:** This feature allows tenants to build custom sensitive information types by [using AI training based on a set of examples](#). Microsoft's default classifiers include document types like resumes and source code and classifiers used to detect objectionable behavior like profanity and threat.
- **Sensitive Info types:** Lists the sensitive information types known in the tenant, including the default set (over 200) created by Microsoft and those created by the tenant through digital fingerprinting, dictionaries, or simple rule matching.
- **EDM classifiers:** The regular sensitive information types used in Microsoft 365 match items using generic patterns, an approach that works well for document-centric information. As the name implies, [exact data matches](#) (EDM) use more precise matching and are more suitable for structured data. This option allows administrators to define EDM schemas and use those schemas to build custom sensitive information types.

Separate options bring you to:

- **Content Explorer:** Allows compliance administrators to see where retention and sensitivity labels are applied in Exchange Online, SharePoint Online, and OneDrive for Business. To view the locations where labels are applied, the user must hold the *Content Explorer List Viewer* permission; to view the source content of items in those locations, their account must hold the *Content Explorer Content Viewer* permission.
- **Activity explorer.** Shows usage data for both sensitivity and retention labels.

The overview is available with an Office 365 E3 license. Organizations need to have Office 365 E5 or Microsoft 365 E5 compliance licenses to use the content explorer, activity explorer, and trainable classifiers.

Content Explorer

The content explorer is especially useful in validating the effectiveness of label usage. The explorer allows administrators to see how users and policies apply retention and sensitivity labels and the type of content users apply labels to. For example, let's assume that you define a retention label for formal company records with a ten-year retention period. You probably don't want this label applied to run-of-the-mill documents and messages, and the content explorer allows you to see what's in the labeled items to check if the content is as valuable as the label implies.

The downside of the content explorer is its access to any user information in a SharePoint Online site, OneDrive for Business account, or Exchange Online mailbox. Although compliance administrators can use other features to access user data (a content search, for instance), because the content explorer organizes items by label, it's easy to find information labeled as being the most confidential or valuable to the organization and then peruse the content (items protected with sensitivity labels with encryption can't be opened by content explorer). For this reason, it's wise to make sure that the only people with the permissions needed to use content explorer are those who must have it to perform specific operations, and then remove those permissions once the need passes.

Activity Explorer

The Activity Explorer displays information about the application of retention and sensitivity labels to content in Exchange Online, SharePoint Online, and OneDrive for Business to help compliance administrators understand the use of labels within the organization. Data flows through to the Activity Explorer when sensitivity and retention labels are applied using Office Online, desktop (Microsoft 365 apps for enterprise), and mobile apps. Using a 30-day sliding window, the explorer gives an insight into:

- How labels were applied (manually by a user or by policy).
- Who applied, changed, or removed a label, including labels applied by an auto-labeling policy. If a user or policy changed a label on an item, you see details of the old and new labels. Details of labels applied by endpoint monitoring are also available.
- The location (Exchange Online, SharePoint Online, including OneDrive for Business).
- The target document or folder (the data does not show labels inherited by files from a label assigned to a folder).

You can filter by date range, label activity (all actions or just label changes, removals, or applications), user, workload, or specific label to focus on a specific activity. To see added information, click on an individual record to open the details pane. Sometimes it's good to create your view on this data. The Auditing and reporting chapter includes an example of using PowerShell to extract and interpret the audit records capturing when users assign retention labels. The Information protection chapter covers the capture of audit records for sensitivity labels. Alternatively, connect to the compliance endpoint and use the [Export-ActivityExplorerData](#) cmdlet to export data used by the Activity Explorer.

Trainable Classifiers

A [*trainable classifier*](#) is a digital map of a defined category of documents such as a customer invoice, order form, or personnel review. Microsoft 365 includes a set of built-in classifiers (created by Microsoft) such as HR, Healthcare, Legal Affairs, and Threat for use out-of-the-box. The pre-trained classifiers are available in English, Spanish, Japanese, French, German, Portuguese, Italian, and Chinese (simplified).

Organizations can create custom trainable classifiers by going through a training process. The major steps in the process are:

- Define the kind of information you want the trainable classifier to recognize. For example, you might want to create a trainable classifier that recognizes financial reports in a specific format.
- Assemble a set of sample documents for the training process to scan and build a digital picture using machine learning. The set acts as seed content for the classifier and should include between 50 and 500 “positive” samples available on a SharePoint Online site. Leave the content on the site for a day or so to allow indexing to happen before creating the classifier. By analyzing the seed content, the classifier builds a prediction model (the digital picture) to allow it to recognize documents of the same type when it processes them in the future. The more representative the seed content is of real-life documents, the more accurate the prediction model is likely to be.
- Test the classifier to see how it performs when it processes real content and tweak it if necessary. The seed set might require a refresh to introduce new examples to help the classifier refine its prediction model. During this phase, compliance administrators help the refining process by marking files identified by the classifier as good or bad matches. The aim is to increase the percentage of good matches to as close to 100% as possible.
- Publish the classifier to make it available for use with Microsoft Purview compliance solutions. If you discover that the classifier does not work well in production and retraining the prediction model with feedback does not improve its accuracy, you might need to withdraw (delete) the classifier and restart the training process with a new set of sample documents, including samples not detected by the previous iteration of the classifier. For this reason, use new trainable classifiers in limited policies (for instance, against a small number of SharePoint sites) and monitor its results closely until the classifier works as expected.
- Over time, monitor the items matched by the classifier and mark them as good or bad matches. The prediction model incorporates received feedback from administrators into new, hopefully, more accurate, versions. The caveat here is that feedback is only valuable when compliance policies use a trainable classifier to detect content. If this is not the case, retraining to take account of feedback is useless.

Machine learning takes time, and you cannot rush the creation of the prediction model for a trainable classifier. The entire end-to-end process from assembling the sample document set to publication might take several weeks before the classifier is accurate enough for production use (98% or better). After publishing the classifier, it becomes available to find items in:

- Communication compliance policies.
- Data Loss Prevention policies.
- Auto-label policies for sensitivity labels and retention labels.
- The Content explorer.

Trainable classifiers require Office 365 E5 or Microsoft 365 E5 Compliance licenses. See [this page](#) for more information.

Ingesting Items for Review from External Sources

Companies that need to supervise employee communications need coverage over more than just email. Employees can conduct business using a variety of consumer and business services including Twitter, Facebook, Bloomberg, HipChat, Thomson Reuters, and BlackBerry messaging. Microsoft has signed deals with [third parties specializing in the extraction of data](#) from different communication systems to create connectors to extract data from those systems and ingest the data into Microsoft 365. The basic approach is:

- A connector from a selected partner connects to the source data using whatever API is available. The connection runs on a scheduled or ongoing basis to find and extract data of interest.
- The connector uses Exchange Web Services to connect to an Azure endpoint for the ingestion of data into Exchange Online.
- Data flows across the connector to either:
 - User mailboxes, if a match exists between the identifier used by Exchange Online (usually the User Principal Name) and the identifier used by the source service. For instance, if the corporate Twitter account logs in as TwitterService@tenant.com and a user account exists with the same identifier, a match exists, and the data extracted from Twitter goes to that mailbox. Because you do not want someone to be able to access the information brought in via the connector, the items go into the Purges folder within Recoverable Items. The items are indexed and discoverable but invisible to anyone who logs into the mailbox.
 - Connector mailboxes are set up explicitly as a target for data ingested into Exchange Online through a connector. In this case, the items go into the Inbox folder because someone usually needs to check the items and decide where to keep the items over the long term.
- As items flow into Exchange Online through the connector, a separate set of agents watch the Exchange Web Services traffic to apply communication compliance policies.

When the data reaches Exchange Online, the imported items are indexed as normal and the content they hold is discoverable and usable by other data governance features. You can apply the data governance policies that exist within the tenant. In other words, you can assign retention policies to the mailboxes used by the connectors to ensure that you keep the ingested content for the desired retention period, including the mailboxes in content searches and eDiscovery cases, and so on.

Microsoft Connectors for Third-Party Data

Microsoft supports methods to import information from third-party sources into Exchange Online where the third-party information is then subject to data governance functionality. Many connectors are currently available including popular social media feeds like:

- **LinkedIn:** Import information from a [company's LinkedIn page](#).
- **Facebook:** Import information from a [Facebook business page](#).
- **Twitter:** Import tweets sent and received from a [company's Twitter account](#).

Preview versions of other connectors are also available. In general, connectors work by extracting information from the target source and creating items in an Exchange Online mailbox as described above.

Using PowerShell with Retention Labels and Policies

The cmdlets to manage retention labels and policies are available after connecting to the compliance endpoint. To access the cmdlets, connect to the compliance endpoint. It is not our intention to have a detailed and in-depth discussion of all the cmdlets here as it would occupy too much space. In any case, given the complexity of some of the operations involving compliance, it is usually best to create and update policies and labels through the GUI.

Working with Retention Labels

The `*-ComplianceTag` cmdlets manage retention labels. In this example, we extract the set of retention labels defined in a tenant and list the most important properties of each tag to understand the purpose of the tag: to mark an item as a record, has a retention action, the retention duration (in days), the retention action, and if it is in use.

```
Get-ComplianceTag | Format-Table Name, IsRecordLabel, HasRetentionAction, RetentionDuration, RetentionAction, Mode -AutoSize
```

Name	IsRecordLabel	HasRetentionAction	RetentionDuration	RetentionAction	Mode
Confidential	False	True	1825	Keep	Enforce
Remove after 1 week	False	True	7	Delete	Enforce
Patent Materials	False	True	7300	Keep	Enforce
Board Records	False	True	Unlimited	Keep	Enforce
Formal Company Record	True	True	7300	KeepAndDelete	Enforce

Labels marked as regulatory records can be found by examining the *Regulatory* property.

```
Get-ComplianceTag | Where-Object {$_.Regulatory -eq $True} | Format-Table Identity, Notes
```

Identity	Notes
Regulatory Record (Legal)	A legal regulatory record

The *New-ComplianceTag* cmdlet creates a new retention label. In this example, we create a retention label to keep content for ten years. This retention label does not mark content as a formal record.

```
New-ComplianceTag -Name "Patent Information" -IsRecordLabel $False -RetentionDuration 3650
-RetentionAction Keep -Comment "Items marked with this classification are associated with patents"
-RetentionType ModificationAgeInDays
```

The *Set-ComplianceTag* cmdlet updates the properties of a retention label while the *Remove-ComplianceTag* cmdlet removes a label from a tenant. For example, this command sets the retention duration for the "Patent Materials" label to 15,000 days (the maximum is 24,855):

```
Set-ComplianceTag -Identity "Patent Materials" -RetentionDuration 15000
```

The audit log captures changes made to retention tags with the *SetComplianceTag* event. Updates to retention policies generate *SetRetentionCompliancePolicy* events for updates to policy settings and *SetRetentionComplianceRule* events for changes to rules belonging to policy rules, like updating the retention period.

Working with Retention Policies

Retention policies use a parent/child structure. The parent is the policy itself and the child is the set of rules that implement the policy settings. Another way of thinking about this is that the parent for a policy defines the overall data to which the policy applies while the rules govern the application of a policy. It is a little simpler than it seems because a 1-to-1 relationship usually exists between retention policies and retention rules (including label policies). The Compliance portal hides the links between retention policies and rules, but the connection needs to be understood when we manage retention policies through PowerShell. Two cmdlet sets are used:

- The **-RetentionCompliancePolicy* cmdlet set manipulates retention policies. Use these cmdlets to manipulate the workload locations to which a policy applies or to enable or disable a policy.
- The **-RetentionComplianceRule* cmdlet manipulates the rules for retention policies. Use these cmdlets to work with properties such as the retention duration of a policy.

When you fetch details of retention policies with the *Get-RetentionCompliancePolicy* cmdlet, the set returned includes policies used to:

- Apply retention settings to workloads.
- Publish retention labels to workloads.

Not all the retention policies in a tenant publish retention labels to workloads. The *Get-RetentionCompliancePolicy* cmdlet returns all the policies used for retention labels. Here is some code to find

the set of retention policies used to publish retention labels and then tell us what retention labels are in each policy:

```
$Policies = (Get-RetentionCompliancePolicy -RetentionRuleTypes | Where-Object {$_._RetentionRuleTypes -eq "Publish"} )
ForEach ($P in $Policies) {
    Write-Host "Processing" $P.Name
    $Tag = $Null
    $Rules = (Get-RetentionComplianceRule -Policy $P.Guid)
    ForEach ($R in $Rules) {
        If (-Not [string]::IsNullOrEmpty($R.PublishComplianceTag)) {
            $Tag = $R.ComplianceTagProperty -Split ","
            $TagValues = Get-ComplianceTag -Identity $Tag[0]
            Write-Host $P.Name "includes the retention label" $TagValues.Name
        }
    }
}
Processing Company Confidential Policy
Company Confidential Policy includes the retention label eBook Content
Company Confidential Policy includes the retention label Contractual Information
Company Confidential Policy includes the retention label Confidential...
```

Get-RetentionCompliancePolicy does not return all retention policies listed by the compliance portal. Microsoft regards the retention policies for Teams private channels and Viva Engage conversations as “app specific” policies and the cmdlet does not return details of these policies (compliance records for conversations from Teams shared channels are in the mailboxes of channel members). Instead, you must manage app specific policies using:

- *Get-AppRetentionCompliancePolicy*.
- *Set-AppRetentionCompliancePolicy*.
- *New-AppRetentionCompliancePolicy*.
- *Remove-AppRetentionCompliancePolicy*.

These cmdlets behave in the same way as the cmdlets that interact with regular compliance policies do.

The different treatment for compliance records for Teams private channels and Viva Engage communities possibly exists because of the way that these records are intermingled with other compliance items (such as those for Teams chat) in user mailboxes. Special background processes apply the app-specific retention policies against the compliance records for private channels and Viva Engage communities.

Retention Rule Types

As shown in the example above, the *RetentionRuleTypes* property of a policy tells us what kind of policy an individual retention policy is. To see this information, you must return the policy type by including the *RetentionRuleTypes* parameter in the call to *Get-RetentionCompliancePolicy*. For example:

```
Get-RetentionCompliancePolicy -RetentionRuleTypes | Sort RetentionRuleTypes | Format-Table Name, RetentionRuleTypes
```

Three values report the types of retention policies:

- **Apply:** The policy uses advanced settings (like a keyword search) to find the content to which it applies labels. These are also known as auto-label policies.
- **Default:** The policy publishes retention settings to workloads (static or adaptive policies).
- **Publish:** The policy publishes labels to workloads.

Fetching Retention Policies

To fetch the properties of an individual retention policy, run the *Get-RetentionCompliancePolicy* cmdlet:

```
Get-RetentionCompliancePolicy -Identity 'GDPR Personal Data' -DistributionDetail | Format-List
ExchangeLocation, SharePointLocation, OneDriveLocation, ModernGroupLocation, TeamChatLocation,
TeamChannelLocation, Workload, Enabled, Mode, RestrictiveRetention, DistributionStatus

ExchangeLocation : {All}
SharePointLocation : {All}
OneDriveLocation : {}
ModernGroupLocation : {}
TeamChatLocation : {}
TeamChannelLocation : {}
Workload : Exchange, SharePoint, OneDriveForBusiness, ModernGroup
Enabled : True
Mode : Enforce
RestrictiveRetention: False
DistributionStatus : Success
```

We can interpret the output as follows:

- **ExchangeLocation:** Lists the names of the mailboxes covered by the policy. If All, it means that all mailboxes are covered (the same is true for the other locations).
- **SharePointLocation:** Lists the SharePoint Online sites covered by the policy.
- **ModernGroupLocation:** Lists the aliases for the Groups covered by the policy.
- **OneDriveLocation:** Lists the OneDrive for Business locations covered by the policy.
- **TeamChatLocation:** Lists the locations for personal and group chats covered by the policy.
- **TeamChannelLocation:** Lists the Teams (all channels) covered by the policy.
- **Workload:** Lists the workloads where the policy is active. In this case, Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft 365 Groups.
- **Enabled:** Tells you whether the policy is active or not. The default is \$True, but if a policy has been disabled for some reason, this value is \$False.
- **Mode:** If "Enforce", the policy is active.
- **RestrictiveRetention:** The default is False, meaning that the policy can be changed. If True, a preservation lock exists on the policy, meaning that administrators can only make limited changes to the policy.
- **DistributionStatus:** Success means that the different workloads have the information needed to enforce the policy settings. Pending means that Microsoft 365 is distributing details of a policy change to workloads. Any other value shows that a problem has occurred in the policy distribution. Sometimes this happens for good reason, such as a change occurring in a data center. If you see problems when distributing labels to certain locations, it might be possible to figure out where the problem lies by examining the *DistributionResults* property for the policy. You won't see the current distribution status or any errors unless you include the *DistributionDetail* parameter (see example below).

If you see "All" listed as a value for a workload, it means that the policy covers every location supported by that workload. For example, "All" listed in *ExchangeLocation* means that the policy covers every Exchange mailbox in the tenant. You can exclude specific mailboxes or sites in a workload from the policy. If this is the case, you will find a list of those locations in the properties *ExchangeLocationException*, *SharePointLocationException*, and so on.

To find retention policies using adaptive scopes, check the value of the *IsAdaptivePolicy* property:

```
Get-RetentionCompliancePolicy -DistributionDetail | Where-Object {$_.IsAdaptivePolicy -eq $True} | Format-List Name, IsAdaptivePolicy, AdaptiveScopeLocation

Name : Retention Policy for French IT Architects
IsAdaptivePolicy : True
AdaptiveScopeLocation : {French IT Architects, Executive Mailboxes}
```

Retention policies for Teams private channel messages use the *ExchangeLocation* property to indicate the set of locations (compliance records for these messages are in Exchange mailboxes). The *Applications* property is set to **User:MicrosoftTeamsChannelMessages** to indicate the type of information the policy covers. The same approach applies for retention policies for Viva Engage messages. In this case, the *Applications* property holds **Group:Yammer** to indicate that the policy processes community messages and **User:Yammer** for user messages.

Including Distribution Details

When you look at retention policies with the *Get-RetentionCompliancePolicy* cmdlet, you won't see details of the individual mailboxes or sites specified for locations, the up-to-date distribution status, or any error information unless you include the *DistributionDetail* parameter. To see details of locations or errors, you need to expand the relevant property for the location you want to examine. For example, here's how to examine details of the mailboxes to which a policy applies.

```
Get-RetentionCompliancePolicy -Identity "Senior Leadership Team" -DistributionDetail | Select-Object -ExpandProperty ExchangeLocation

DisplayName      : Kim Akers
Name            : Kim.Akers@Office365itpros.com
ImmutableIdentity : f120e18f-8305-41e3-abd4-de93d4a2a493
Type            : IndividualResource
Workload         : Exchange
SchemaVersion    : 2

DisplayName      : Brian Weakliam
Name            : Brian.Weakliam@office365itpros.com
ImmutableIdentity : aae8332a-6832-4c00-b873-6ec443c36395
Type            : IndividualResource
Workload         : Exchange
SchemaVersion    : 2
```

Here's an example of looking at retention policies that have encountered problems when distributed to workloads. Often the issue is a transient problem caused by a recipient selected for the policy being unavailable for some reason that you can fix by editing the policy to remove the recipient and then add them back again.

```
$Errors = (Get-RetentionCompliancePolicy -DistributionDetail | Where-Object {$_ .DistributionStatus -eq "Error"})
ForEach ($E in $Errors) {
    $Results = ($E | Select-Object -ExpandProperty DistributionResults)
    Write-Host "Policy:" $E.Name "Issue:" $Results
}
Policy: Company Confidential Policy Issue: [Exchange]SMO-Academy@office365itpros.onmicrosoft.com:Recipient not found: f120e18f-8305-41e3-abd4-de93d4a2a493
Policy: Black Matter Policy Issue: [ModernGroup]'ModernGroup' Resources:Policy deployment has been interrupted by an unexpected Office 365 data center issue. Please contact Microsoft support to fix the deployment issue.
[ModernGroup]BlackMatterTeam@office365itpros.com:Recipient not found: 6661b878-83b5-41bb-aad4-ba14e8879b90
```

Retention Policy Rules

Returning to our discussion about rules, when you create a new retention policy, Microsoft 365 creates the underlying rule for the policy is created to instruct workloads on how to process content. We can see the rule for a retention policy by using the *Get-RetentionComplianceRule* cmdlet. Because policies can have similar names, passing the GUID identifying the policy makes sure that the correct information is returned. To discover the identifiers for retention policies, run the command:

```
Get-RetentionCompliancePolicy | Format-Table Name, Guid
```

If you don't want to use a GUID, pass the policy name and hope it's unique:

```
Get-RetentionComplianceRule -Policy 'Patent Materials' | Format-List ContentMatchQuery, RetentionDuration, RetentionComplianceAction, ExpirationDateOption, Workload
```

ContentMatchQuery	:	Patent NEAR(10) claim Patent NEAR(10) prosecution Patent NEAR (10) application
RetentionDuration	:	3650
RetentionComplianceAction	:	KeepAndDelete
ExpirationDateOption	:	ModificationAgeInDays
Workload	:	Exchange, SharePoint, OneDriveForBusiness, ModernGroup

Some of the output (Workload in this case) matches what you see when examining the policy. The interesting pieces here are:

- **ContentMatchQuery**: The KeyQL query to determine whether items come under the scope of the retention policy. In this case, three separate tests are used.
- **RetentionDuration**: The length of time in days to retain items. You can also use "unlimited". In this case, the items remain held indefinitely until the hold set by the policy lapses or the policy is removed from the tenant. The hold duration is calculated using the created date for email items and the date last modified for files in SharePoint Online or OneDrive for Business sites.

Rule settings can be changed using the *Set-RetentionComplianceRule* cmdlet. For example, this command sets the retention duration for a rule to 3,600 days (the maximum duration is 24,855 days):

```
Set-RetentionComplianceRule -id 86f67249-74b9-48bf-8fe6-9e0c58416dfb -RetentionDuration 3600
```

Changes made to a rule will not be effective until the publication of the policy update becomes known to all the workloads. This might take a few hours.

To publish labels and make them available to workloads, we create a retention label policy and associate a rule for each label with that policy. In other words, every label published by the policy has a separate rule. Labels can be in multiple label policies and the connection between label and rule is through the label GUID. If you run the *Get-RetentionComplianceRule* cmdlet to find all the rules belonging to a policy, you can find the different labels by looking at the *PublishComplianceTag* property, which holds the GUID pointing back to the label. The rule for an auto-label policies specifies its label in the *ApplyComplianceTag* property.

Setting Retention Policies

You can force the republication of a policy to the workloads by running the *Set-RetentionCompliancePolicy* cmdlet. For example:

```
Set-RetentionCompliancePolicy -Identity 'Patent Materials' -RetryDistribution
```

Republishing a policy to workloads only works if an error previously prevented a policy from reaching a workload. If a policy cannot be published to workloads for some reason, you should file a support incident with Microsoft.

The *Set-RetentionCompliancePolicy* cmdlet can also add or remove workload locations to the policy. In this example, we remove a mailbox and add a mailbox to the set of Exchange locations. The same approach is taken remove and add some SharePoint sites. Note that you must give the URL for each site.

```
Set-RetentionCompliancePolicy -Identity 'Patent lock-down'  
-AddExchangeLocation 'Frank Clonan' -RemoveExchangeLocation 'Rob Young'  
-RemoveSharePointLocation 'https://office365itpros.sharepoint.com/Projects/'  
-AddSharePointLocation 'https://office365itpros.sharepoint.com/Exchange Connections'
```

Reporting Retention Policies Applied to SharePoint

As an example of using information about distribution detail and retention rule type to analyze or report on retention policies, let's say that you want to know what retention policies apply to SharePoint sites. The code in [this GitHub script](#) fetches information about the retention policies including their distribution detail, excluding retention policies for Teams, those that don't process SharePoint, and policies used to publish retention labels. We then examine each policy to extract the locations within the policy scope and figure out whether the retention settings are simple or advanced (using a keyword query or sensitive information type). Some policies apply to every SharePoint site, so the location is "All." Others have specific SharePoint sites defined, and some policies process everything except a set of excluded sites. The output is an ordered array. We can look at the data in different ways with PowerShell (see below) or export it to a CSV file to load into Excel or Power BI.

Policy	Site	Duration	Action
SharePoint Online Retention Policy	*Exclude* Interesting Patent		
SharePoint Online Retention Policy	*Exclude* Frank's Italian Job		
Label Customer Invoices	All SharePoint Sites	2555	Keep
SharePoint Online Retention Policy	All SharePoint Sites	2555	Keep
Preserve Office 365 for IT Pros Files	Company Communications	Unlimited	Keep
Preserve Office 365 for IT Pros Files	GDPR Planning Mark II	Unlimited	Keep
Senior Leadership Team (SLT) Retention Policy	Office 365 Speakers	3600	KeepAndDelete
Office 365 for IT Pros eBook Content	Office 365 for IT Pros	3650	Keep
Preserve Office 365 for IT Pros Files	Office 365 for IT Pros	Unlimited	Keep
Preservation Lock - Mailboxes and Sites	PL Test Group	3650	KeepAndDelete
Management Preservation Policy	Projects	Unlimited	Retain

Viewing Teams Retention Policies

Remember that a Teams retention policy can only cover Teams personal chats and channel conversations and a general retention policy applied to other locations cannot cover Teams. If you only want to work with retention policies that affect Teams, use the *TeamsPolicyOnly* parameter when fetching retention policies:

```
Get-RetentionCompliancePolicy -TeamsPolicyOnly
```

Likewise, to exclude the Teams policies, use the *ExcludeTeamsPolicy* parameter:

```
Get-RetentionCompliancePolicy -ExcludeTeamsPolicy
```

Remove a Retention Policy

To remove a retention policy, run the *Remove-RetentionCompliancePolicy* cmdlet. Remember that you will not be able to remove a policy if a preservation lock is in place.

Tracking Retention Holds for Mailboxes

When a non-org-wide retention policy applies an in-place hold to a mailbox, Exchange Online notes the fact by updating the *InPlaceHolds* property of the mailbox with the GUID for the hold. Thus, you can get a quick view of what mailboxes are on hold by checking the mailbox properties for *InPlaceHolds* using PowerShell. For instance:

```
Get-ExoMailbox -RecipientTypeDetails UserMailbox -Properties InPlaceHolds | Where-Object {$_._InPlaceHolds -ne $Null} | Format-Table DisplayName, InPlaceHolds
```

DisplayName	InPlaceHolds
Tony Redmond	{skp748f77b020124e6e8304e66021fb297b:3, mbx748f77b020124e6e8304e66021fb297b:3}
Kevin A. Laahs	{UniH26c5d797-0fd3-496d-92ac-4f405700c917}
Kim Akers	{mbx748f77b020124e6e8304e66021fb297b:3, skp748f77b020124e6e8304e66021fb297b:3, UniHec6...}

One reason why you might want to check the holds set on mailboxes is to find out what holds are keeping inactive mailboxes alive.

```
Get-ExoMailbox -RecipientTypeDetails UserMailbox -InActiveMailboxOnly -Properties InPlaceHolds | Format-Table DisplayName, InPlaceHolds
```

DisplayName	InPlaceHolds
Holly Holt	{}
James Gangley	{mbx29550d04cffd42109bdd94cc56c65041:2}
Jodie Smith (Program Manager)	{}
Rob Young	{d9eb7052cc0f4200b6a1ad0d6f2171ed...}
Mary Smith (Customer Support)	{}
Ed Banti	{skp748f77b020124e6e8304e66021fb297b:3}

When you see an inactive mailbox shown with a null value in *InPlaceHolds*, you know that the hold on the mailbox comes from an org-wide retention policy (or an Exchange Online litigation hold) instead of a non-org-wide policy. More on this topic in a little while.

To get a full view of the holds that apply to an individual mailbox, use the *Get-ExoMailbox* cmdlet, and expand *InPlaceHolds*:

```
Get-ExoMailbox -Identity "Ben Owens" -Properties InPlaceHolds | Select-Object -ExpandProperty InPlaceHolds
```

mbx748f77b020124e6e8304e66021fb297b:3
skp748f77b020124e6e8304e66021fb297b:3
UniH47f67751-1036-4621-80d6-d25837adf813
UniHec6163be-6ed6-4b16-afe8-1b2165b9359f
UniH84dea76f-c845-4101-b066-a8b10c13c210

One of the holds listed applies to Skype for Business conversions (skp). Another is for mailbox contents (mbx). If you see a minus sign before an “mbx” hold, it means that a retention policy explicitly excludes the mailbox. The numeric notation following the hold identifier tells you the kind of hold it is:

- 1: The retention policy deletes items. Microsoft also uses this value for label publishing policies for retention labels and sensitivity labels.
- 2: The retention policy holds items. Microsoft 365 doesn’t remove the items after the hold lapses.
- 3: The retention policy holds items and then deletes them after the retention period expires.

The holds with a “UniH” prefix are “unified holds” and belong to:

- A hold placed by an eDiscovery case created through the Microsoft Purview Compliance portal.
- A hold placed by an old preservation policy now upgraded to a retention policy.

If a hold shows up as a GUID without a prefix or it has a “cld” prefix, it belongs to an Exchange in-place hold managed from the EAC. These include holds created for mailboxes included in eDiscovery cases managed in the SharePoint eDiscovery Center. While you might come across these GUIDs, they should begin to disappear over time as workload-specific holds expire.

The GUID for a hold placed by a retention policy can be used to find which policy the hold belongs to. Take the value stored in the *InPlaceHolds* property, remove the prefix (like “mbx”) and suffix (like “:3”), and use the value to check against the set of retention policies for the organization.

```
Get-RetentionCompliancePolicy 748f77b020124e6e8304e66021fb297b
```

Name	Workload	Enabled	Mode
Senior Leadership Team (SLT) Retention Policy	Exchange, ModernGroup	True	Enforce

We now know that the mailbox comes under the scope of the Senior Leadership Team (SLT) Retention Policy. This is a non-org wide policy that applies to selected Exchange locations (mailboxes). If we look at the *ExchangeLocation* property, we see a list of the mailboxes the policy applies to, or "All" if the policy applies to all mailboxes. For example, here's a typical entry for a mailbox.

```
Get-RetentionCompliancePolicy 748f77b020124e6e8304e66021fb297b -DistributionDetail | Select-Object -ExpandProperty ExchangeLocation
```

DisplayName	:	Tony Redmond
Name	:	Tony.Redmond@office365itpros.com
ImmutableIdentity	:	d446f6d7-5728-44f8-9eac-71adb354fc89
Type	:	IndividualResource
Workload	:	Exchange
SchemaVersion	:	2

The *ImmutableIdentity* property reported for each mailbox on hold equates to the GUID identifying the user account and is the same value that you see if you run the *Get-ExoMailbox* cmdlet and examine the *ExternalDirectoryObjectID* property.

Group Mailboxes and Holds

To discover if any holds apply to a group mailbox, run the *Get-UnifiedGroup* cmdlet and examine the contents of the *InPlaceHolds* property:

```
Get-UnifiedGroup -Identity "Office 365 for IT Pros" | Select-Object InPlaceHolds
InPlaceHolds
-----
{grp6a9f7bf0507b4a4983c301a701958d11:2, UniH26c5d797-0fd3-496d-92ac-4f405700c917}
```

To find what groups a hold applies to, specify the *DistributionDetail* parameter when calling *Get-RetentionCompliancePolicy* to return details of the locations covered by the policy. For example:

```
Get-RetentionCompliancePolicy -DistributionDetail | Where-Object {$_._.ModernGroupLocation -ne $Null -and $_._.ModernGroupLocation -notlike "*All" } | Format-List Name, ModernGroupLocation
Name : Clean up Groups with Connectors
ModernGroupLocation : {office365tenantservicehealth, office365roadmapupdates, askhr}

Name : Senior Leadership Team (SLT) Retention Policy
ModernGroupLocation : {Senior Leadership Team}
```

This technique only works to report details of the holds placed by retention policies. We need to process the other types of holds differently to uncover their secrets. More on this topic soon.

Org-wide Retention Policies

Org-wide retention policies applying to all mailboxes do not stamp hold information on individual mailboxes. Instead, the Exchange Online organizational configuration for the tenant stores details of the holds belonging to retention policies applicable to all mailboxes. This approach avoids the need to write the hold information into every mailbox and then check for individual holds when evaluating items for deletion. Here is how to retrieve information about the holds for org-wide retention policies.

```
Get-OrganizationConfig | Select-Object -ExpandProperty InPlaceHolds
mbx15382841af9f497c83f9efe73e51888d:1
mbx9696959111f74ecda8a40aef97edd2c2:1
mbx703105e3b8804a1093bb5cb777638ea8:1
mbxf6a1654abdba4712a43c354e28a4d56c:2
grpf6a1654abdba4712a43c354e28a4d56c:2
```

"mbx" refers to policies applied to user mailboxes and "grp" means policies applied to group mailboxes.

Phantom Holds for Sensitivity Labels

If your tenant uses sensitivity labels, sensitivity label policies exist to publish the labels to workloads. As explained earlier, sensitivity policies appear like retention policies and must be excluded if you want to focus solely on retention policies. Even though the policies only publish labels, the policies insert entries into the set of org-wide retention holds held in the Exchange organization configuration. These holds can be ignored.

Discovering Holds in Force for a Mailbox

Taking all that we know about the different forms of holds into account, we can come up with a PowerShell script ([downloadable from GitHub](#)) to report the set of holds that are in force for a mailbox. The script accepts the name of a mailbox and reports any organization-wide holds followed by holds where the mailbox is in scope.

Enter User to check: Ben Owens	
The following organization-wide mailbox holds are in force...	
Name	Workload
GDPR Personal Data	Exchange, SharePoint, OneDriveForBusiness, ModernGroup
General sensitivity policy	Exchange, SharePoint, OneDriveForBusiness, ModernGroup
Office 365 for IT Pros ...	Exchange, SharePoint, OneDriveForBusiness, ModernGroup
Formal Company Records	Exchange, SharePoint, OneDriveForBusiness, ModernGroup
Company Confidential Po...	Exchange, SharePoint, OneDriveForBusiness, ModernGroup

The following specific holds are in place on the Ben Owens (Business Director) mailbox...
Exchange In-Place Hold: New EAC Search
Hold Applied by: Senior Leadership Team (SLT) Retention Policy on Exchange, SharePoint, OneDriveForBusiness, ModernGroup
Hold Applied by: Management Preservation Policy
Litigation hold is enabled on the mailbox Ben Owens (Business Director)

If your tenant uses sensitivity labels, you need to amend the code to exclude the holds set by sensitivity label policies in the Exchange organization configuration. See the earlier discussion.

The *ComplianceTagHoldApplied* and *DelayHoldApplied* Properties

If a user applies a retention label that's configured to retain content to an item or folder in their mailbox, Exchange Online updates the *ComplianceTagHoldApplied* property for the mailbox. Because a specific hold is in place for one or more items, Exchange regards the mailbox as being in the same state as if an administrator assigned it a retention policy or placed the mailbox on litigation hold. For this reason, if the account for the mailbox is removed, Exchange puts the mailbox into an inactive state and keeps it there until the longest retention period for any label assigned to the mailbox expires. To see a list of mailboxes with applied retention labels, use the command:

```
Get-Mailbox -Filter {ComplianceTagHoldApplied -eq $True} | Select-Object DisplayName
```

If a mailbox is not listed, it does not mean that its contents are not on hold due to a retention policy, in-place hold, or litigation hold. It simply means that the mailbox owner has never applied a retention label to an item or folder.

Delayed Holds

After any type of hold is removed from a mailbox, Exchange puts the mailbox into a delayed hold state and keeps it there for 30 days. The extra retention step exists to give administrators the chance to recover information released by the hold after the hold is removed. In effect, this is a backstop to stop Exchange purging data in case a mistake is made in releasing a hold. While the mailbox is on delay hold, Exchange treats it as if it were on litigation hold and everything is kept. The Managed Folder Assistant is responsible for tracking holds on mailboxes. When it notices the release of a hold, the Managed Folder Assistant updates one

or both mailbox properties to mark that a delay hold is in force. Because of the variety of information stored in Exchange Online mailboxes, the Managed Folder Assistant uses two properties to track delay holds:

- **DelayHoldApplied** is used when a hold applied to user-generated content created using email clients like Outlook. User content is stored in visible folders.
- **DelayReleaseHoldApplied** is used for app content such as compliance records stored in mailboxes. App content is stored in hidden mailboxes.

For instance, to see which mailboxes are on delayed hold for user-generated content, run this command:

```
Get-Mailbox -RecipientTypeDetails UserMailbox -Filter {DelayHoldApplied -eq $true} | Select-Object DisplayName
```

It takes a little time after releasing a hold before the delay hold status is visible for a mailbox. Exchange does not expose any information about when the delayed hold status starts or ends, nor does Exchange give any information about the removed holds. When the 30-day delay hold period elapses, the Managed Folder Assistant sets the property back to `$False` and purges the items that were on hold.

If the need exists to release a delayed hold, you can do so by running the `Set-Mailbox` cmdlet to set the `RemoveDelayHoldApplied` or `RemoveDelayReleaseHoldApplied` switch, depending on the type of delay hold that's in place. For example, this command clears the delay hold for user-generated content on any mailbox where it is set.

```
Get-Mailbox -RecipientTypeDetails UserMailbox -Filter {DelayHoldApplied -eq $true} | Set-Mailbox -RemoveDelayHoldApplied
```

You can remove a delayed hold for an inactive mailbox to speed its removal. Two operations are necessary to remove the different types of delay hold:

```
Set-Mailbox -Identity Peter.Jenkins -InactiveMailbox -RemoveDelayHoldApplied  
Set-Mailbox -Identity Peter.Jenkins -InactiveMailbox -RemoveDelayReleaseHoldApplied
```

Exchange Retention Holds

Apart from in-place holds, Exchange Online supports retention holds. This is not a hold of the type generally referred to as Exchange in-place or litigation holds, holds due to retention policies, or eDiscovery case holds, all of which stop the removal of information by a user or a system process (except retention processing). An Exchange retention hold stops the Managed Folder Assistant from processing the retention policy for a mailbox for a period and is usually applied when a mailbox owner cannot manage their mailbox because they are ill, on vacation, or absent for some other reason.

Exchange retention holds are still in use. Because they affect how MFA processes mailboxes, they influence the retention policies applied to mailboxes. In other words, if a retention hold stops MFA from processing a mailbox, MFA will not process either Exchange mailbox retention policies or retention policies for that mailbox while the retention hold exists. To set a retention hold, set the `RetentionHoldEnabled` property for a mailbox as follows:

```
Set-Mailbox -Identity "Kim Akers" -RetentionHoldEnabled $True
```

When the user can resume working with their mailbox, it is usual to give them a week or so to allow them to process new messages awaiting their attention. You can then disable the retention hold by setting the `RetentionHoldEnabled` property to `$False`. MFA will then restart applying retention policies to the mailbox.

Moving Data Between Tenants

Content can have multiple policies controlling how it is retained or disposed of. These policies exist within a tenant but have no application elsewhere. Therefore, if you move content from a tenant, even to another

tenant, the effect of retention policies and labels disappear. This problem already exists when users move from on-premises environments to the cloud and the situation is similar in merger/acquisition scenarios when tenants join or split. The migration technology available from Microsoft does not take retention policies into account because the focus is on extracting information from one tenant to bring it to another. It is unlikely that Microsoft will change its approach due to the complexities of reconciling retention demands as content moves from one organization to another. Instead, they'll leave the problem to ISVs to solve in third-party migration products, some of which do a better job in this respect.

Some basic steps can be taken to help:

- Understand how data governance functions within the source tenant (or tenants, in the case of amalgamations). Know what retention policies exist and how those policies treat content.
- Prepare for the migration by understanding where data is stored after the move.
- Create a new data governance strategy for the target tenant.
- Execute the strategy as data is moved from source tenants so that it is managed from day 1. In other words, have the retention policies in place in the target tenant so that newly arriving content is preserved as soon as it is transferred. This task might take some PowerShell scripting.

Data subject to holds remains in the source tenant until its retention period expires. That is, the data is kept if the owning tenant is funded (licensed). In the case of tenant mergers, the source tenants will likely eventually close. At this point, any data kept due to retention policies will be removed from workloads.

Understanding the Exchange Mailbox Lifecycle

Items held in Exchange Online mailboxes follow a lifecycle from their creation by the user (calendar, posts, tasks, contacts, and so on) or when delivered as new messages. The major points in the lifecycle of Exchange Online items are:

- **Mailboxes** store and process incoming and outbound emails. Mailboxes can be archive-enabled to enable long-term retention of less-frequently accessed items for extended periods.
- The **Deleted Items** folder is the equivalent of the Trash or Wastebasket folder used by other email systems. The Deleted Items folder holds items that the user removes from other folders. Items stay in the Deleted Items folder until the user empties the folder or a retention policy dictates the removal of the items.
- Items removed from the Deleted Items folder move into **Recoverable Items**, a set of sub-folders used to preserve deleted items. The Recoverable Items folder also holds system items, such as audit entries to record actions taken within the mailbox. The Recoverable Items structure is not part of the normal IPM_SUBTREE folder tree exposed by clients. It is in the hidden part of the mailbox that clients never synchronize to local copies. The Recoverable Items folder structure is also known as the "dumpster". This term goes back to its first implementation allowing users to recover deleted items without the need for administrator intervention.
- The **Managed Folder Assistant** (MFA) is a background assistant that processes mailboxes regularly to remove items no longer needed from the Recoverable Items structure, remove items from other folders, and move items into folders in archive mailboxes. Retention policies applied to mailboxes control MFA's processing. Holds that might exist for those mailboxes constrain the removal of items until their retention period lapses.
- Administrators create **Retention policies and tags** to define how the MFA automatically manages mailbox items on behalf of users. A mailbox can have a single retention policy, consisting of a set of tags that apply to default folders (such as the Inbox and Sent Items folders), other folders and items as dictated by the user, and every other item in the mailbox (including the archive if available) that is not under the control of another tag.

- Administrators can apply different forms of **holds** (retention hold, legal or litigation hold, or in-place hold) to mailboxes to control whether users can remove information. Holds usually come about through a legal or other authorized action that forces a company to keep data for some purpose. When a mailbox is on hold, MFA will not permanently remove items that come within the scope of the hold from the mailbox, and Exchange Online copies any item that the user attempts to remove or update.

Collectively, these components interact with each other to form the lifecycle of Exchange Online mailbox items. Let's discuss what happens during the deletion of items to gain a better understanding of how the different parts of the lifecycle fit together.

Cleaning Mailboxes

Over time, users remove items from various mailbox folders. Some remove messages immediately after reading, and some keep everything and leave items to accumulate. Exchange uses a two-stage removal process. First, the item is "soft-deleted" and moves to the Deleted Items folder, a default mailbox folder that acts as a convenient collection point for any item removed from another folder. Then, if the user empties the Deleted Items, the items are "hard deleted" (sometimes called "purged") and moved to the Recoverable Items\Deletions folder. You can also assign a folder retention tag to the Deleted Items folder to govern how long items stay in the folder.

A user can force a "hard delete" for an item by using the *Shift+Delete* key combination in either Outlook or OWA. This command instructs Exchange to ignore the Deleted Items folder and move the item directly to the Recoverable Items\Deletions folder. Exchange also moves items into the Deletions folder when a user moves an item from a mailbox folder to a PST. The reason here is that the move is a combination of an item deletion from the mailbox folder and an item creation in the PST.

When a user soft- or hard-deletes an item, Exchange writes a pointer to the original folder into the item's Last Active Parent Folder Identifier property (the MAPI property is *LastActiveParentEntryID* or LAPFID). Knowing which folder an item originally came from allows OWA to restore the item into that folder using the **Recover Deleted Items** feature, even if the mailbox owner renames or moves the folder. Exchange Online has recorded LAPFID information since 2016, but some older items might not have a value stored in this property. If this is the case, OWA uses a scheme called "folder type origin" to figure out where to recover items.

Calendar items go back to the Calendar folder, Task items into Tasks, Contacts into Contacts, and mail and any other items go into the Inbox. It can be a little strange to find recovered items in the Inbox, especially if they are not mail items. For instance, if you recover a Word document or Excel spreadsheet (many people store these files in their mailbox), it shows up in the Inbox.

Outlook clients use a different mechanism to recover items. First, Outlook does not use the LAPFID to restore items. Second, Outlook recovers all items into the Deleted Items folder, the idea being that users can then decide the permanent location to move the items to. Table 16-5 summarizes the target recovery location used by Outlook and OWA for different types of items.

	Outlook	OWA
Mail item (message)	Deleted Items	Original folder or Inbox
Contact item	Deleted Items	Original folder or Contacts
Calendar item	Deleted Items	Original folder or Calendar
Task item	Deleted Items	Original folder or Tasks
Any other non-mail item	Deleted Items	Original folder or Inbox

Table 16-5: The recovery destination for various Exchange item types

If you remove a complete folder, you can recover the individual items within the folder, but you cannot recover the complete folder as a single entity.

Deletions, Purges, and Versions

The Recoverable Items structure uses sub-folders to organize items that it needs to keep. Some items stay until their deleted items retention period elapses. Others stay in the structure for a lot longer because one or more holds exist on the mailbox.

Items reach the Recoverable Items\Deletions folder when:

- They are hard-deleted.
- They are deleted from the Deleted Items folder.
- The Deleted Items folder is emptied.

Items stay in the Deletions folder for the period set in the deleted items retention period for the mailbox. In Exchange Online, the default period is usually 14 days. You can increase the deleted items retention period to a maximum of 30 days by running the *Set-Mailbox* cmdlet (and while you will probably use whole days, you can specify a retention time down to the second). For example:

```
Set-Mailbox -Identity 'Sanjay Patel' -RetainDeletedItemsFor 29.23.57.03
```

An exception exists for calendar items, which Exchange keeps for 120 days.

Recoverable Items Only Online. Because the Recoverable Items folder is only present on the server, you can only use Recover Deleted Items when Outlook can make a network connection to Exchange Online. In addition, if you ever need to use [the MFCMAPI utility](#) to see the items in the various sub-folders under Recoverable Items, you must configure MFCMAPI to open the message store online. Do this by going to the **Tools** menu, selecting **Options**, then setting the checkbox "Use the MDB_ONLINE flag when calling OpenMsgStore".

When the deleted item retention period expires for an item, MFA removes it from the database and the user can no longer recover the item. The exception to the rule is when a mailbox is on hold or has single item recovery enabled as Exchange then moves items into the Recoverable Items\Purges folder and keeps the items there until the hold or the single item recovery period lapse. During this period, administrators can recover items with a content search.

A user can try to remove an item permanently by using the Recover Deleted Items feature to select the item and then select **Purge**. What happens next depends on the *SingleItemRecoveryEnabled* setting for the mailbox. Exchange uses the Single Item Recovery (SIR) feature to ensure that a deleted item can be recovered during the longest possible time set by the deleted item retention period:

- If *SingleItemRecoveryEnabled* is *False* and the mailbox is not subject to a hold, Exchange removes the item from the database at once and it is irrecoverable. Mailboxes subject to a hold comply with the conditions of the hold(s).
- If *SingleItemRecoveryEnabled* is *True* (the default value) and the mailbox is not subject to a hold, MFA moves the item to the Recoverable Items\Purges folder. The item stays there until its deleted item retention period (between 14 and 30 days as defined for the mailbox) expires. At that point, MFA removes the item from the database and the item is irrecoverable. However, as discussed below, while this description is true, a retention policy might cause something different to happen.
- If *SingleItemRecoveryEnabled* is *True* and the mailbox is subject to a legal hold, Exchange moves the item into the Recoverable Items\Purges folder and keeps it there while the hold applies.
- If *SingleItemRecoveryEnabled* is *True* and the mailbox is subject to an in-place hold, part of MFA known as the Email Lifecycle Assistant (ELC) determines whether a copy needs to be retained to satisfy the hold criteria (query and date range). If this is the case, MFA moves the item to the Recoverable Items\DiscoveryHolds folder, where the item stays until the hold lapses. ELC examines items that have exceeded the deleted items retention period in mailboxes at least once a day.

Nothing moves to DiscoveryHolds: If you review items in the Recoverable Items structure, you might see that nothing ever moves into the DiscoveryHolds (or Purges) folder in the primary mailbox, even if those items are subject to an in-place hold. This can happen when the mailbox is under the control of the Default MRM Policy and is archive-enabled. Here is why.

When Exchange Online empties items from the Deleted Items folder or users hard-delete items, they end up in the Deletions sub-folder. Items in any folder under Recoverable Items are subject to the folder tag contained in the MRM policy, which instructs the Managed Folder Assistant to move the items to the archive after 14 days. If the mailbox is archive-enabled, the items are moved. If not, they stay in the primary mailbox.

ELC processes items when they reach the deleted items retention period. By default, this is between 14 and 30 days. ELC moves items subject to a hold to the DiscoveryHolds folder when their deleted items retention period expires. However, no items reach the 30-day deleted item retention period in the primary mailbox because they have already been moved to the archive. ELC processes the archive and will move the held items to the DiscoveryHolds folder in the archive, but no trace is seen of an item in the DiscoveryHolds folder in the primary mailbox. This can be confusing at first, but it is quite logical when you consider the age limits that control where items stay for different periods in a mailbox.

No client can permanently remove items under hold, including low-level utilities such as MFCMAPI. Exchange integrates checks for holds into how it manages data in its databases, and no one can circumvent the effect of a hold. Preventing the unauthorized removal of data from mailboxes allows Exchange to preserve items in an immutable fashion when needed by an organization.

Exchange monitors mailbox items that are subject to an in-place hold to detect if the user or any other process changes the item. If this happens, a copy of the original item is moved into the Recoverable Items\Versions folder to ensure that everything that happens to an item is fully recorded. This action is called a "copy on write". When the hold elapses, MFA removes the items from the Versions folder along with items held in the DiscoveryHolds and Purges folders.

The SearchDiscoveryHoldsFolder and SubstrateHolds folders: *SearchDiscoveryHoldsFolder* is a sub-folder of the DiscoveryHolds folder used by ELC when it processes the DiscoveryHolds folder to decide if it can remove any items. If ELC finds any items, it moves the items to *SearchDiscoveryHoldsFolder*. The items remain there until the Managed Folder Assistant eventually removes them. *SubstrateHolds* is another folder you'll find in Recoverable Items. This folder holds copies of original items after a user deletes or edits items

under hold (by an in-place hold, litigation hold, or retention hold). Once again, items in *SubstrateHolds* remain until the Managed Folder Assistant determines that it's safe to remove the items.

Recoverable Items Quota

The Recoverable Items structure has a separate storage quota from that given to the primary mailbox. If a mailbox is archive-enabled, a separate quota is available to a similar Recoverable Items structure in the archive mailbox. The default quota for recoverable items is 30 GB, and Exchange Online increases the quota to 100 GB automatically when it applies the first hold to a mailbox. Mailboxes created when org-wide holds exist in the organization, have their recoverable items quota set to 100 GB. Between the primary and archive mailbox, Exchange can keep up to 200 GB of recoverable data for a user. Items stored in the Recoverable Items folder in the archive behave in the same manner as if they were in the primary mailbox and are discoverable by eDiscovery searches.

You cannot change the *RecoverableItemsQuota* for a mailbox with the EAC or PowerShell, but you can log a support case with Microsoft Support if a mailbox is likely to exhaust its recoverable items quota. To find out how much data exists in Recoverable Items for a mailbox, use either of the *Get-MailboxStatistics* or *Get-MailboxFolderStatistics* cmdlets:

```
Get-ExoMailboxFolderStatistics -Identity Kim.Akers -FolderScope RecoverableItems | Format-Table
Name, FolderSize, ItemsInFolder, FolderAndSubFolderSize -AutoSize
```

Name	FolderSize	ItemsInFolder	FolderAndSubfolderSize
Recoverable Items	0 B (0 bytes)	0	563.3 MB (590,650,854 bytes)
Audits	523.1 MB (548,504,424 bytes)	149324	523.1 MB (548,504,424 bytes)
Calendar Logging	18.37 MB (19,261,189 bytes)	734	18.37 MB (19,261,189 bytes)
Deletions	10.72 MB (11,236,121 bytes)	115	10.72 MB (11,236,121 bytes)
DiscoveryHolds	0 B (0 bytes)	0	0.B (0 bytes)
SearchDiscoveryHoldsFolder	0 B (0 bytes)	0	0 B (0 bytes)
Purges	5.707 MB (5,984,254 bytes)	753	5.707 MB (5,984,254 bytes)
Versions	5.402 MB (5,664,866 bytes)	53	5.402 MB (5,664,866 bytes)

Add the *Archive* switch to the cmdlet parameters if you want to see data for the archive mailbox.

If the mailbox exceeds the Recoverable Items quota:

- The user cannot remove items from their mailbox.
- The Managed Folder Assistant cannot move (hard-delete) items into the Recoverable Items.
- Copy on write cannot create copies if users alter items subject to a litigation or in-place hold.
- Exchange cannot save audit items if mailbox auditing applies to the mailbox.

Three actions are available to restore the Recoverable Items folder to normal working order. First, you can ask Microsoft support to increase the recoverable item quota for the problem mailboxes. This might take a day or so to be effective and during that time the mailbox might experience problems such as those listed above. The second solution is to run the Managed Folder Assistant and instruct it to clean up duplicate items that might be present in Recoverable Items. This step should have an immediate effect and restore the mailbox to good health. To run the Managed Folder Assistant in clean-up mode, use a command like this:

```
Start-ManagedFolderAssistant -Identity Kim.Akers -HoldCleanup
```

Check the reported data for the Recoverable Items folder after the Managed Folder Assistant completes and you should discover a reduction in the folder size. For more information about how to track what the Managed Folder Assistant does, see the section "Logging the Managed Folder Assistant" later.

The last action is to follow [the procedure laid down by Microsoft](#) to use PowerShell to clean up Recoverable Items.

Exchange Mailbox Retention Policies

As we know, retention policies allow administrators to control how long data workloads retain or remove data. Both Exchange Online and Exchange on-premises servers support mailbox retention policies. Although these policies only cover Exchange mailboxes, they are still important where tenants want to impose the same retention regime for both online and on-premises mailboxes. In addition, mailbox retention policies can apply control at the level of individual folders instead of applying the same settings to a complete mailbox. Finally, mailbox retention policies can move items to archive mailboxes, something that is still not possible with Microsoft 365 retention policies.

Mailbox retention policies instruct the Managed Folder Assistant (MFA) about how long users can keep mailbox content (the retention period) and what to do once the retention period lapses (the retention action). The choice for retention action is to either remove the item (recoverable or permanent) or move it to the archive mailbox. A mailbox can have only one retention policy, and often the mailbox receives this policy when created through the application of mailbox plan settings (see the Exchange Online chapter). Many mailbox retention policies can exist within a tenant to ensure that the needs of different user groups are met.

A mailbox retention policy consists of one or more tags. These are:

- Tags for the default mailbox folders (**folder tags**): Among the default folders are the Inbox, Sent Items, and Deleted Items folders. Folder tags control how long items remain in these folders and what happens once the retention period elapses. Items in folders with folder tags inherit these tags unless the mailbox owner assigns them a personal tag.
- **Personal tags:** Users can apply these tags to any mailbox item and any folder except an Exchange default folder. A personal tag always has precedence over any other tag.
- **Default tags:** A mailbox retention policy can include a default delete tag and a default archive tag. The first determines the deletion of items not under the control of a folder or personal tag. The second determines when MFA moves items into the archive.

A mailbox retention policy commonly contains several folder tags, some personal tags, and one or both default tags.

How MFA Processes Retention Policies

MFA processes both Microsoft 365 retention policies and mailbox retention policies against mailboxes. When MFA processes a mailbox to apply a retention policy, it examines the mailbox to "stamp" folders and items according to policy settings. MFA updates several MAPI properties for mailbox items with information, including:

- A GUID for the retention policy. Administrators can update the display name of a name, but its GUID (the retention identifier) is immutable.
- Retention period. The number of days that an item can stay in the folder before MFA removes it.
- Retention expiry. The calculated date when MFA will remove an item.
- Retention flags, including whether the item inherits the retention tag from the parent folder, or a user assigned the tag to the item.
- Archive period. The number of days that an item can stay in its folder before MFA moves it into the archive.
- Archive date. The calculated date when MFA will move an item to the archive.

When moving items into the Deleted Items folder, MFA makes sure that it does not remove items with Purview retention labels before the expiration of their full retention period. This applies even when the Deleted Items folder has a default folder tag or when items receive labels through an auto-label policy. For example, if a user deletes a message with a retention label with a retention period of 365 days, Outlook moves

the item into Deleted Items. Let's assume that Deleted Items has a 30-day folder retention tag. Normally, MFA hard-deletes items from Deleted Items after 30 days, but because the item's retention label dictates a 365-day retention period, the item remains in Deleted Items until that period elapses.

In addition to processing normal messages, MFA can process compliance records for Teams, Viva Engage, and Planner. If a mailbox only has a mailbox retention policy, MFA ignores the compliance records. If it has a Microsoft 365 retention policy, MFA processes the compliance records for Planner along with other mailbox content. Special Microsoft 365 retention policies apply to Teams compliance records and Viva Engage compliance records.

Logging the Managed Folder Assistant

You can use the `Export-MailboxDiagnosticLogs` cmdlet to find out the last time that the Managed Folder Assistant processed a mailbox and what happened during the run. The "Elc" (Electronic life cycle) properties in the report contain details of MFA activity. For example, the `ElcLastRunSuccessTimeStamp` tells you the date and time that MFA last successfully processed the selected mailbox while `ElcLastRunDeletedFromDumpsterItemCount` holds the total number of items removed from the Recoverable Items folder (the famous "dumpster"). In this truncated version of the output, we can see the last successful run of the assistant was at 23:43 on 4 June 2023 and that MFA removed 2 items (from all folders under the mailbox root) and moved 63 items to the archive.

```
$Log = Export-MailboxDiagnosticLogs -Identity James.Ryan -ExtendedProperties
$xml = [xml]($Log.MailboxLog)
$xml.Properties.MailboxTable.Property | Where-Object {$_.Name -like "ELC*"} |
```

Name	Value
----	-----
ElcLastRunTotalProcessingTime	127725
ElcLastRunSubAssistantProcessingTime	106198
ElcLastRunUpdatedFolderCount	76
ElcLastRunTaggedFolderCount	0
ElcLastRunUpdatedItemCount	105
ElcLastRunTaggedWithArchiveItemCount	0
ElcLastRunTaggedWithExpiryItemCount	99
ElcLastRunDeletedFromRootItemCount	2
ElcLastRunDeletedFromDumpsterItemCount	0
ElcLastRunArchivedFromRootItemCount	63
ElcLastRunArchivedFromDumpsterItemCount	0
ELCLastSuccessTimestamp	04/06/2023 23:43:47
ElcLastRunSkippedNoTagItemCount	0
ElcLastRunSkippedWithTagItemCount	0
ElcLastRunSkippedNotExcludedItemCount	0
ElcFaiSaveStatus	SaveSucceeded
ElcFaiDeleteStatus	DeleteNotAttempted

MFA Workcycle

MFA runs on a workcycle basis where a goal is set and the server hosting the mailbox figures out how to meet the goal, taking system load and available resources into account. In an on-premises deployment, the MFA workcycle aims to process every mailbox at least once daily. However, in Exchange Online, the workcycle used for the MFA aims to process every mailbox at least once weekly. The larger quotas granted to Exchange Online mailboxes is one reason why it is safe to extend the workcycle. However, although the formal workcycle goal is weekly, experience (and observation of mailbox statistics as described above) proves that MFA can process mailboxes up to five times weekly. If system resources are available, Exchange Online releases the resources to background processes like MFA, and this accounts for any discrepancy between formal workcycle goals and what happens in practice.

Knowing how to check whether MFA has processed a mailbox, we can write some code to check all user mailboxes. It's easy to amend this code to select a different group of mailboxes for processing, such as all

those belonging to a department. In addition, the script only reports two of the ELC properties and you could add others as needed, such as the count of items moved to an archive mailbox.

```
[array]$Mbx = Get-ExoMailbox -RecipientTypeDetails UserMailbox -ResultSize Unlimited | Sort-Object
$Report = [System.Collections.Generic.List[Object]]::new()
ForEach ($M in $Mbx) {
    $LastProcessed = $Null
    Write-Host "Processing" $M.DisplayName
    $Log = Export-MailboxDiagnosticLogs -Identity $M.Alias -ExtendedProperties
    $xml = [xml]($Log.MailboxLog)
    $LastProcessed = ($xml.Properties.MailboxTable.Property | Where-Object {$__.Name -like
    "*ElcLastSuccessTimestamp*"}).Value
    $ItemsDeleted = $xml.Properties.MailboxTable.Property | Where-Object {$__.Name -like
    "*ElcLastRunDeletedFromRootItemCount*"}
    If ($LastProcessed -eq $Null) {
        $LastProcessed = "Not processed"
    }
    $ReportLine = [PSCustomObject]@{
        User      = $M.DisplayName
        LastProcessed = $LastProcessed
        ItemsDeleted = $ItemsDeleted.Value}
    $Report.Add($ReportLine)
}
$Report | Select-Object User, LastProcessed, ItemsDeleted
```

Forcing MFA to Process a Mailbox

If you need the Managed Folder Assistant to process a mailbox urgently, for instance, to publish updated retention policy information to a mailbox, run the *Start-ManagedFolderAssistant* cmdlet:

```
Start-ManagedFolderAssistant -Identity "Ben Owens"
```

If you apply a different retention policy to a mailbox and want the retention tags in the new policy to become effective as quickly as possible, use the *FullCrawl* parameter.

```
Start-ManagedFolderAssistant -Identity "Ben Owens" -FullCrawl
```

Sometimes starting the MFA processes a mailbox immediately, sometimes it does not. Exchange Online throttles background processing and does not allow mailbox assistants like MFA to run on demand. Microsoft wants to smoothen server load to reduce the risk that background processing interferes with the ability to be responsive to clients, which is why a seven-day workcycle exists for mailbox assistants. Telling MFA to process a mailbox has an effect if MFA considers that it has not processed the mailbox recently. Running *Start-ManagedFolderAssistant* several times to convince MFA to start processing is a fruitless exercise.

The *Start-ManagedFolderAssistant* cmdlet supports an *-InactiveMailbox* switch to force immediate processing of inactive mailboxes. MFA applies Exchange mailbox retention policies and retention policies to the content in inactive mailboxes. One difference exists in the processing done for active and inactive mailboxes in that MFA does not process archive tags when it deals with inactive mailboxes.

Stopping MFA Processing a Mailbox

It can happen that you want to stop the Managed Folder Assistant from processing one or more mailboxes. For example, when you want to remove items from a mailbox when it is on hold because that information should not be in the mailbox as when someone forwards a message with confidential information to mailboxes that should not receive them. To remove the items from a mailbox that is on hold, you must release the holds temporarily, remove the items, and then replace the holds. During this time, MFA might process the mailbox and remove other items. To stop this from happening, you can disable MFA temporarily by running the *Set-Mailbox* cmdlet to set the *ElcProcessingDisabled* flag.

```
Set-Mailbox -Identity "Kim Akers" -ElcProcessingDisabled $True
```

When the holds are in place again, you can reverse the process and release MFA by switching the value to `$False`. You cannot disable MFA processing if a preservation lock applies to the mailbox.

Moving from Exchange Retention Policies

Exchange mailbox retention policies have been in use since Exchange 2010. Microsoft's long-term direction is to move away from workload-specific processing, like that done by mailbox policies, to use retention policies instead, whenever it makes sense for a tenant. If you are a new tenant starting with a retention strategy, the right decision is to use retention policies. However, if you have been using mailbox retention policies for many years and have a hybrid tenant, that decision is not quite so clear-cut.

To make retention policies available to other workloads, Microsoft evolved and expanded the core principles behind Exchange retention policies. In doing so, they have dropped some Exchange-specific features, like the ability to move items to archive mailboxes. Losing the ability to archive items automatically is regrettable but this action is only valid for Exchange and does not apply to other applications. A more fundamental problem for some is the loss of granularity in that an Exchange retention policy can include tags for default folders, personal tags, and a set of default tags to control deletion, archival, and voicemail. By comparison, a retention policy applies the equivalent of a single default tag (to remove or keep content) to mailboxes.

Retention policies create in-place holds when they include a retention action. The holds apply for all locations covered by a policy and last until the policy's retention period expires, meaning that users cannot remove content from Exchange, SharePoint, OneDrive for Business, Teams, or Groups if that content comes within the scope of the policy. The integration of in-place holds into retention policies is an advantage over Exchange mailbox retention policies.

Significant differences in functionality exist between the two types of retention policies. The most attractive feature of retention policies is that they apply to many locations rather than just Exchange Online. Another good point in their favor is that you can combine Exchange retention policies with retention policies and labels, even if that might be a double-edged sword in terms of the resulting complexity in retention processing. Being able to apply a single consistent policy across multiple workloads is a huge advantage, but the loss of some of the granular processing available in Exchange retention policies reduces its impact. The decision to move to retention policies therefore needs considerable preparation.

Every tenant is different and although it might be easy for a cloud-only tenant with relatively simple retention needs to go ahead and embrace retention policies, the situation is probably very different for large and complex tenants that already have a well-defined retention strategy in place. Things become even more complicated for hybrid tenants, who often want to use the same processes on-premises and in the cloud.

Experience and time will allow us to develop better answers. In the meantime, new tenants should start with retention policies and labels while older tenants test, compare, and contemplate what is their best course of action. For instance, you might decide on a strategy based on four stages:

1. Remove personal tags from Exchange Online mailbox retention policies and replace the tags with Microsoft 365 retention labels with the same name and retention settings. Users will begin using the retention labels to retain new items while the older retention tags will age out over time.
2. Remove folder tags from Exchange Online mailbox retention policies and replace them with Microsoft 365 retention policies. This means that no folder-specific retention processing is available because the retention policies apply the same settings and actions to the complete mailbox.
3. Replace default deletion tags in Exchange Online mailbox retention policies with Microsoft 365 retention policies. This is a natural consequence of step 2 and the only action required once a Microsoft 365 retention policy processes mailboxes is to remove the default deletion tag from the mailbox retention policy.

4. Eventually, limit the use of Exchange Online mailbox retention policies to moving items to archive mailboxes. When Microsoft 365 retention policies support this action, you can remove the default archive tags from Exchange Online mailbox retention policies.

This is an outline of tactics to move to Microsoft 365 retention policies that need to be adjusted to meet the unique circumstances of individual organizations. For example, you should run Exchange Online mailbox retention policies (with all tags intact) and Microsoft 365 retention policies alongside each other for a few weeks or so to make sure that no interregnum happens when retention processing does not occur for mailboxes. MFA will resolve any inconsistencies (such as having a personal tag and retention label with the same name).

The availability of the older workload-specific functionality allows organizations time to make the transition. It's a wise approach because the nature of retention is that items often require retention for long periods, and no one wants software to force them to change their data governance strategy in such a way that it might affect terabytes of retained content.

Communication Compliance

[Microsoft Purview Communication Compliance](#) is part of the Microsoft 365 Insider Risk solution set. These policies are the third iteration of functionality designed to help organizations monitor communications sent and received by employees. The normal reason why an organization wants to monitor communications is to reduce the potential for risk due to mistakes or deliberate actions by employees in their internal and external communications. The loss caused by inappropriate or illegal communications might be reputational or financial. Either way, it's undesirable, especially for large enterprises, which is why organizations want to proactively detect any potential problems and then prove that they are on top of the situation should the need exist to demonstrate this point to regulators or other corporate bodies.

Although it might seem sneaky and reminiscent of a "big brother" approach to employees, certain industries have regulations that force companies to ensure that they have a supervision policy in place, perhaps only for employees that work in specific areas. For example, [FINRA](#), the U.S. Financial Industry Regulatory Authority, enforces rules governing the activities of brokers and dealers to ensure market transparency and fairness. It was common to find that on-premises organizations created special software called "transport sinks" to capture and examine messages sent between employees. The code ran in the Exchange transport pipeline to examine and capture copies of messages and route the copies to personnel skilled in regulations and compliance, who reviewed the traffic to ensure that no problems exist. Companies often combined transport sinks with transport rules to control how certain groups of users communicated with each other.

Organizations using communication compliance policies must have Office 365 E5, Microsoft 365 E5, or Microsoft 365 E5 Compliance for all accounts covered by the policies.

Reviewing Microsoft 365 Communications

Communication compliance policies set guidelines for acceptable internal and external communications. In a Microsoft 365 context, communications mean:

- Exchange Online email.
- Teams personal chat and channel communications, including messages sent by users with on-premises mailboxes and messages in shared channels. The Teams messages reviewed by communication compliance policies are the compliance records captured by the Microsoft 365 substrate and used for eDiscovery (see the Teams management chapter for more information).
- Conversations in Viva Engage communities.
- Messages imported from an external source [through a connector](#) like Bloomberg messaging.

Communication compliance policies depend on messages stored in Exchange Online. Background agents check mailboxes to scan for policy violations in normal messages and the compliance records captured for Teams chat and channel conversations (including records for conversations with external users in other tenants and Skype consumer users).

When the agents detect violations, they copy messages to special mailboxes to make them available for review and resolution. This isn't a real-time process, and you can expect a delay of approximately an hour before policies detect and flag problem messages for review. In most cases, this isn't a problem because compliance checking is a reactive process. In any case, it's usual that policies select only a percentage of detected messages for review, so not every message that could contain a violation will turn up in the portal for review.

Components of a Communication Compliance Policy

Communication Compliance policies are managed through the Microsoft Purview Compliance portal. A policy includes the following components:

- **Reviewees:** The people (individuals or groups) whose communication come within the scope of the communication compliance policy. You can use email distribution lists or Microsoft 365 groups to define the reviewees for a policy. You can't use dynamic groups or dynamic distribution lists to define reviewees. From February 2023, communication compliance policies support adaptive scopes to define the set of reviewees for a policy.
- **Locations:** Define the workloads monitored by the policy, including Exchange, Teams, and Viva Engage.
- **Conditions:** Define the characteristics of communication items policies examine to detect policy violations. The conditions include:
 - Internal communication between the monitored accounts.
 - Sensitive information types as used elsewhere in Microsoft 365, as in Data Loss Prevention policies.
 - Classifiers, both those provided by Microsoft to match content such as personal resumes and, source code or those that look for content that indicate a type of user behavior like money laundering or bribery. The tenant can create and use trainable classifiers to match items commonly used by the business.
 - Message properties such as message size, attachment type and size, originating domain, and sensitivity label.
- **Sample size:** The percentage of messages which meet the policy conditions captured for review.
- **Reviewers:** The people who will access the items captured for review to decide whether the content of those items complies with the regulations in force. Reviewers process captured items through the Compliance portal and decide whether items are compliant or non-compliant. In the latter case, reviewers can then escalate the situation to the offending user's manager, HR, or some other department for resolution.

An organization can deploy multiple communication compliance policies within their tenant, each of which monitors a set of users. With the structure of a policy in mind, before you can create a new policy, you should answer the following questions:

- What set of users come within the scope of the policy? How is the target set identified?
- Communication between users includes a vast variety of content. How do we focus on the messages for review? For example, are we looking for a specific codeword or terms?
- What is an adequate sample for review? A policy might review 100% of detected messages during the testing or initial deployment phase of deployment to make sure that the conditions specified for the policy are accurate and not too broad. After reaching this point, it's usual to reduce the percentage to

10% or so to lessen the load on reviewers. Experience with supervision policies proves that selecting too high a percentage can generate so many items that reviewers cannot cope with the volume and turnaround reviews in a reasonable time.

- Who will examine the captured traffic? The reviewers need to understand what constitutes a problem when they see it in a message. They also need to understand what is a serious violation that needs immediate action and what is not so serious. Reviewers do not have to be fluent in all the languages used for communications because Microsoft Translator can translate messages into a reviewer's preferred language.
- What happens when a violation occurs? All violations have consequences, but some violations have more grave consequences than others. The organization might require an escalation process to allow reviewers to escalate violations to a higher authority for a decision about how to handle a matter, including potentially reporting a case to a regulatory authority.
- User awareness. Before the tenant begins to monitor communications, it is only fair to inform the users whose communication is under review about potential violations and the consequences if a policy detects a problem that proves to be a real issue. This is an area where the company's legal and HR departments have a key role to play.

After determining the answers to these questions, you can go ahead and create a policy, assuming your account holds the right roles.

Communication Compliance Role Groups

Five role groups support granular management of communication compliance policies and the data captured by policies:

- **Communication Compliance:** Includes all the other communication compliance role groups.
- **Communication Compliance Administrators:** Manages communication compliance policies.
- **Communication Compliance Analysts:** Can view communication compliance message metadata to analyze the effectiveness of policies.
- **Communication Compliance Investigators:** Can view the full body of messages detected by communication compliance policies.
- **Communication Compliance Viewers:** Allows access to communication compliance reports and widgets.

The Communication Compliance role might be the only one used in smaller tenants. The other roles exist to allow granular assignment of permissions to specific people to do certain tasks. For more information, see [this page](#).

Workflow Considerations

Communication compliance includes simple workflow processing (what Microsoft calls "*flexible remediation workflows*") to help track and resolve violations, mostly by the dispatch of emails to offenders and their managers and recording the outcome. For the most serious cases, communication compliance is integrated with Microsoft 365 Advanced eDiscovery, allowing for information gathered about violations to be transferred to eDiscovery as prepackaged cases for further investigation and resolution.

Thought must be put into how to integrate what's available in the application to complement and build on existing HR procedures. For instance, what should happen upon the detection of a violation by an employee? And what escalation steps happen if someone proves to be a serial offender? These are decisions that Microsoft can't make because every company is different. The implementation of employee monitoring is highly dependent on the industry the organization works in and the applicable regulations.

Machine Learning and Classifiers

Communication compliance policies can include classifiers to detect types of information. Microsoft 365 uses a variety of classifiers for different purposes and tenants can create their own by going through a training process. During this process, machine learning processes sets of sample documents to build a map of common characteristics that solutions can use to detect the content of the same type. The prepackaged classifiers include:

- Offensive language (now deprecated).
- Profanity.
- Resumes (CVs).
- Source code.
- Targeted harassment.
- Threat.
- Adult images.
- Gory images.
- Racy images.
- Sexual harassment.

Microsoft's text-based classifiers can handle multiple languages (the set grows over time), including English, French, German, Italian, Japanese, Arabic, Dutch, Korean, Spanish, Portuguese, and Chinese (including Chinese traditional). Image-based classifiers are language-independent. Images examined by these classifiers can be in JPEG, GIF, BMP, and PNG formats.

Having classifiers makes it easier for tenants to monitor communications based on well-known and well-understood characteristics. For instance, if someone tells another person that "I hate you," the harassment classifier will recognize the "hate" keyword and the context of its use. Using classifiers and machine learning helps communication compliance policies generate fewer false positives than supervision policies do. We will probably never have zero false positives but eliminating most of these reports eases the load on reviewers.

Even the best machine learning detection experiences problems with the way language flex and evolves. One person's offense is another person's norm, which makes it imperative that reviewers consider messages selected for review in context. For instance, a [scatological reference](#) about someone in an email or Teams chat might be innocuous or offensive, depending on how it is phrased. And calling someone a pile of brown smelly bovine output is likely to pass most machine learning tests. The evolving use of language and the variation of acceptance of different terms can cause many false positives, which is one of the reasons why Microsoft deprecated the offensive language classifier and replaced it with a combination of threat, profanity, and harassment qualifiers, each being more focused and therefore more likely to generate a correct result.

Anonymized Results

Communication compliance settings include the option to see anonymized usernames (like *Anony10-lbb*) instead of the real display names of users who cause policy matches. You might prefer to select this setting to preserve user privacy during the initial phases of potential violation reviews and investigations.

Creating a New Communication Compliance Policy

You can create a new policy from scratch, or you can use one of the template policies provided by Microsoft. Here are some of the standard template policies:

- **Financial Compliance:** looks for entries in a custom lexicon of words that might indicate violations if present in messages between a specific group of accounts. Internal teams responsible for monitoring regulatory compliance probably deal with violations of this nature.

- **Sensitive Information:** looks for the presence of sensitive information types in messages (Microsoft 365 includes many sensitive information types covering anything from passport numbers to social security numbers). Violations of this policy are like those encountered in Data Loss Prevention processing.
- **Conflict of interest** looks for evidence in communications between users or groups of actions that conflict with the interests of the company.
- **Inappropriate text** uses built-in classifiers to detect text in messages that the organization might consider inappropriate, abusive, or offensive. An example of country-level regulations in this area is [Japan's "power harassment" law](#), which took effect for large companies on 1 April 2020.
- **Inappropriate images** detects adult or "racy" images.
- **Inappropriate content** uses built in qualifiers to detect when people include inappropriate text, such as violence, hate or sexual language in Exchange messages, Teams chat and channel conversations, Viva Engage private messages and community posts, and Microsoft 365 Copilot interactions.
- **Microsoft 365 Copilot interactions** detects when people use sensitive information types or trainable qualifiers in Copilot prompts.

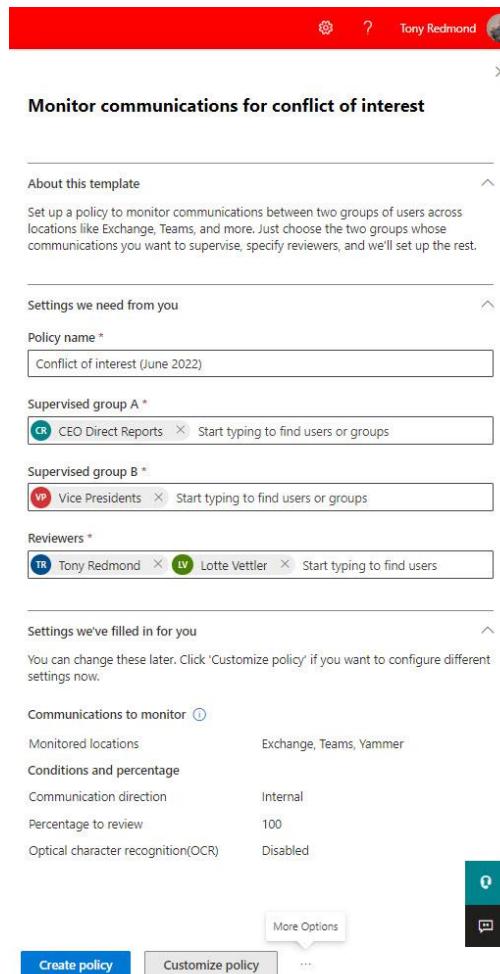


Figure 16-21: Creating a new communication compliance policy

The template policies cover (at least in part) many of the scenarios that create the need to monitor communications, so the quickest way to get going is to create a new policy from a template and amend it afterward to meet your needs. The Inappropriate text template is a good example to start with because it's easy to generate some sample messages for the policy to capture. To create a new policy, click **Create policy** and choose *Detect inappropriate text* from the drop-down list. Several policy settings are pre-populated from

the template, and all you need to do at this point is change the policy name (if you want) and add the users or groups to supervise and the reviewers.

In Figure 16-21, we see the screen used to collect details of the new policy. A distribution list defines the sets of users to monitor, and we've appointed a single reviewer. It's usually best to have more than one reviewer per policy. When you go ahead and create the policy, some background processes run to create the special mailbox used to collect items for review and inform the communications monitoring assistants that a new policy is active. It can take up to an hour for this process to complete setup and a further 24 hours before the assistants begin to monitor messages.

Tweaking a Communication Compliance Policy

When you create a policy from a template, you can only change certain policy settings until the setup has finished. If you want access to all policy settings during creation, choose to create a custom policy. Once setup is complete, you can tweak the policy to make it more effective. Common changes include:

- Extend the scope of the policy to include additional users or groups, or to make it apply to all users. You can also use adaptive scopes to define the set of users covered by a communications compliance policy.
- Exclude selected users from the policy.
- Select the locations to monitor. By default, the policy covers Exchange and Teams. Viva Engage is only available when the tenant network is in native Microsoft 365 mode.
- Select the direction of communications to monitor. By default, policies check all communications:
 - **Inbound:** communications to the recipients specified in the policy from users who do not come under the scope of the policy. Traffic can come from other users within the organization or people outside the organization.
 - **Outbound:** communications from the people specified in the policy to anyone else.
 - **Internal:** communications between the people included in the policy.
- Amend the policy rules used to detect violations. If you're used to working with data loss prevention rules, you'll find the process very similar.
- Change the percentage of messages to review from the set detected to contain violations.

You can also exclude bulk mail (like newsletters) to reduce the number of false positives detected by policies.

Figure 16-22 shows the conditions generated for a policy created from the *Inappropriate text* template. As you can see:

- Communications are monitored in all directions.
- Three classifiers are used to identify potential violations. The combination of these classifiers should catch messages containing profane, threatening, harassing, or offensive language subject to the caveats expressed above.
- 100% of all matching messages are selected for review.

You could add more conditions to improve the effectiveness of the checking. Policies focused on language could be improved by adding a condition to check for particular words or terms that the classifiers might not catch, such as new slang or a word used in known cases of harassment. Other policies will depend on checking for:

- A lexicon of specific words that might indicate suspicious or problematic behavior.
- Microsoft 365 sensitive information types (social security numbers, credit card numbers, and so on) and custom sensitive information types defined by the tenant.
- Message properties. These include:
 - Specified words or phrases appear in the message body (or its subject). Use KeyQL syntax to define the query, but do not try to get too complex. Alternatively, you can add a condition that

checks for messages where the specified words are not present. You will see an error if the specified query is too complex for a supervision policy.

- Any attachment to the message includes or does not hold the specified words or phrases.
- The message has an attachment of a specific type or does not have an attachment of a specific type.
- An attachment is larger than a specified size (in KB, MB, or GB).
- The overall message size is larger than the specified size.
- Messages are sent to or received from a specific domain.
- Messages have a certain sensitivity label.

Once ready, click **Next** and **Save** to save the updates to the policy. Once again, it will take up to a day before the new policy settings are effective.

Communication compliance > **Edit Identify Bad Words Used by Senior Management**

Choose conditions and review percentage

Communication direction *

- Inbound.** Sent to users you choose to supervise from people not included in this policy.
- Outbound.** Sent from the users you choose to supervise to people not included in the policy.
- Internal.** Sent between the users or groups you identified in this policy.

Conditions

By default we will monitor all communications from the users and groups you specified. Add conditions to limit the results to communications matching specific criteria. Learn more about these conditions

Content matches any of these classifiers

Classifiers	Actions
Targeted Harassment	<input type="button" value="Delete"/>
Profanity	<input type="button" value="Delete"/>
Threat	<input type="button" value="Delete"/>
Add <input type="button" value="▼"/>	

Review percentage

If you want to reduce the amount of content to review, specify a percentage. We'll randomly select the amount of content from the total that matched any conditions you chose.

100%

Buttons: Back, Next, Cancel, Need help?, Give feedback

Figure 16-22: Amending conditions and sample percentage for a communication compliance policy

Supervision Mailboxes

Communication compliance policies use special supervision mailboxes to store the copies of messages captured by the background agents for review. These hidden mailboxes can't receive email, and don't appear in any Microsoft 365 administrative interface except PowerShell, where you can run the `Get-SupervisoryReviewPolicyV2` cmdlet from the compliance module to reveal the name:

```
Get-SupervisoryReviewPolicyV2 "Regulatory Compliance" | Format-Table reviewmailbox
```

```
ReviewMailbox
```

SupervisoryReview{d7c6eb96-20e5-4ccb-9838-2d230f64efb1}@office365itpros.onmicrosoft.com

Reviewing Captured Messages

The task of a policy reviewer is to examine captured items to decide whether any compliance violation exists. Do not underestimate the amount of work involved in processing several hundred review items, a volume that a busy tenant can easily generate daily. Apart from the opening and reading of each item, the reviewer must understand the context of the communication and how the content fits with regulations. Hours of work might be consumed to process items at a high level of accuracy.

To review messages, navigate to the Communication compliance section of the Compliance portal where you can see a list of the policies and statistics for each policy (Figure 16-23). Policies generate an alert any time processing detects four violations within 60 minutes.

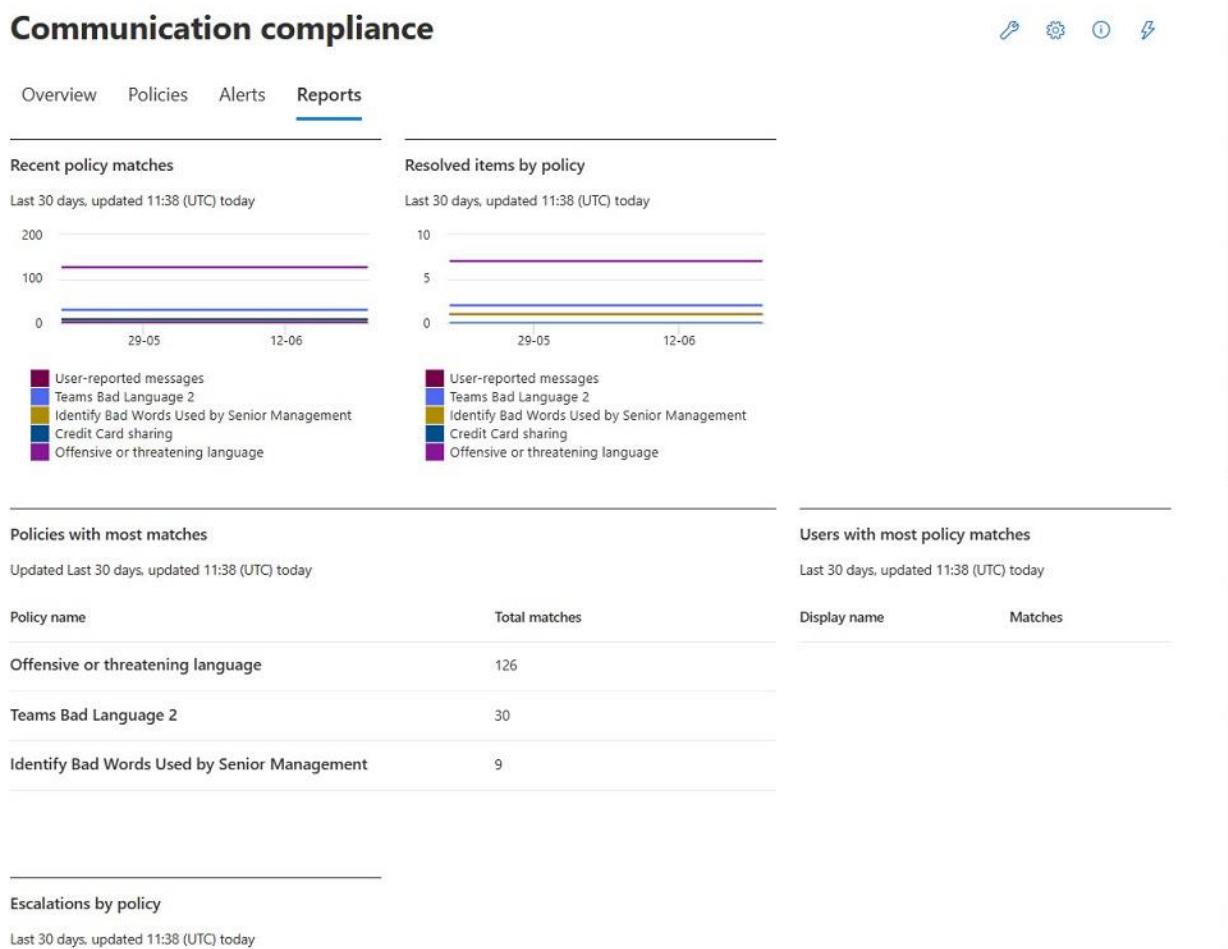


Figure 16-23: Statistics for communication compliance policies

To check waiting items, go to the Policies tab, select a policy, and click the *Pending* link. The items pending review can be filtered to focus on specific recipients, senders, domains, item types, subjects, and other properties. Items can then be grouped by family (for instance, show all email together) or by conversation, which assembles the messages in a Teams or email conversation (like a Teams meeting recording transcript) to allow the reviewer to see how an interaction unfolds. This is important because a remark taken out of context can look quite different when considered amid a full conversation.

The reviewer can then examine items to decide if a violation is present. The Compliance portal offers several views:

- **Source:** View an item as the user sees it.
- **Plain text:** Strip away all the formatting to show plain text with line numbers. This helps to focus on the words without the distraction of other elements.
- **Conversation:** Show the individual message containing the violation in context within the conversation where it occurred. Up to five messages before and after the offending item are available.
- **User history:** Show previous instances when the user had policy violations.

In addition, the reviewer can see the user history to know if the sender of the message has previous violations for the same behavior. First-time offenders often receive more flexibility and understanding than serial offenders do. If the reviewer needs to download an item, they can do so as a message item or PDF.

The item selected for review in Figure 16-24 is a Teams message detected as containing some offensive text. The user history shows that the person sending the message has some other outstanding policy matches awaiting review. This might indicate that some corrective intervention is necessary to help the person modify the text they use in messages. It's likely that reviewers make the decision after checking each of the policy matches to understand the ebb and flow of the conversations and the context of the text detected as policy violations.

The screenshot shows the Microsoft 365 Compliance Center interface. At the top, there's a navigation bar with 'Communication compliance > Policies > Teams Bad Language 2'. Below the navigation is a filter section with 'Pending (32)', 'Resolved (2)', and 'Exports' buttons. There are also 'Filter' and 'Reset' buttons. The main area displays a list of items under 'Subject line'. One item is selected, showing a tooltip: 'Pattern detected. Recently, Vasil Michev (MVP) sent 4 messages matching this policy's conditions to Tony.Redmond@redmondassociates.org.' Below the list, there's a section for 'Recent policy matches and remediation actions' showing '4 Policy matches' and '0 Remediation actions'. At the bottom, there are buttons for 'Resolve', 'Summarize', 'Notify', 'Tag as', and 'Escalate', along with a dropdown menu for escalation actions: 'Escalate for investigation', 'Remove message in Teams', and 'Automate'.

Figure 16-24: Reviewing pending items for a communication compliance policy

The steps that a reviewer can take to progress an item include:

- **Resolve:** Mark the item as resolved, perhaps after some invention. This action removes the item from the pending list. Eventually, the aim is for reviewers to resolve all items on the pending list. If an item was misclassified, you can resolve it by marking it as misclassified and optionally send a copy of the item to Microsoft to help train its models. If cross-policy resolution is enabled (the default setting), resolving a message for one policy resolves it for any other policy that detected the item as a possible violation. Cross-policy resolution is enabled or disabled in Communication compliance settings.

- **Summarize:** If the reviewer has a Copilot for Security license, Copilot can review messages to detect problems and summarize contents.
- **Notify:** Send an email to the sender to tell them about the potential violation and (possibly) to ask for their input. Messages created from *Notice Templates* (see below) help ensure that notifications use the right tone and words and include any necessary references to organization policies.
- **Tag as:** Mark the item as compliant, non-compliant, or questionable.
- **Escalate:** Send the message forward to a higher authority for their review and decision. For instance, a message might go to the sender's manager.
- **Escalate for investigation:** Create an advanced eDiscovery case for the item and notify administrators about the new case. This step might be useful when a systematic problem is detected involving multiple people, such as potential insider trading.
- **Delete the item.**
- **Download the item.**
- **View item history** and **View message details**.
- **Automate:** Create a [Power Automate flow based on the message](#). You can create a new flow or use a template such as the Notify manager (CC) flow. This flow sends a message to a user's manager when they violate a policy.

If the review message comes from Teams and the violation is clear and obvious, the reviewer can remove the message from its source chat or channel conversation.

It's worth emphasizing that these are generic explanations, and a tenant is free to use their interpretation of how to resolve review items based on their business, regulatory environment, and HR policies.

Many of the messages detected by a policy don't need much investigation and reviewers can dismiss them quickly. Reviewers can select multiple messages (or all) and resolve them in a single operation, which speeds up the review process dramatically.

Communication Compliance Settings

The settings section of the communication compliance solution covers:

- **Privacy:** Decide if anonymized versions of user display names should be shown.
- **Sentiment analysis:** If enabled, Azure Cognitive Service for Language analyses messages to label messages as positive, neutral, and negative to help investigators decide which messages to process first.
- **Notice templates:** Because notifying someone that they might have done something wrong is an exercise fraught with potential problems, compliance communication policies use notice templates to ensure that notifications use the right tone and appropriate wording. Notice templates are available through the Settings section for communication compliance. An organization must add at least one notice template before they can use communication compliance policies.
- **Cross-policy resolution:** As noted above, this setting is enabled by default and means that if an investigator resolves an item detected by a policy, all other instances of the same message are automatically resolved across any other policy that detected it.
- **Teams:** To enable this setting, an administrator must grant consent to an enterprise app called O365-CC-Export to allow the app to read details about SharePoint Online sites, read files stored in any SharePoint Online site, read SharePoint and OneDrive tenant settings, and read user profiles. The app is unverified, but it is a Microsoft app (AppId value 615337d1-ef21-4491-8760-2735a65f6f3f). If enabled, policies that detect Teams messages will include Teams meeting transcripts in matching results.

A notice template includes email basics such as:

- **The originating mailbox:** It is usually better when notification messages come from a specific mailbox set aside for this purpose instead of an investigator's personal mailbox.
- **Boilerplate CC and BCC recipients:** For instance, notifications might need to be copied to an HR mailbox.
- **Subject:** The subject of notification messages is often dictated by HR or legal guidelines.
- **Message body:** Boilerplate text to inform the recipient why they are being notified and what policy is violated. The text might also include some "next steps" for the recipient to take, such as talking to their manager or contacting HR to arrange for an interview.

When an investigator chooses the *Notify* action, they select a template, and Purview copies the boilerplate settings into a message form. The investigator can then modify the settings as required by taking steps such as including some details about the violation. When everything is ready, they can send the message for delivery as normal to the recipient mailboxes.

Information Barriers

Exchange has long supported the concept of software barriers to stop defined sets of users from communicating with each other. In the past, organizations wrote bespoke customizations like transport sinks for this purpose. Usually, organizations operating in highly regulated industries deployed ethical firewalls to stop groups of people from communicating. For instance, a bank might stop traders and brokers from communicating. Since the advent of transport rules in Exchange 2007, transport (mail flow) rules are a favorite method to prevent communication between groups. Ethical firewalls are still available in Exchange Online, but other methods of communication exist, notably Teams. Information Barriers deliver a cross-workload answer by preventing sets of users from communicating using its supported workloads. Figure 16-25 shows the Information Barrier architecture to control access across Exchange Online, SharePoint Online, Teams, and OneDrive for Business (because of the work needed in the transport system, Exchange Online does not currently support information barriers).

Information Barrier Architecture

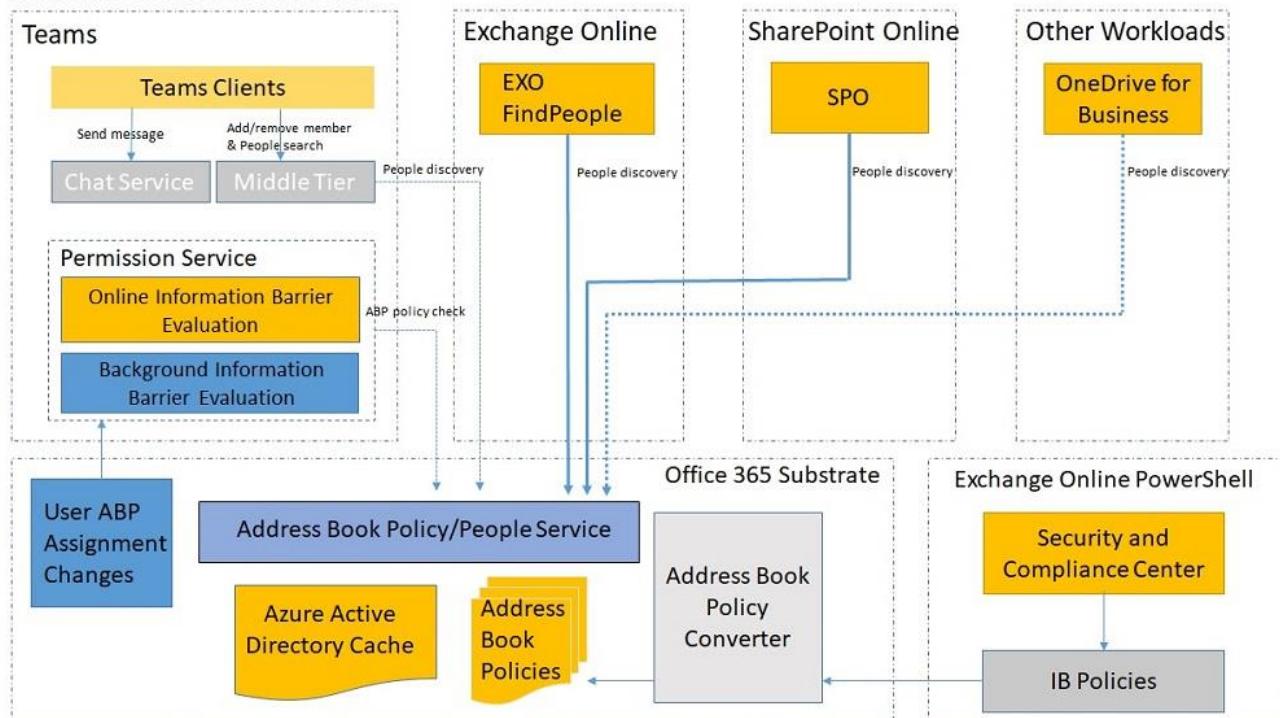


Figure 16-25: Information Barrier architecture (source: Microsoft – Ignite 2018)

Accounts under the control of Information Barrier policies require an Office 365 E5 license or the Microsoft 365 E5 Compliance add-on. An exception exists for education licenses because Microsoft bundles Information Barriers into the A5, A3, and A1 plans. Information Barriers are also part of the Microsoft Insider Risk solution.

The documentation for how to configure Information Barriers is [available online](#). Although global administrators often manage information barrier policies for a tenant, you can restrict permissions by assigning accounts the Information Barrier Compliance Management role as this is all that's needed to manage the policies.

Exchange Online currently doesn't support Information Barriers. Given that these policies depend on Exchange address book views, it's likely that the eventual implementation of information barriers in Exchange Online will replace Address Book Policies (ABPs), which restrict user access to the directory and have been in use since Exchange 2010.

In legacy mode, Teams depends on Exchange to scope directory queries, meaning that you must remove existing ABPs from a tenant before you can define Information Barrier policies. This can be a little tricky if any inactive mailboxes exist with assigned ABPs (assigned before the mailboxes become inactive): you can't remove an ABP if any mailbox (inactive or active) exists with a connection to the ABP, so you need to restore all inactive mailboxes with ABP assignments (restoring an inactive mailbox deletes the assignment) and then rem

Organization Segments

The sets of users used by Information Barrier policies are known as organization segments. Information Barrier policies define which segments can communicate with each other or those blocked from communication. The first step in implementing Information Barriers is to define organization segments for the users whose communication the organization wants to control. You don't have to create segments for the entire organization, but if you don't, the risk exists that some users will be able to communicate where a block should apply.

To define organization segments, you create queries to find user accounts. Microsoft suggests that you use the same property as the basis for all segments. In other words, if you decide to divide the organization by department, use the department property for all segments. It's also best if the segments don't overlap (multiple segments cover the same set of accounts).

Because Information Barrier policies depend so heavily on Entra ID, it follows that the information in the directory must be accurate. All the properties used to define organization segments must contain appropriate values, so a prerequisite for Information Barriers is to review the state of the directory to ensure that the right data is available. For instance, if you decide to use the department attribute as the basis, you could create a spreadsheet of all accounts including this data to verify its correctness. This PowerShell command does the job:

```
Get-MgUser -All -Filter "UserType eq 'Member'" | Select-Object department, displayName, userPrincipalName, officeLocation | Sort-Object department | Export-Csv -NoTypeInformation c:\temp\UsersDepartments.csv
```

Multi-Segment Mode

Originally, information barriers supported the assignment of users to a single segment. Information barriers supports user assignment to multiple segments. To discover what mode your tenant is in, run this command:

```
(Get-PolicyConfig).InformationBarrierMode
```

The value will either be *Legacy*, *SingleSegment*, or *Multisegment*. See [this article](#) for more information.

Creating Organization Segments

Information Barrier policies work by either allowing or blocking segments from communicating with each other. To create a policy, we must first define the segments. Each segment has a filter to tell Entra ID which accounts come within its scope. Think of this as like the filter used by a dynamic group. In the example scenario, we want to create an ethical firewall for Teams to stop staff in the Trading and Sales departments from communicating with each other. To do this, we need two organization segments: one defines the accounts in the Trading Department, and the other defines the accounts in the Sales Department.

Organization segments can include both tenant and guest accounts.

You can manage information barriers through PowerShell or the Microsoft Purview Compliance portal. The GUI includes a filter builder that makes it easier to construct complex filters used in organization segments and the conditions for information barrier policies. It's recommended that you start off using the GUI to build segments and policies and use PowerShell whenever necessary for automation.

To use PowerShell, connect to the [compliance endpoint](#). In this example, we create two organization segments.

```
New-OrganizationSegment -Name "Trading Department" -UserGroupFilter "Department -eq 'Trading'"  
New-OrganizationSegment -Name "Sales Department" -UserGroupFilter "Department -eq 'Sales'"
```

To test the effectiveness of the query used by an organization segment, we can run the query with the *Get-Recipient* cmdlet. For example:

```
Get-Recipient -RecipientPreviewFilter {Department -eq 'Sales'}
```

Name	RecipientType
Andy.Ruth	UserMailbox
Eoin.Smith	UserMailbox
JAbrahams	UserMailbox

If you need to replace the filter, use the *Set-OrganizationSegment* cmdlet. To avoid user disruption, it's best to settle on segment definitions before introducing Information Barrier policies into production. Sometimes organizational changes such as the renaming of a department or other structural updates can force an alteration in a filter. For example:

```
Set-OrganizationSegment -Name "HR Department" -UserGroupFilter "Department -eq 'Human Resources and People'"
```

The segments defined above use simple queries. You can construct more complex queries using the [set of filterable attributes supported by information barrier queries](#). The 'co' listed in the set of attributes refers to the country name, like Singapore, Germany, or United Kingdom.

If you can't find a suitable attribute to use, you might be able to use the membership of a distribution list or Microsoft 365 group instead. This example creates a segment based on the membership of a Microsoft 365 group identified by its external directory identifier (the documentation says that you can use the group name, but this doesn't appear to work).

```
Get-UnifiedGroup -Identity "Trading Team" | Select ExternalDirectoryObjectId  
  
ExternalDirectoryObjectId  
-----  
29b959d6-56ab-4aea-b70d-ffb8397d397f  
  
New-OrganizationSegment -Name "Trading Controlled Segment" -UserGroupFilter "MemberOf -eq '29b959d6-56ab-4aea-b70d-ffb8397d397f'"
```

After deploying information barrier policies and letting the deployment jobs run to validate segment membership, you can check what policy applies to an individual user with the *Get-InformationBarrierRecipientStatus* cmdlet:

```
Get-InformationBarrierRecipientStatus -Identity Andy.Ruth -Identity2 JAbrahams
```

Creating Information Barrier Policies

After creating the necessary segments, we can create two Information Barrier policies. One policy prevents people in the trading department from communicating with sales, the other blocks reverse traffic. To make it clearer when looking for a policy, it's a good idea to capture the nature of the block in the policy name:

```
New-InformationBarrierPolicy -Name "Trading Block Sales" -AssignedSegment "Trading Department" -SegmentsBlocked "Sales Department" -State Inactive
```

```
New-InformationBarrierPolicy -Name "Sales Block Trading" -AssignedSegment "Sales Department" -SegmentsBlocked "Trading Department" -State Inactive
```

We deliberately create the Information Barrier policies in an inactive state to allow administrators to set everything up (and do some testing) before activating policies across the organization. You can't use a segment in an information barrier policy if it is already in use by another policy (even if that policy is inactive).

Note that you cannot remove an organization segment once an information barrier policy is active. However, you can change its user filter so that the segment no longer applies to any recipients.

Activating and Debugging Information Barrier Policies

To activate a policy, run the *Set-InformationBarrierPolicy* cmdlet to change the state to Active.

```
Set-InformationBarrierPolicy -Identity "Trading Block Sales" -State Active
```

After changing policies to an active state, run the *Start-InformationBarrierPoliciesApplication* cmdlet to begin the process of applying the policy conditions to the affected users.

```
Start-InformationBarrierPoliciesApplication
```

It can take some time before the application executes active policies to make them fully effective for users in the relevant organization segments (don't try to start multiple jobs as this generates some horrible errors). The *Get-InformationBarrierPoliciesApplicationStatus* cmdlet returns the status of the information barrier policy application. In this example, the application processed 4,343 recipients.

```
Get-InformationBarrierPoliciesApplicationStatus
```

RunspaceId	:	6f427633-0a48-4f57-9c84-ec5e8bb946f1
Identity	:	b4cf044a-e915-4960-9baa-7804415c2a3a
CreatedBy	:	Administrator
CancelledBy	:	
Type	:	ExoApplyIBPolicyJob
ApplicationCreationTime	:	11/16/2021 21:11:54
ApplicationEndTime	:	11/16/2021 22:22:19
ApplicationStartTime	:	11/16/2021 21:11:54
TotalBatches	:	5
ProcessedBatches	:	5
PercentProgress	:	100
TotalRecipients	:	4343
SuccessfulRecipients	:	4343
FailedRecipients	:	0
FailureCategory	:	None
Status	:	Completed

By default, the cmdlet returns the status of the last run of the information barrier policy application. To see details of all runs, use:

Get-InformationBarrierPoliciesApplicationStatus -all:\$True

The application processes all mail-enabled recipients, including mail contacts. This is to make sure that the address book segmentation functionality works for all recipient types. If the job reports failed recipients, it's probably because those recipients are in multiple organization segments. To resolve the problem:

- Note the identity for the job reported by *Get-InformationBarrierPoliciesApplicationStatus*. In the example shown above, the identity is b4cf044a-e915-4960-9baa-7804415c2a3a.
- Search the audit log to find audit records with the *InformationBarrierPolicyApplication* record type for the date when the application ran and filter the set to find errors belonging to the run.

```
[array]$AuditLogs = Search-UnifiedAuditLog -ResultSize 5000 -Formatted -RecordType InformationBarrierPolicyApplication -StartDate (Get-Date).AddDays(-60) -EndDate (Get-Date).AddDays(1) -SessionCommand ReturnLargeSet | Where-Object {$_._AuditData.Contains("b4cf044a-e915-4960-9baa-7804415c2a3a") -and $AuditData.Contains("IBPolicyConflict") }
```

- Examine the AuditData property of each audit record to find the issue reported by the application, noted under *ErrorDetails*:

```
"ErrorDetails": "Status: IBPolicyConflict. Error: IB segment \"352e1fe3-fbee-4980-9208-103dde4b370\" and IB segment \"93889a38-0cbf-4d0f-a260-005a6a1c4893\" has conflict and cannot be assigned to the recipient \"fdc6b121-44b8-4262-9ca7-3603a16caa3e\".\r\n."
```

- We can see that the problem is that the conflict is between two segments. To see what the segments are, run the *Get-OrganizationSegment* cmdlet:

```
Get-OrganizationSegment | Where-Object {$_._ExoSegmentId -eq "352e1fe3-fbee-4980-9208-103dde4b370" -or $_._ExoSegmentId -eq "93889a38-0cbf-4d0f-a260-005a6a1c4893"} | Format-Table Name
```

Name
Trading Controlled Segment
Sales Department

- To resolve the recipient name, run the *Get-Recipient* cmdlet:

```
Get-Recipient -Identity fdc6b121-44b8-4262-9ca7-3603a16caa3e
```

Name	RecipientType
Andy.Ruth	UserMailbox

You now know why the error happened. The two segments both found the user Andy Ruth. Recipients identified in segments must be unique, so the solution is to update the recipient's properties to move them out of one of the two segments. You can't update a recipient's properties or the filter in an organization segment while the information barriers application is active, so wait until the active job finishes before making any necessary changes.

Microsoft's SLA for the application to detect a change in an account's properties that impact an information barrier policy is 24 hours. Usually, the application detects changes like updating someone's department faster (3-4 hours). The thing to realize is that it takes time for workloads to react to changes in the directory and to set expectations accordingly. Updating someone's role at 9 am does not mean that a barrier exists to stop them from communicating with others by 9:30 AM. This is especially true when the directory is in a state of churn due to department reorganizations or other major changes.

If a problem occurs in deploying Information Barrier policies or you make changes to policies, you can run the *Start-InformationBarrierPoliciesApplication* cmdlet to process all active policies.

Checking User Accounts

After processing an account to activate Information Barrier Policies, the account has an Information Barrier GAL (for the policy applied to the mailbox). This is how Information Barrier policies replace Exchange ABPs.

```
Get-Mailbox -Identity Andy.Ruth | Select -ExpandProperty AddressListMembership
\IBPolicyGAL_1bd52480-82f2-4416-814a-022776e46bef
\Default Global Address List
\Mailboxes(VLV)
\All Users
\Offline Global Address List
\All Mailboxes(VLV)
\All Recipients(VLV)
```

The *Get-Recipient* cmdlet also returns organization segment information for the user.

```
Get-Recipient -Identity Andy.Ruth | Format-Table InformationBarrierSegments
InformationBarrierSegments
-----
{352e1fe3-fbee-4980-9208-103ddea4b370}
```

We can check the membership of an organization segment by running a query using the GUID for a segment:

```
Get-Recipient -RecipientTypeDetails UserMailbox, GuestMailUser -Filter {InformationBarrierSegments -eq "352e1fe3-fbee-4980-9208-103ddea4b370"} | Format-Table DisplayName
```

You'll also see that mailboxes that do not come under the scope of an information barrier policy also receive policy address lists. In effect, although Exchange Online does not support information barrier policies and the mailbox is unrestricted, a policy applies to allow the mailbox owner to communicate with any other user in the organization. Behind the scenes, workloads are aware of policies applicable to mailboxes. Clients use the *FindPeople* API to request this information from the server and receive a restricted or open view in response.

```
Get-Mailbox -Identity James.Ryan | Select-Object -ExpandProperty AddressListMembership
\IBPolicyGAL_40ed3838-a6fd-4d1f-aa54-652537d5a708
\IBPolicyGAL_1bd52480-82f2-4416-814a-022776e46bef
\Mailboxes(VLV)
\All Mailboxes(VLV)
\All Recipients(VLV)
\Default Global Address List
\All Users
\Offline Global Address List
```

Outlook desktop users can see the names of the address lists created for Information Barrier policies. As the names are quite obscure, this might cause some questions for the help desk until people realize that they are just internal names.

It might take some time before the organization segments are acceptably accurate and reflect the communication paths allowed by the organization (or by regulation). There's also the small matter of synchronization and client caching to consider as it will take more time for clients to update changes synchronized from Entra ID and respect the blocks imposed by the policy.

Allowing Communication by Policy

Information Barriers also support the concept of an allow list to allow segments to only communicate with one or more other segments. For example, this command permits communications between accounts in the Group HQ segment with five other segments.

```
New-InformationBarrierPolicy -Name "Group HQ Communications" -AssignedSegment "Group HQ"
-SegmentsAllowed "Sales Department", "Marketing", "Research", "Trading Department", "Engineering"
```

If workloads can't find a policy to block or allow communication between two accounts, it assumes that communication is allowed.

Information Barriers in Teams

As you might expect, workloads implement Information Barriers to match their style of communication. The implementation of Information Barriers in Teams uses several different components, including:

- [Directory scoping](#) to limit the access of users to specific parts of the directory.
- Organization segments (common across all workloads) to define sets of users using queries against Entra ID.
- Information Barrier policies define how segments can or cannot communicate with each other.
- Background processes to apply the settings in Information Barrier policies to personal chats, team memberships, meetings, calls, and (optionally) sharing documents in SharePoint Online and OneDrive for Business.

Each team has a property called *InformationBarrierMode* to control if it comes within the scope of information barrier policy processing. After implementing information barriers for Teams, the property for new teams is set to *Implicit* to mark the team for processing. If you need to backfill the property for older teams, this is easily done with PowerShell:

```
[array]$Teams = Get-UnifiedGroup -Filter {ResourceProvisioningOptions -eq "Team"} -ResultSize Unlimited | Where-Object {$_.InformationBarrierMode -ne "Implicit"}  
Write-Host ("{0} teams are being backfilled for Information Barriers" -f $Teams.Count)  
ForEach ($Team in $Teams) {  
    Set-UnifiedGroup -Identity $Team.ExternalDirectoryObjectId -InformationBarrierMode "Implicit"  
}
```

The various modes supported by information barriers are [described here](#).

Note: The [Teams view-only experience](#) does not support information barriers. If the organization runs large meetings with over 1,000 attendees that force Teams to automatically use view-only for some attendees, you might need to consider disabling view-only by running the *Set-CsTeamsMeetingPolicy* cmdlet

```
Set-CsTeamsMeetingPolicy -Identity Global -StreamingAttendeeMode Disabled
```

Disabling view-only will restrict the attendance for meetings to 1,000 participants.

How Teams Uses Information Barriers

Teams imposes blocks to implement Information Barriers at several points.

Team membership: If a team owner tries to add someone to a team when a member already exists who is blocked from communicating with the new potential member, Teams won't allow the new member to be added. For existing teams, if a background scan of the membership detects a violation, the Information Barrier Processor removes members to bring the team into compliance. In most cases, removals are processed on a last-in, first-out basis: in other words, the last person who joins a team and causes a violation is removed and existing members are left in place. Action depends on when the Information Barrier Processor detects a violation caused by a change to the properties of individual user accounts or updates for organization segments, so removals might happen in a different order.

Any member of a team, including org-wide teams, whose presence causes a policy violation is removed by the Information Barrier Processor. Removal includes owners if they are in violation, meaning that a team can be left ownerless. Audit records for removals are in the audit log where you'll see that the user removing the account from the group is noted as "*ServicePrincipal_Guid*".

Information Barriers, Teams, and Guest Users: One problem that Teams currently has with Information Barriers is that team owners can't add a new guest user account. Existing guest accounts don't cause problems because Teams can check that adding them to a team roster won't violate a policy. If you try to add an external person whose account doesn't already exist in the directory, Teams can't validate that the barrier is respected, and the attempt to add the member fails even though the guest account is created in Entra ID. The workaround is simple: create the guest account through the Entra admin center or by adding them to the membership of the underlying group using Outlook or OWA. The addition of the new member will be replicated to Teams and any Information Barrier checks will then be imposed. Microsoft is aware that this situation is unsatisfactory and is working on a fix.

Chats: Teams won't start the chat if the participants are blocked by policy. At least, Teams will start a chat, but if the chat was created as a 1:1 chat, the only participant will be the person who tries to communicate with the person in violation. In the case of group chats, Teams removes the participants whose presence violates policy and leaves the other participants.

Joining meetings: When an account tries to join a meeting, Teams blocks them if other participants blocked by the policy are in the meeting.

Screen sharing: Any time someone shares their screen in a meeting, Teams checks for policy violations and won't allow the sharing if a violation is detected.

VOIP calling: When someone calls another person or a group, Teams checks the call to make sure that it doesn't violate a policy and terminates the call if a violation is detected.

Sharing a file with another user: Teams checks if the sharing violates an information barrier. This includes when users send a sharing link to grant access to a file stored in OneDrive for Business or SharePoint Online.

Users blocked from communicating with each other won't be able to see blocked accounts in organization charts, activity feed, suggested contacts, people cards, and call and chat contacts.

In addition, whenever Information Barrier policies or user accounts are updated, the Information Barrier Policy Evaluation Service evaluates existing chats and team memberships to ensure that no policy violation results from the update. Existing chats become read-only if Teams finds that participants are blocked by policy (Figure 16-26). The contents of the chat prior to the detection of the violation remain untouched.

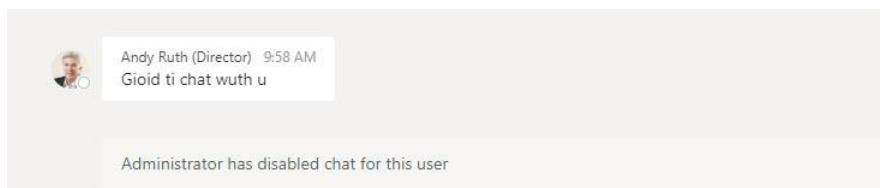


Figure 16-26: An information barrier policy blocks a user from an existing personal chat

Adding Group Members Using Administrative Interfaces

Although Teams can control the addition of members and how members communicate, it can't control how administrators add members to Groups through administrative interfaces. For instance, you can add a prohibited team member using the Teams admin center or the Microsoft 365 admin center. Likewise, you can do the same by running the *Add-UnifiedGroupLinks*, *Add-TeamUser*, or *Add-MgGroupMember* cmdlets. This is the reason why the Information Barrier Processor exists. It serves as a backstop to eliminate violations introduced through interfaces that do not know (yet) about Information Barrier policies. Here's what happens:

- Someone makes a change to the membership of a group using an administrative interface.
- The change synchronizes to Entra ID.

- The Teams – Entra ID synchronization process detects the violation(s) when it runs to update Teams with changes in Entra ID and blocks the changes. Teams accepts changes that don't violate Information Barrier policies. Clients subsequently download the changes to their local cache.
- The Information Barrier Processor runs later and removes the members in violation from the group.

The Information Barrier Processor serves as a backstop to eliminate violations introduced through interfaces that do not action the settings in Information Barrier policies.

Information Barriers and SharePoint Online and OneDrive for Business

To use information barriers with SharePoint Online, you associate organization segments with sites, and access to the site is thereafter determined by the segments associated with the site and the information barrier policy assigned to user accounts. Before using information barriers for SharePoint Online and OneDrive for Business, you must first enable the capability by setting tenant properties:

```
Set-SPOTenant -InformationBarriersSuspension $False
```

Segment assignment happens automatically for any site connected to Teams. SharePoint admins cannot change the assigned segment for teams-connected sites. For sites not associated with Teams, you can assign segments using the SharePoint admin center or PowerShell. With PowerShell, the first step is to connect to the compliance endpoint and run the *Get-OrganizationSegment cmdlet* to return the set of segments defined in the organization:

```
Get-OrganizationSegment | Select Name, EXOSegmentId  
  
Name          ExoSegmentId  
----  
Trading Department 5517962f-c1e2-4a4b-b905-997d99bdc393  
Sales Department   352e1fe3-fbee-4980-9208-103dde4b370  
Group General     c0ccc7f3-c44c-4ef6-a847-e1388bbec1c2
```

Then assign segments with the *Set-SPOSite cmdlet*:

```
Set-SPOSite -id https://office365itpros.sharepoint.com/sites/TradingDepartment  
-AddInformationSegment 5517962f-c1e2-4a4b-b905-997d99bdc393
```

A background assistant called the [Information barriers compliance assistant](#) runs every 24 hours to monitor group-connected SharePoint Online sites (excluding those connected to Teams) to detect and remove users who violate IB policies from site membership. Make sure that site owners are part of the segments assigned to the site as otherwise, they won't be able to access the site. In addition:

- SharePoint Online disables the option to use Anyone sharing links (if permitted by the tenant).
- The site and its contents can only be shared with people who match the segments assigned to the site.
- New users can only be added to the site if their segment matches one of those assigned to the site.

If a site has no segments assigned, SharePoint only permits users to share based on the information policy assigned to their accounts. For instance, if a user belongs to the Sales segment and policy blocks interaction with Trading, SharePoint won't allow that user to share content with people in the Trading segment.

The same approach applies to assigning segments to OneDrive for Business sites. In this case, because a OneDrive site is for personal storage, it is even more important to ensure that the assigned segment includes the site owner.

Audit Events for Information Barriers

Details about the processing of Information Barrier policies are captured in several audit events in the audit log, including:

- *New-ExoInformationBarrierSegment*: when a new organization segment is created.
- *RecipientChange*: when an account is updated because of information barrier settings.
- *ApplyIBPolicy*: when an account is evaluated for information barrier policies.

The Impossibility of Stopping User Communication

Information Barriers won't stop users from communicating with each other. In fact, in practical terms, no software barrier will stop people from communicating. Information Barriers don't stop users from emailing each other if they know each other's SMTP addresses or decide to use personal email accounts. This is the reason why you might want to use communication compliance policies to check email flowing between different parts of the organization or implement ethical firewalls with transport rules, especially if you want to control communication to specific domains.

It's also true that Information Barriers won't stop users from sending messages to VIP mailboxes, which is why mailbox moderation exists. Because all messages stay within a tenant, Information Barriers are more effective in stopping chat and voice communication with Teams, but again, they won't stop someone using a PSTN number to dial up another Teams user for a voice call.

If blocks stop people from communicating through email and Teams, they will find another route to share information, be it WhatsApp, a simple text message, or a surreptitious note scrawled on a scrap of paper. But that's not the point of Information Barriers or why you would want to deploy these policies. Instead, having policies like this in place helps organizations satisfy regulatory requirements in a demonstratable and provable manner. And if people want to do wrong, the organization should define and communicate HR processes to enforce company policy in a way that humans understand.

Chapter 17: Managing eDiscovery

The Microsoft Purview Compliance portal is the access point for cross-service compliance and protection operations, including the tools Microsoft creates to help tenants to run eDiscovery operations to recover information from mailboxes, sites, and other locations needed for investigations. This chapter covers:

- **Content searches:** How to search through locations (sites, mailboxes, teams, etc.) to find information. Information found by content searches can be exported for review by investigators or subject matter experts.
- **Microsoft Purview eDiscovery (Standard) – previously Core eDiscovery:** How to run eDiscovery operations spanning searches, holds, and exports. Standard eDiscovery is available to tenants with Office 365 E3 licenses to organize content searches (including exports) and in-place holds into cases to make it convenient for investigators to process information. A single eDiscovery case can span multiple searches and holds. The holds are *in-place*, meaning that the items that come within the scope of the hold remain inside the host repositories (for instance, an Exchange mailbox or a SharePoint document library).
- **Microsoft Purview eDiscovery (Premium) – previously Advanced eDiscovery:** Uses completely different technology to process high-end eDiscovery cases which typically cover much higher volumes of data than Standard eDiscovery cases do. The organization of Premium eDiscovery cases is different too. eDiscovery Premium requires Office 365 E5 or Microsoft 365 Advanced Compliance licenses.

eDiscovery is a specialized subject and not everyone is interested in how to run searches, create holds on different resources, or export results. However, given the massive increase in data stored by companies and the litigious nature of the world, it is likely that many tenants will meet the need to run some form of search in any given year, even just to find a document or message that a user thinks they have lost. With that thought in mind, we begin by looking at content searches.

A New eDiscovery Experience

Microsoft is consolidating its Purview solutions into a single portal. The new portal includes a new implementation of Purview eDiscovery (available in preview) that combines the functionality currently available in content searches and the standard and premium versions of eDiscovery. Users can access different eDiscovery functionality based on the license they hold. The plan of record is for the transition to happen by the end of 2024. We will update the content of this chapter when the new software is generally available. For more information, [see this article](#).

Content Searches

The design goal for eDiscovery technology is to meet the needs of investigation professionals who need to pursue a compliance query from start to finish, potentially to the point where a company produces evidence in court to prove wrongdoing or other legal points. Searching for evidence is where investigations begin, and that is why content searches are so important.

Before beginning the process to create a content search, you should know:

- **What locations to search:** You can search Exchange Online user mailboxes (including shared and inactive mailboxes), group mailboxes, Exchange Online public folders, SharePoint Online and

OneDrive for Business sites, tasks (To-Do), Sway, and Forms (owned by Microsoft 365 Groups). Any information held in mailboxes, including compliance records for Teams channel and private conversations or Viva Engage community messages, is available. Planner tasks are discoverable if the Microsoft 365 substrate captures compliance records when users create or edit tasks (see the Planner chapter). Viva Engage messages are discoverable (in Exchange Online mailboxes) for networks configured in native mode.

- **The keyword query to use to find information:** Content searches depend on the content indexes created and updated by Microsoft Search. As users create information using a supported workload, Microsoft Search automatically processes the information and adds it to its content indexes. Queries can be all-encompassing ("find everything"), basic ("search for this term"), or very complex.

Content searches use the Microsoft 365 server fabric, which means that a tenant can run multiple concurrent searches. No limitation exists on the number of mailboxes or sites that you can include in a search as Microsoft designed this generation of search technology to be able to handle the demands of the largest tenant. While content searches take care of finding and exporting information from Microsoft 365 locations, if you need to apply a hold to keep email and documents until investigators no longer need that information, you create an eDiscovery case. The holds processed by eDiscovery cases depend on content searches to find the information to hold. Content searches can also be part of an eDiscovery case, where investigators can use a set of searches to interrogate various locations using different queries to retrieve the information that they need. Table 17-1 lists some scenarios where content searches are useful.

Scenario	Search action
Assess the risk to the business from data shared by users with external people from SharePoint Online or OneDrive for Business sites	Include the <i>ViewableByExternalUsers</i> keyword in the search and set it to True. In order to exclude the .aspx files used by SharePoint Online, the full query is <i>ViewableByExternalUsers:true AND ContentType:document NOT FileExtension:aspx</i>
Find documents that match specific sensitive information types (as defined for Data Loss Prevention – see the DLP chapter)	Include the <i>SensitiveType</i> keyword in the search and specify the sensitive information type to look for and the number of instances of that type that must be in a document for the search to retrieve it. For instance, <i>SensitiveType:"Credit Card Number 5.."</i> finds documents that have more than five credit card numbers. See this page for more information.
Investigate whether anyone sent emails holding confidential information to a specific address outside the organization	Include the <i>Recipients</i> keyword and specify their SMTP email address in a search. For example, <i>Recipients:"TRedmond@Yandex.com"</i>
Investigate whether mailboxes have received a specific phishing message (or not)	Include the <i>Sender</i> and <i>Subject</i> keywords with values to search. For example <i>Sender:"SomeGuy@FortuneForYou.com" AND Subject:"I have transferred \$100million to you"</i>
Check that a message that has some specific text in its body is not circulating within the organization	Include the <i>Body</i> keyword in the query. For example, <i>Body:"We are about to be taken over by MegaCorp"</i>

Table 17-1: Content search scenarios

Microsoft limits the number of search jobs that tenants and individual users (administrators) can run. Jobs include searches and exports. The limits are outlined in Table 17-2.

eDiscovery Premium	Tenant Limit	User limit
Concurrent job limit (any jobs)	100	50
Concurrent job limit (tenant wide job)	50	25
eDiscovery Standard		
Concurrent job limit (any jobs)	50	25
Concurrent job limit (tenant-wide jobs)	5	5
Maximum number of jobs per day	500	
Maximum data size limit per day	2 TB	

Table 17-2: Search job limits

Microsoft says that the limits should not interfere with normal tenant operations and exist to ensure service stability and reliability. Searches can be resource-intensive operations, especially if asked to search through a large number of locations, such as all sites or all mailboxes. The limits exist to stop some organizations running too many jobs at the same time. From a marketing perspective, they also help to emphasize the difference between eDiscovery Standard and Premium.

Limiting Search Sources for Better Results

A content search can scan tens of thousands of target repositories and return multiple terabytes of results. To ensure that searches execute in a reasonable time, it is important to limit the number of locations where the search looks for relevant information by either restricting the number of targets or by refining the search query so that it excludes irrelevant items from the search results. As the foundation for successful searches is based on precision, the latter approach is always the best one to pursue.

As a very large multi-national company, Microsoft follows many legal and regulatory requirements around the world. Its litigation team uses eDiscovery to manage investigations and has written a [white paper to explain how it handles eDiscovery cases](#). In 2017, Microsoft said that its use of Microsoft 365 compliance technology contributed to an annual cost saving of some \$4.5 million. Your mileage might vary.

Content Search Scalability

The speed and scalability available to Microsoft 365 content searches originate from the way that the searches use the Microsoft 365 infrastructure. A limit exists for the on-premises searches performed by either Exchange or SharePoint based on the load that a single server can manage. For instance, the older In-place Hold and eDiscovery tool used in Exchange on-premises servers ([retired from Exchange Online in mid-2020](#)) uses a single server to control searches and uses synchronous connections to all the mailbox servers that host mailboxes within the scope of the search. The search eventually collates the results returned by individual servers to form the set of found items.

Content searches use the Microsoft 365 server fabric to process searches and split work across multiple servers. Asynchronous messages pass between the servers doing the work to keep them updated about search progress. This implementation reduces the potential for failure and parallelizes the workload to scale up to deal with far higher volumes of data (such as over 700,000 mailboxes in a single operation). Microsoft [documents the expected search performance for mailboxes](#) based on statistics gathered for searches against different numbers of mailboxes.

Searches need some time to spin up, so the time cited by Microsoft is indicative rather than precise. Once the search starts, it rapidly processes target locations to find items based on the keywords and conditions in the

search criteria. The number of mailboxes included in a search is the biggest single factor influencing how long the search will take. Apart from user-created items in the mailbox, the Microsoft 365 substrate stores many other items in user and group mailboxes, including “digital twin” copies of data from SharePoint Online and OneDrive for Business and compliance records for workloads like Teams and Yammer. Online mailboxes are usually larger than their on-premises counterparts and can have large recoverable items and archive components. All contribute to the number of items stored in mailboxes and increase the time needed to search mailboxes. The bottom line is that if you want fast records, be precise about the mailboxes included in a search.

Content searches also include some retry logic to handle the situation where a required mailbox or site is offline for some reason. Usually, a retry is enough to complete a search. See this page to understand more about [the limits applying to content searches](#).

SharePoint and Exchange Support for Sensitive Information Types

You can combine keywords to build a search query that covers multiple conditions. SharePoint Online and Exchange Online have different abilities to use keywords. Some of the keywords are specific to documents and some to mailbox items. For example, you cannot include the *ViewableByExternalUsers* keyword in a search that scans Exchange Online mailboxes because this kind of sharing concept does not exist for Exchange. In addition, although both SharePoint Online and Exchange Online support [sensitive information types](#) (like credit card numbers, passport numbers, and national identification numbers) used by Data Loss Prevention and retention policies, only searches of SharePoint content support these keywords. If you include unsupported keywords in a search, the search ignores them when it builds its results. This [page gives guidance about the keywords](#) that you can use for Exchange and SharePoint locations.

Creating and Running a Content Search

You must be a member of the Compliance eDiscovery Manager or Organization Management role groups to be able to create and execute a content search. In addition, an account used to conduct compliance searches should have a functional Exchange Online mailbox. Although no strict licensing requirement exists for a mailbox, the preview function for search results does not work if the account used for searching has no mailbox.

To access content searches, open the Microsoft Purview Compliance portal and go to the **Content Search** section. You then see a list of the existing searches for the tenant. You can select a search and continue working with it to amend its search criteria and run new queries or create a new search. In the example explained below, we create a new search from scratch. After naming the search and adding a description, we define the locations, keywords, and conditions to frame the search.

Search Locations

After assigning a suitable name to the search, the next step is to define where the search should scan for matching items. The three basic locations (Figure 17-1) are:

- **Exchange mailboxes:** All Exchange Online mailboxes, including inactive mailboxes. Searching Exchange mailboxes also covers Teams and Viva Engage messages because the Microsoft 365 substrate captures compliance records for Teams and Viva Engage conversations in Exchange personal mailboxes (for personal and group chats and Viva Engage private messages, including the call records for people who participate in meetings or calls) and group mailboxes (for Teams channel and Viva Engage community conversations). Content searches cannot process on-premises mail boxes managed by Exchange Server. Searches for on-premises content must be conducted on the target servers.

- **SharePoint sites:** Includes all SharePoint sites and OneDrive for Business accounts. Searching SharePoint includes the sites created to store Teams files, including the wiki (.mht file) created for each channel.
- **Exchange public folders:** If your organization uses public folders, you can search for information stored in any public folder. You cannot search a subset of public folders.

Checking the *Add App content for On-Premises users* option instructs the search to include the cloud-only mailboxes used to store compliance records captured for Teams and Yammer messages sent by hybrid, guest, and federated users.

Locations

Status	Location	Included	Excluded
<input checked="" type="checkbox"/> On	Exchange mailboxes Microsoft 365 Groups, Teams, Yammer user messages	All Choose users, groups, or teams	None
<input checked="" type="checkbox"/> On	SharePoint sites OneDrive sites, Microsoft 365 Groups, Teams	All Choose sites	None
<input type="checkbox"/> Off	Exchange public folders		

Add App Content for On-Premises Users. [Learn more](#)

[Back](#) [Next](#)

Figure 17-1: Specifying target locations for a content search

Adding Exchange Online Mailboxes

To refine the set of Exchange mailboxes, click the **Choose users, groups, or teams** link and then use the search box to find the target mailboxes, Microsoft 365 groups, and distribution lists. You can't add dynamic distribution lists to a search. When the set of mailboxes is input, the search expands the current membership of distribution lists and adds the individual mailboxes to the set of target mailboxes.

Disconnected mailboxes and Content Searches: Although content searches can scan inactive mailboxes, you can't include disconnected mailboxes in a content search. These are mailboxes belonging to Microsoft 365 accounts where an administrator removes the Exchange Online license from the account. Disconnected mailboxes stay in a soft-deleted state for 30 days following the removal of the license before Exchange Online permanently deletes them from the system. If disconnected mailboxes are in the set of mailboxes used for existing searches, the search ignores them when it generates results.

Continue to add mailboxes (remember to select mailboxes from the list and then click **Choose**) until you have added the desired target selections to the search.

Adding SharePoint Online and OneDrive for Business Sites

Click **Choose sites** to add new locations to the set of SharePoint and OneDrive sites. For each site, select its URL or part of its display name into the search box. When you've found the set of sites to search, click **Add** to add them to the search criteria.

To add specific SharePoint Online and OneDrive for Business sites to a search, you must know the complete URL for the target sites. You can find the URL by opening the site in a browser and copying the URL, or you find the site URL with PowerShell. The `Get-SPOSite` cmdlet returns all the sites in a tenant, including their URLs, and is the obvious way to find a site URL, including for OneDrive for Business accounts. To find a list of all OneDrive for Business sites in the tenant, connect to SharePoint Online with PowerShell and run the command below. You could also export the list to a CSV file to keep as a handy reference:

```
Get-SPOSite -IncludePersonalSite $True -Limit All -Filter "Url -like '-my.sharepoint.com/personal/'"
| Select-Object Owner, Url | Sort-Object Owner
```

If a site belongs to a Microsoft 365 Group or Team, you can find the URL with the command:

```
Get-UnifiedGroup -Identity MyGroup | Select-Object SharePointSiteURL
```

```
SharePointSiteUrl
```

```
-----
```

```
https://mytenant.sharepoint.com/sites/mygroup
```

Adding SharePoint Sites for Teams Private and Shared Channels

Teams private and shared channels keep their conversations and files separate from the other parts of the team to ensure that only channel members can access this content. Each private or shared channel has a dedicated SharePoint site, which is a child of the site owned by the team. Searching the parent team automatically includes the conversations in a private channel (using the compliance records in the team's group mailbox). To search for conversations in a shared channel, you must add one or more members of the channel to search the compliance records stored in the personal mailboxes. If you want to add the SharePoint site belonging to a private or shared channel to a content search, you need to know its URL. The easiest way is to open the channel in Teams and use the "Open in SharePoint" option in the Files tab to open the channel site in the SharePoint browser interface. Then you can copy the URL shown in the browser navigation bar.

On an admin level, because the settings of these sites come from the parent team site, the SharePoint admin center does not support management of the sites used by private or shared channels. However, PowerShell can manage the sites. For example, when run by a SharePoint administrator, this PowerShell code returns all the sites belonging to private and shared channels and uses the group identifier to retrieve the team name from the Microsoft 365 group before writing out the display name and site URL.

```
[array]$Sites = Get-SPOSite -Template "TeamChannel#1"
ForEach ($Site in $Sites) {
    $SPOSite = Get-SPOSite -Identity $Site.url -Detailed
    $Group = Get-UnifiedGroup -Identity $SPOSite.RelatedGroupID.Guid
    Write-Host "Team" $Group.DisplayName "owns channel site" $Site.URL }
```

Notice that the SharePoint template used for the sites used by both private and shared channels is "TeamChannel#1." This is the current template used by Microsoft when it creates private and shared channel sites. Older private channel sites might have the `TeamChannel#0` template. To return sites with both templates, use a command like:

```
[array]$Sites = Get-SPOSite -Limit All | Where-Object {$_.Template -eq "TeamChannel#0" -or
$_.Template -eq "TeamChannel#1"}
```

When you examine the URLs created for sites used by private or shared channels, you'll see the following naming convention:

```
https://tenant.sharepoint.com/sites/TeamName-PrivateSharedChannelName
```

For example, the site for the "Legal Discussions" private (or shared) channel owned by the "Corporate Acquisition Planning 2020" team is:

Search Keywords and Conditions

Content searches run queries composed in the Keyword Query Language (KeyQL) against content indexes to find information. You can use either the query builder or KeyQL editor to compose a query. The KeyQL editor is also available to create content queries for Premium eDiscovery searches. In the past, the language was referred to as KQL, but this caused confusion with the [Kusto Query Language](#) (used with Microsoft Sentinel, Microsoft Fabric, and other products), so the keyword-based query language is now KeyQL.

The query builder allows you to add keywords and conditions in a GUI while the KeyQL editor supports auto-completion for searchable properties and conditions along with checking for acceptable input, such as the available operators for a property. New search administrators usually find it easier to start with the query builder while those who are more experienced use the KeyQL editor. You can toggle between the query builder and the KeyQL editor as needed while working on a query. This is useful because you can compose a query with the query builder that has an error. When you toggle to the KeyQL editor, the editor highlights any syntax problems it detects to allow you to fix them. The KeyQL editor is there to make it easier for people to compose queries that don't contain obvious syntax errors. However, there's no guarantee that a query passed by the KeyQL editor will work or, if it does, will find the information you expect. For this reason, it's important to understand the fundamentals of KeyQL queries.

Queries are formed from keywords and conditions. The keywords are free-text expressions, meaning that you can use individual words or complete multi-word phrases. If you include phrases, you must enclose them in double quotation marks. You can leave the keywords box empty if you want to search for everything in the locations that you choose.

Keywords support prefix matching, which means that you can include the wildcard operator (*) with the beginning or end of a word (for instance, "Office*"). You can combine free-text expressions with KeyQL operators such as OR, AND, NOT, and NEAR. For example, this query finds items in SharePoint Online or OneDrive for Business that include the keywords NDA, "Non-disclosure agreement," or "non disclosure" in Word or PDF formats. The reason for specifying non-disclosure and non disclosure is to pick up documents that use either variant:

(NDA OR "Non-disclosure agreement" OR "non disclosure") AND (filetype:doc OR filetype:pdf)*

This query uses a wildcard operator to find spreadsheets containing "Microsoft 365 Groups" and a special relative date comparison to specify that we're looking for spreadsheets modified in the current year:

("Microsoft 3" AND "Groups") AND (filetype:xls*) AND (LastModifiedTime = "this year")*

Other special date comparisons include today, yesterday, this week, this month, last month, and last year. We can also find items using date ranges. This query looks for any document or message created in October 2020 which includes the word *shareholder* within 10 terms of the word *agreement* where the author is Tony Redmond.

("shareholder" NEAR(10) "agreement") AND (Author:"Tony Redmond") AND (LastModifiedTime >= 2020-10-01 AND LastModifiedTime <= 2020-10-31)

To preserve the order in which words appear, use ONEAR instead of NEAR.

If you include multiple free-text expressions in a query, KeyQL combines the expressions in the search using the AND operator. If you enter an operator in lowercase (like "and"), the search will offer to uppercase the operators when it checks the query. You should always accept this offer as uppercasing the operators makes their purpose obvious (and lowercase operators don't work). Figure 17-2 shows an example of a search using

some keywords to tell the search that we're interested in items where the words Office 365 and E5 are found in email sent by a specific person received within a date range.

The screenshot shows the 'Define your search conditions' interface. It consists of three stacked AND clauses:

- Keywords:** "Office 365" AND E5
- Sender/Author:** Equals any of Kim.Akers@Office365itpros.com
- Received:** Between 2023-05-06 and 2023-06-06

A 'Show keyword list' checkbox is located below the first clause. Navigation buttons 'Back', 'Next', and 'Cancel' are at the bottom. A small sidebar on the right includes a message icon and a 'Q' icon.

Figure 17-2: Building search criteria for a content search

The *Show keyword list* checkbox allows you to input a keyword in each row of a list. The reason why you would want to do this instead of typing all the keywords into the keyword box is that the search generates statistics for each keyword. When the search runs, you can review the statistics to understand which keyword is most effective in terms of search results.

If you toggle to use the KeyQL editor for the query shown in Figure 17-2, you'll see the query in KeyQL format:

```
"Office 365" AND E5(c:c)(senderauthor=Kim.Akers@Office365itpros.com)(received=2023-05-06..2023-06-06)
```

The KeyQL editor supports cut and paste, so you can copy a complex query from one search, paste it into another, and modify the keywords and conditions as needed.

Keywords with non-English characters: By default, content searches are language-neutral. However, if you find that a search does not return the expected results, the cause might be that some of the keywords use non-English characters (such as Chinese). You can force a search to be language-sensitive by clicking the **Query-language-country/region** icon on the top of the search query box and then selecting a language country culture code value for the search (for example, Chinese – Hong Kong SAR).

Search Conditions

Conditions narrow searches by filtering the results generated by the keywords. When you specify a condition, the search adds a clause (shown using the (c:c) operator) to the search query used to find results. For example,

you might only be interested in items created by a certain person, in which case you use the author condition to specify the person. To apply a further filter, you could add the created (date) condition to focus on items created in a certain period. When the search query runs, items must satisfy the keyword query and one or more conditions before the search includes them in the results.

To make it easy for you to include conditions in searches, the **Add conditions** button in the query builder exposes a dialog listing the most common conditions. [Some conditions](#), like Sender/Author, are valid conditions for searches against both Exchange Online and SharePoint Online items. Other conditions are workload-specific. If you attempt to add a condition that won't work for the chosen target locations, the Microsoft Purview Compliance portal flags an error to tell you which condition has a problem. For instance, if you try to use the message type condition to search SharePoint Online, you'll see an error because SharePoint doesn't support that condition. To proceed with the search, you must remove the condition.

To complete a condition and add it to the search criteria, you must define what the condition checks for. For instance, if you add a retention label condition to the search, you must say what compliance tag (classification label) or tags you want to look for. If you add a date to a search, you must input the date range for the search and say whether you want to look for items between two dates, before a date, or after a date.

Remember that people can change their names for good reasons, such as marriage or divorce, which means that you might need to include addresses for people other than their current user principal name or primary SMTP address. Queries can handle this situation by including variants of names in the sender/author condition.

Run the Search

After defining the search criteria, the Microsoft Purview Compliance portal launches a preview for the search automatically. Before this happens, the portal checks the query for any syntax errors and identifies any potential improvements. The search then runs the query against the target locations. A preview search is not a full search. Instead, the preview uses content indexes to retrieve a sample of items that a full search will find to allow the search author to decide if the criteria are accurate enough to find the desired information. The preview also generates estimates for the number of items a full search will find. The actual number of items that a full search will find will probably differ from the preview, but the difference is usually of minor importance. For instance, the results shown by preview searches against SharePoint sites sometimes include ASPX files (used by SharePoint) that are of no interest to an investigator. It's also possible that users create or delete items matching the search criteria between the time of a preview search and when the actual search happens, or indeed that a lag in indexing stops a file from appearing in a preview when a subsequent search finds it.

A full search might have to process thousands of mailboxes and sites, so it is better to get quick results back from a preview rather than having to wait for the full search to complete. Equipped with the preview information, you can assess the effectiveness of the query and then tweak the search parameters. The process of tweaking search criteria might need multiple iterations before you are happy with the results delivered by the search and proceed to perform the full search and export its results.

When the preview search is ready, the search selects samples from the top locations (those that hold the most matches). You can view the items retrieved by the preview search by selecting the **Review sample** option from the search summary. As shown in Figure 17-3, sample items include email messages, Teams compliance records, and files (list items are not available for preview). If an item has an attachment, it also shows up as viewable if the attachment is an Office document. Preview can decrypt protected files and messages too.

Preview searches don't support the display of some document formats. For example, you cannot preview the contents of a OneNote file or a video message from Teams chat. Although search can find these items using

either item contents or their metadata, a viewer is unavailable to preview their content. Instead, investigators must export the search results and view the copy of these files retrieved from the search locations.

Naturally, the fewer the number of results, the less time is necessary to show the preview results. If the preview of the source for a found item displayed in the viewing pane isn't sufficient to fully understand the content of an item, use the *Download Original Item* link in the item preview pane to download a copy of the item for review.

The screenshot shows the Microsoft Purview Compliance portal interface. At the top, there's a red header bar with the Microsoft Purview logo, a 'New Microsoft Purview portal' button, and a user profile for 'Tony Redmond'. Below the header is a navigation bar with back, forward, and search icons. The main area has a title 'Confidential Documents samples' and a toolbar with 'Download list', 'Refresh', '1 selected', 'Customize columns', and sorting arrows. A table lists search results with columns for 'Subject/Title', 'Date', and 'Sender/Author'. One row is selected, highlighted with a blue border. To the right of the table is a 'Source' pane showing detailed information for the selected item, including 'From', 'To', 'Subject', and 'Send Date'. Below this is a 'Download Original Item' link. Further down is a list of eight numbered items, each with a link. The first item is '4. Use Azure Automation and PowerShell to Create a Daily Microsoft Entra Risk Report'.

Figure 17-3: Reviewing sample items retrieved by a content search

The Microsoft Purview Compliance portal [limits the number of items selected from estimate searches for preview](#). This is acceptable because the intention behind the preview sample is to help investigators understand the effectiveness of the search query in terms of finding the required data. The preview sample is not a tool to browse through the complete set of items uncovered by a search.

The search summary screen includes search statistics for the estimated items that a full search will find (Figure 17-4). The three sets of statistics are:

- **Search content:** Displays the estimated items for the locations scanned (SharePoint and Exchange), the number of locations with hits (matching results), the number of matching items found, and the size of those items.
- **Condition report:** Displays the location type (SharePoint or Exchange), the condition (search query used), the number of locations with hits, the number of matching items found, and the size of those items. If you use a keyword list, you can see how effective each keyword is in terms of locating items (a result recorded as Primary means the complete search query; Keyword means the results from a specific keyword). You can also see whether any unindexed items matched the query. Unindexed items are often graphic files like a bitmap or JPEG file, or the MP4 files used for Teams meeting recordings.
- **Top locations:** The sites and mailboxes where most matching items were found, including the number of those items and their size.

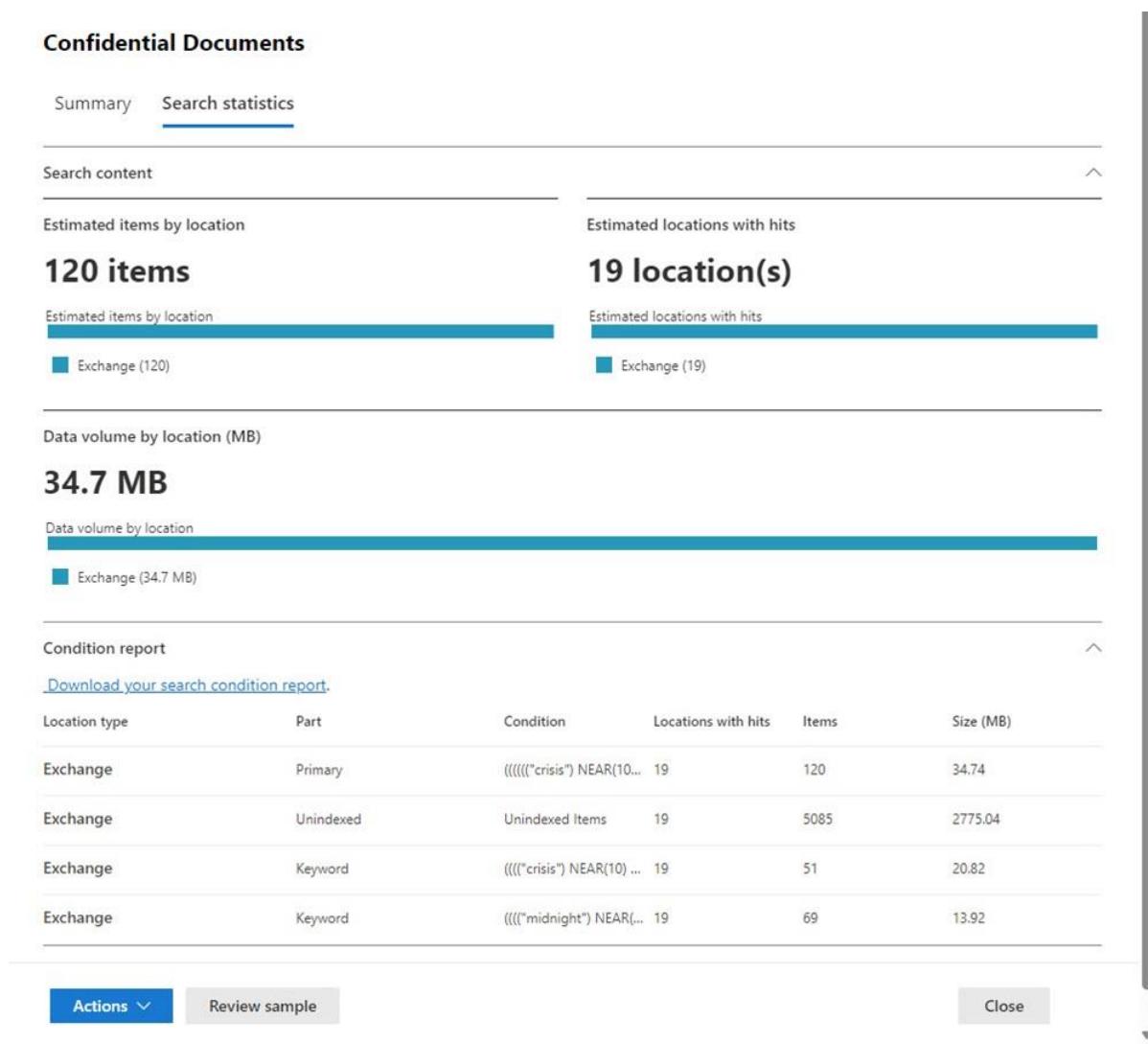


Figure 17-4: Reviewing statistics for a preview search

Hybrid SharePoint searches: If a hybrid connection is in place, it is possible to use hybrid SharePoint searches to find content stored within on-premises SharePoint farms. However, when you run content searches, the search filters out the results from the on-premises sources because no method exists to allow Microsoft 365 to apply holds to on-premises SharePoint data or to export data from an on-premises SharePoint location.

Expired Searches

If you look at the details of a search and see that "*the search has expired*," you know that it is more than seven days since the last run of the search. As such, Microsoft 365 considers the result results to be unreliable because it doesn't include potentially important information added to the search locations in the last week. To proceed to use other search features such as exporting results, you must first rerun the search to make it current.

Exporting Search Results

Eventually, you will be happy that a search finds the right information. At this point, you might want to export the files and messages found by the search to perform a more detailed examination of individual items, give the data to external investigators, or make it available to someone who does not have the necessary permission to run searches in the Microsoft Purview Compliance portal. The export function allows you to extract search results from the source locations, copy them to a secure holding point in Azure, and then copy

the data from Azure to PSTs (for messages), individual files, or ZIP files. You can also export a report of the search results, meaning that instead of exporting the actual data, the search creates and exports reports listing the files and messages that it would export for a search.

A content search export can process items found in up to 100,000 mailboxes and will fail if a search covers more than this number. If you need to export information from larger location sets, you should use Premium eDiscovery.

Selecting Export Options

To begin, make sure that the search is current as you will not be able to export results if they are more than seven days old. It is a good idea to refresh search results before beginning an export as this ensures that the exported data will be completely up to date. To start the export job, select **Export results** from the **Actions** menu. Figure 17-5 shows the screen used to gather information for the export process. While the search always exports SharePoint and OneDrive documents as individual files, you can export items extracted from Exchange mailboxes to:

- **A single PST for all Exchange content:** This option is convenient for investigators and is usually the best option when dealing with small amounts of information. Exchange Online does not include the `New-MailboxExportRequest` cmdlet available in the on-premises version to export content from a mailbox to a PST. However, you can mimic the functionality by creating a content search for all content in a single mailbox and exporting the results (the entire mailbox) to a PST.
- **To multiple PSTs** (one per mailbox): This choice allows the people who must process the results to split the workload across multiple individuals. If an export processes more than 10 GB of data, the job will automatically split into multiple PSTs, each of which is up to 10 GB (it is possible to change this limit with [a registry setting](#)).
- **To individual MSG files:** This choice exists because some third-party investigation tools do not support importing data from PST files. In addition, if you want to export messages encrypted with rights management, you must export them as individual files. The export job writes a copy of each message uncovered by the search to the target destination in the file system. The administrator can then move the copied files from there as needed. The export job organizes the individual MSG files into a folder structure. The folder for a mailbox is named after the user principal name of its owner. Underneath this root, the found items are divided into:
 - **Recoverable items:** Items extracted from folders in the Recoverable Items structure are here. For example, if an item was purged by the user but kept due to a hold placed on the mailbox, it is in the `Recoverable Items\Purges` folder in that user's mailbox.
 - **Top of Information Store:** The export job places items extracted from folders visible in the user's mailbox here. The export job creates a separate file system folder for each folder in the mailbox where the search found a matching item. Given the complex folder structure that exists within some mailboxes, the 260-character maximum path to a Windows folder may be reached. When this happens, the export job truncates the folder names to stay within the limit.
- **To a compressed (zipped) folder:** This option includes both Exchange and SharePoint content. Exchange items are in separate MSG files (with attachments) while items found in SharePoint and OneDrive are exported as individual files. Exporting to a compressed folder avoids the issue that sometimes arises when the file path to a SharePoint item exceeds 260 characters. Like PST files, if an export exceeds 10 GB, the search splits the export into multiple ZIP files (you can use the same registry setting mentioned above to control PST sizes to change the maximum size for a ZIP). Note that files in a ZIP folder only have the modified date for files, not the created dates. However, the created date is stored in the XML manifest for the export job.

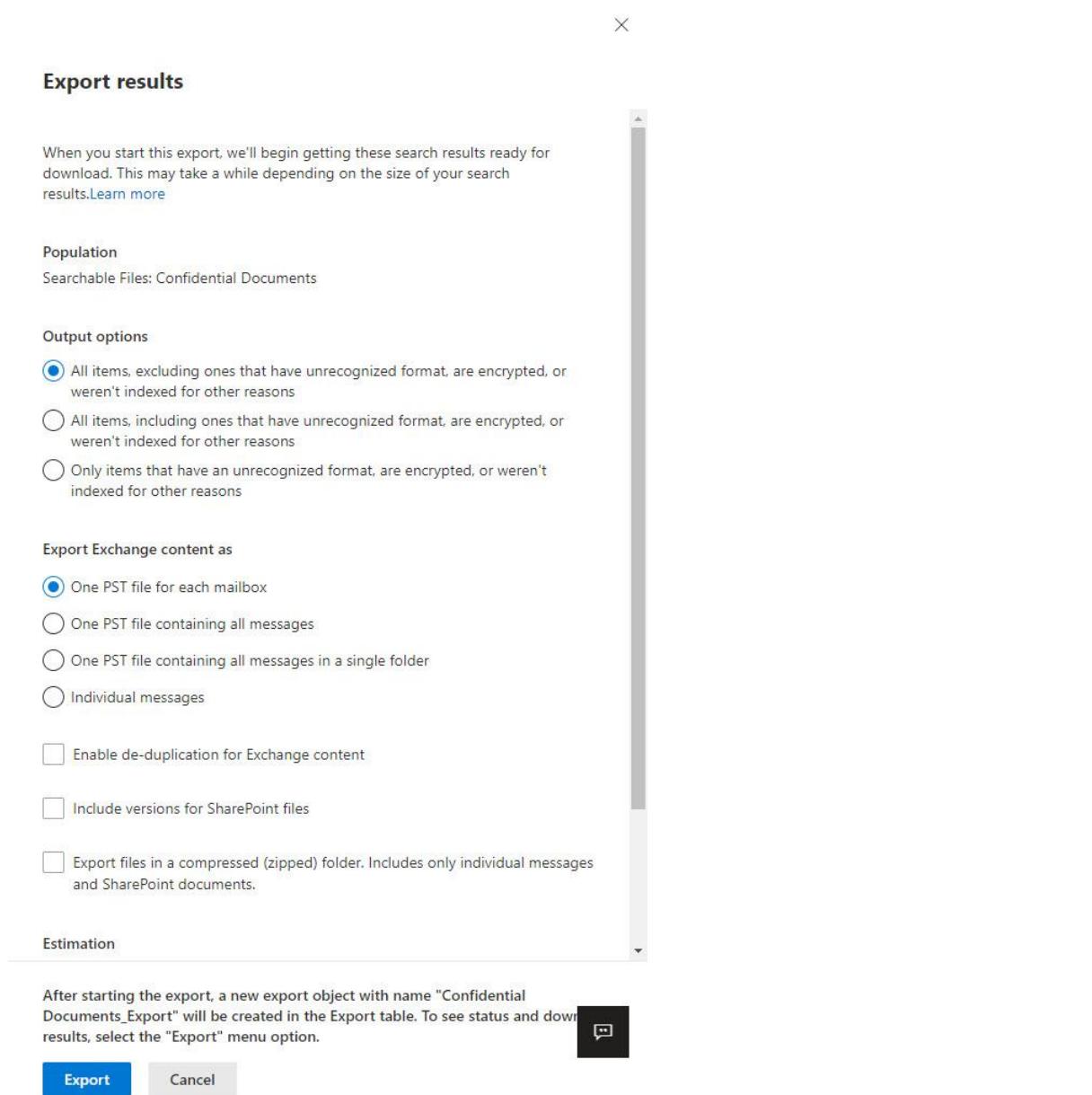


Figure 17-5: Defining settings to export items found by a content search

If the search includes SharePoint or OneDrive for Business sites, you have the choice to include versions for documents found by the search. Versions are only available for documents if versioning is enabled for document libraries. Versions come from the preservation hold library of the sites where the search finds documents. You'll recognize these as versions because their name is composed of the original file name plus a date-based identifier created by SharePoint to make the file name unique.

Due to the way that Exchange Online delivers individual copies of messages to mailboxes, a search will likely find multiple copies of a message. To export just a single copy, enable the de-duplication option for Exchange content. Each message has a unique identifier, so when de-duplication is enabled, the export processes only the first copy of a message returned by the search. If it's important to recover a copy from specific mailboxes (perhaps for legal reasons), you can always run another export to recover copies for each mailbox where a message exists.

System data found by a search in a user mailbox, such as the information used by Viva Insights, doesn't appear in a preview, but the search exports this data to a folder called *Other Office 365 Data*. This data also includes Microsoft Forms owned by the user. Search exports metadata and Forms Q&A in JSON format. These items don't appear in search previews.

Export Mailbox to PST: A content search can find everything in a mailbox. It is therefore possible to use this capability to export a complete mailbox to a PST. To do this, create a search that finds all items in the target mailbox (enter no search criteria), and when the search completes, export its results to a PST. Being able to export a complete mailbox is sometimes necessary for investigations, and content searches make this an easy task.

Decrypting Search Results

The export process decrypts email messages protected with sensitivity labels including any attachments, but only if you export messages as individual MSG files. Protected items exported to a PST remain encrypted. Search marks items decrypted by the export process with "Decoded" in the Decode Status column of the Results.csv file in the export destination.

The Standard eDiscovery and content search export process does not decrypt protected documents exported from SharePoint Online and OneDrive for Business sites. If necessary, you can decrypt these files by running PowerShell cmdlets from an account that holds rights management super-user privilege. See the section on this topic in the Information Protection chapter. The Premium eDiscovery export process can decrypt protected documents, so if you have the necessary licenses, you can use this facility to export decrypted copies of protected files.

Handling Partially or Unindexed Items

Tenants are likely to have a certain percentage of unindexed or partially indexed items in Exchange Online, SharePoint Online, or OneDrive for Business sites. More will be in Exchange than the other workloads simply because users generate more messages than documents. Partially indexed means that the index contains an item's metadata (like subject, author, and creation date) but some of the item's content might not be indexable. Content searches can find partially indexed items using metadata.

The reasons why these items exist are varied. Some attachments or documents might be in an unsupported format; some items are too large (greater than 150 MB); some messages have more attachments than the supported maximum (250); and some formats have specific limits, like Excel's 4 MB limit. The limits for content searches [are available online](#) and the statistics reported for a content search tell you how many unindexed items were found. To help organizations understand the number of these items in their tenant, Microsoft wrote a PowerShell script to analyze how many partially indexed Exchange Online items exist and report the reasons why indexing failed. You can read [the article online](#) and fetch a modified version of [the script from GitHub](#).

Partially indexed items can be of interest to investigators, and you should include these items in exports if you want to be sure that an investigation can consider every possible issue. After all, a human might make sense of a file included in an export where a search cannot. Three options are available:

- **All items, excluding unindexed items.** This is the default and means that the search only exports items meeting the search criteria. Unindexed (partially indexed) items are excluded.
- **All items, including unindexed items:** The export includes unindexed items, but only if the search also finds items matching the search criteria in a site.
- **All unindexed items:** The export includes all unindexed items from all sites in the search, even if the search does not find matching items.

The usual process is to exclude unindexed items from exports and then decide whether a deeper examination is necessary incorporating these items.

Downloading Exported Results

After selecting the options for the export job, click **Export**. A background process starts to extract the information from source locations and copy it to the holding area in Azure. To follow the progress of the

export job, click the **Export** tab in the menu bar to see a list of all the export jobs processed for searches. Select the export job for your content search (it has the same name as the content search with a suffix of “_Export”), to display the status for the export job. Any search which uncovers tens of thousands of items spanning gigabytes of data will need some time to export the matching data. In this case (Figure 17-6), the number of search results is small, and we can see that the export is complete.

Before going ahead to download the exported results from Azure, we must copy the export key. The export key is a [shared access signature](#) to grant access to the secure storage area holding the export results in Azure and is of the form:

?sv=2014-02-14&sr=c&si=eDiscoveryBlobPolicy9%7C0&sig=PpqtiOKpBMzZPtA1ksuY8iciP6jsYYI2VHePjDXY45w%3D

The export key becomes the credentials to authorize the download of the exported data using the Microsoft 365 eDiscovery Export Tool. Essentially, the report key is a token that Azure Data Services recognizes when offered by a process that wishes to access some data belonging to another entity. You cannot use the key to access data held in Exchange Online or SharePoint Online with a browser or another client. After copying the export key to the clipboard, you can paste it into Notepad or another editor to make sure that it is always at hand. However, if you are ready to go ahead and download the results, click **Download Results**. It doesn’t matter if the search has not finished preparing data for export yet because the export tool checks with the search when it downloads information and will pause to let the export complete.

You must use the Microsoft Edge browser to download and install the export tool. You can use any other browser supported by Microsoft 365 to perform all other search functions. The first thing to do is configure Edge to enable *ClickOnce* support (the ability to [install and run an application created with the ClickOnce technology](#)). To do this, open a tab in edge and go to `edge://flags/#edge-click-once` and make sure that the value in the drop-down list is Enabled. If you don’t do this, the export tool won’t be able to run.

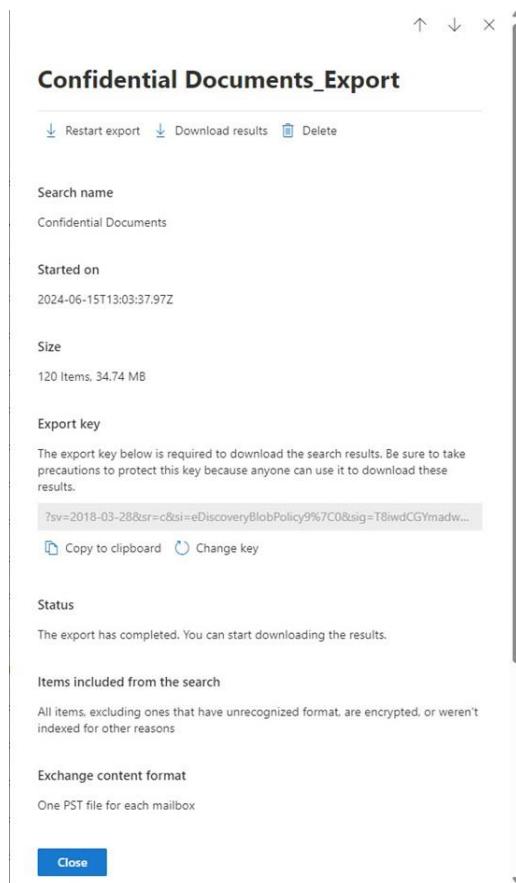


Figure 17-6: Preparing to download the exported results from a search

After Edge downloads the export tool, it installs the tool on the workstation if necessary and then starts the tool. When export results are available in Azure, you can proceed with the export by entering (paste) the export key and the target location for the tool to copy the exported data (Figure 17-7). The export tool then authenticates its access with Azure and downloads the exported data to the selected destination, including metadata for SharePoint and OneDrive documents. If you don't choose to use the advanced option to name the PST to hold exported Exchange content, Purview exports the results to a file called Exchange.PST.

If necessary, you can use **Restart Export** to regenerate the search results (if required) and restart the export process. This action removes any earlier search results stored in Azure and then recopies the search results from the search locations to the holding location in Azure.

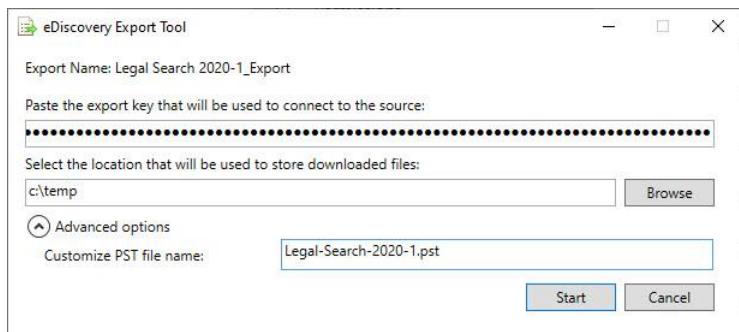


Figure 17-7: The eDiscovery Export tool begins to export information from Azure

The export job creates several sub-folders in the destination to hold the export data. The folder named after the date and time of the export includes an Electronic Discovery Reference Model manifest listing all the exported items. The Exchange folder holds the PST files used to export the data. Figure 17-8 shows the content exported from a SharePoint Online document library. In this case, the export job copied the files to a ZIP file. Once exported to disk, it is easy to give the information found by a search to an external company, such as specialized legal investigators. The external company can then apply whatever tools they choose to analyze the search results.

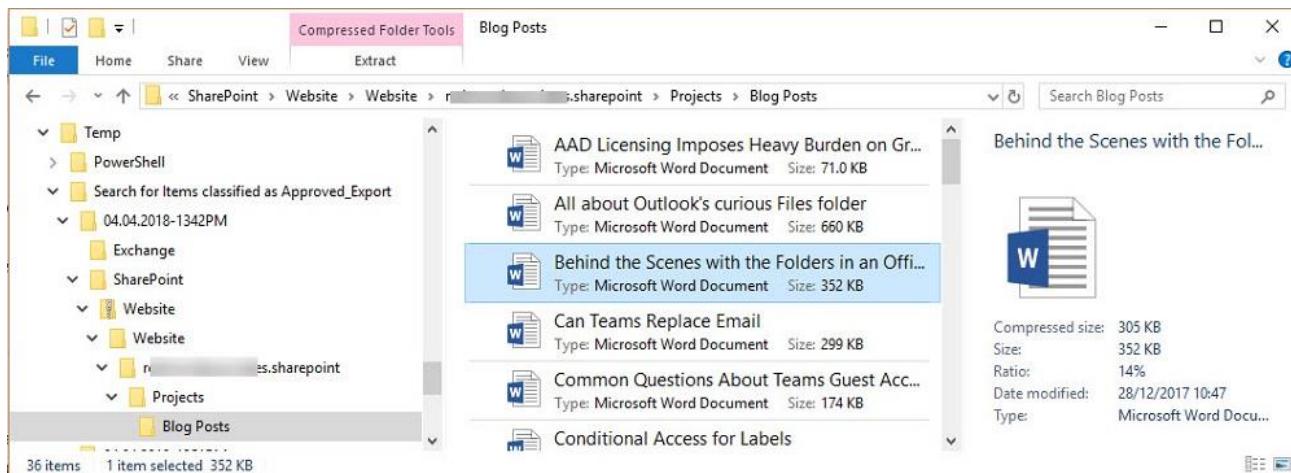


Figure 17-8: SharePoint documents exported from a search

You can export up to 2 TB of data for a single search from up to 100,000 mailboxes. If a search finds more than this amount of data, you will have to split the search to get under the 2 TB limit. One way of doing this is to create several searches, each of which uses the same keyword query but different date ranges. Reflecting that it is a multitenant environment, Microsoft 365 limits a tenant to exporting 2 TB of data in a single day. A tenant can run up to ten export jobs concurrently, but a single user can only run three of those exports.

Protected Documents and Searches

If support for sensitivity labels is enabled for SharePoint Online, the content of documents protected with rights management (Microsoft Information Protection) are indexed and can be found by a content search. If not, a content search cannot find protected documents based on their content and must rely instead on metadata such as the document title, comments, or tags.

Protected documents found by a search are exported like any other item, but they continue to be encrypted and cannot be examined by an investigator unless an arrangement is made to decrypt the files.

The Information Protection chapter contains some advice about how accounts assigned with super-user permission for information protection can run PowerShell code to find and decrypt protected files exported for a search. This is especially important for GDPR data subject requests (and possibly for data erasure requests) because someone must check the content of documents to understand whether they relate to a data subject.

Export Search Report

Being able to review search results gives investigators insight into the kind of information uncovered by a search. However, it would be unreasonable to try to preview every item found by a search, especially when large numbers are involved, in which case an investigator might want to make a broader check of the data uncovered by a search before going ahead to export the data. To export the reports for a search, select the **Select** and then **Export results** from the **Actions** menu. This downloads the same reports (the XML manifest, summary log, and results log) holding details of the information included in the full set of downloaded search results. When you choose to export the report, an export job generates the reports and stores them in Azure. You receive an export key to access the data and can use the same download tool to export the reports to the nominated destination. After checking that the correct results are available, you can then continue to perform a full export.

Export for third-party review: The eDiscovery industry spans many companies that specialize in the analysis of information recovered from IT systems like Microsoft 365. Microsoft has a program to support the export of information recovered by searches in a form that third-party applications can interpret and analyze. The export data exists in a location in Azure Data Services controlled by the third-party. Contact Microsoft to get an up-to-date list of certified partners if you are interested in this capability.

Reopening a Search

You can go back and open a search at any time. Select **Content search** in the Microsoft Purview Compliance portal to list the available searches and select the one you want to work with, and then **Edit search** from the **Actions** menu. If the last search is less than seven days old, you can preview results with the **Review sample** option to see how accurate the search criteria are before making changes. If the search is older, you need to rerun the search before you can preview the sample results.

Searching Targeted Collections

Often, content searches use broad search criteria to find traces of information needed by an investigation. For instance, you might search all mailboxes in the organization for a specific keyword. After analyzing the search results, you can tune them by editing the search to use more precise and focused criteria.

Mailboxes and sites are large containers that can hold thousands of items, so the process of refining a search can take many attempts before the search finds just the desired content. However, if you know the folders where messages and documents are likely stored, you can search against a targeted collection composed of

individual folders. For instance, you might focus a search on just the Inbox and Sent Items folders in a user's mailbox or a folder in a document library.

The queries used by content searches don't accept folder names as search criteria. Instead, you must use the folder identifiers for the target locations. [This article](#) explains how to use PowerShell to retrieve folder identifiers in the correct format from mailboxes to form a content query for a content search.

Compliance Boundaries

When you have the permission to create and run content searches, you can look for anything across the set of supported locations in a tenant, including the ability to pry into sensitive mailboxes or hunt for interesting documents stored in document libraries that you would not otherwise be able to see. Compliance Security Filters allow tenants to impose control over the data visible to investigators by establishing boundaries for searches. Large companies often divide administrative and other responsibilities along geographic or divisional lines. When the time comes to conduct content searches, they might not want those who run the search to be able to include search locations outside their business, country, or region. This makes a lot of sense: someone running a content search to respond to a discovery action in France does not necessarily need to look at German mailboxes. Apart from respecting user privacy, Compliance Security Filters also mean that content searches return a smaller amount of data for investigators to review.

A Compliance Security Filter creates a restrictive view of mailboxes or SharePoint and OneDrive sites within a tenant. When users that conduct searches come within the scope of a filter, they cannot see any data returned by searches except that given by the restrictive view. Therefore, we can set things up that U.S.-based eDiscovery administrators only can see results from mailboxes located in U.S. data centers or that only certain eDiscovery administrators can search particularly sensitive SharePoint sites.

Before starting to plan your filter strategy, you should read the Microsoft [support article about Compliance Security Filters](#). The key point is that you can only create and manage filters through PowerShell. To guide you in creating a filter, answer the following questions:

- **Who will the filter apply to?** You can specify individual users or use the name of a Compliance role group, including a role group created specifically for this purpose. You cannot use a distribution list, Microsoft 365 Group, or security group to define a set of users.
- **What can the users do?** You can restrict users to individual compliance actions (Export, Preview, Purge, Search) or "All". You cannot specify two or three actions. In most cases, you will want to use Search or All.
- **What can the users see?** You can combine mailbox and SharePoint locations into a single filter that works across multiple workloads. In both cases, you can have filters that look for specific objects (mailboxes or sites) or content (based on KeyQL queries).

With these points in mind, here is a simple filter that applies to a single named user to allow them to perform all compliance actions while restricting them to searching mailboxes with a specific value in their *CustomAttribute6* property. To create the Compliance Security Filter, connect to the compliance endpoint and run this command:

```
New-ComplianceSecurityFilter -FilterName VikFraudSearch -Users "Marc Vigneau" -Filters "Mailbox_CustomAttribute6 -eq 'POI'" -Action All
```

To add a mailbox to the set that searches performed by the users identified in the filter can find, we update the *CustomAttribute6* property as follows:

```
Set-Mailbox -Identity Kim.Akers -CustomAttribute6 POI
```

After updating the mailboxes, you can test the filter to check the set returned with *Get-Recipient*:

```
Get-Recipient -RecipientType UserMailbox -RecipientPreviewFilter {CustomAttribute6 -eq 'POI'}
```

Now that we know that the filter is valid and returns a set of mailboxes, we can test it with a search. Log into the Microsoft Purview Compliance portal using the account of one of the users restricted by the filter. The user must have the necessary permission to run searches. Create a new search for all mailboxes with a query that you know will find some information. Launch the search and wait for it to complete. The results should reflect the filter in terms of the number of locations scanned and the amount of information found.

Now log into the Microsoft Purview Compliance portal as another administrator who is not restricted by the filter and run the same search again. This time the results should be very different. Figure 17-9 shows an example of a content search run by restricted (left) and unrestricted (right) eDiscovery administrators. The restricted search only scans 2 mailboxes while the unrestricted search looks through 468. The number of found items is also different, as you'd expect.

Secret Investigation	
Summary	Summary
Search statistics	Search statistics
Description	Description
Fraud	Fraud
Last run on	Last run on
2021-05-22T15:39:32.813Z	2021-05-22T15:37:48.12Z
Searched by	Searched by
Marc Vilas	Tony Redmond
Search conditions	Search conditions
Fraud	Fraud
Status	Status
The search is completed	The search is completed
298 items(s) (4.21 GB)	2,124 items(s) (4.71 GB)
28 unindexed items, 76.51 MB	4,256 unindexed items, 2.67 GB
2 mailbox(es)	468 mailbox(es)
All sites	All sites

[Actions](#) [Review sample](#)

[Actions](#) [Review sample](#)

Figure 17-9: The result of applying a search filter

Microsoft suggests many other examples of Compliance security filters [in its documentation](#), including how to filter mailboxes based on the ISO 3166-1 code (for example, 124 is the three-digit code for Canada while 372 is the code for Ireland). One example of obvious interest is a filter that restricts access to confidential or sensitive mailboxes. The code to create such a filter first finds the distinguished name of a distribution list called the "Senior Leadership Team". The members of the list are the mailboxes that we want to restrict. We include the distinguished name in the filter to stop anyone who runs a search against these mailboxes from being able to preview items found by the search.

```
$DG = (Get-DistributionGroup -Identity SLTDL).DistinguishedName
New-ComplianceSecurityFilter -FilterName NoSLTPreview -Users All -Filters "Mailbox_MemberOfGroup -ne '$($DG)'"
-ACTION Preview
```

The *Get-ComplianceSecurityFilter* cmdlet reveals the details of the filter:

```
Get-ComplianceSecurityFilter -FilterName NoSLTPreview
```

```
FilterName : NOSLTPREVIEW
Description :
Action     : Preview
Users      : {all}
Filters    : {Mailbox_MemberOfGroup -ne 'CN=DL Senior Leadership
Team,OU=tenant.onmicrosoft.com,OU=Microsoft Exchange Hosted
Organizations,DC=EURPR04A002,DC=prod,DC=outlook,DC=com'}
```

This kind of filter effectively stops casual browsing of preview samples from sensitive mailboxes by people who should know better. It does not stop searches from finding items, nor does it stop eDiscovery administrators from being able to export items found by the searches. The downside of using a filter is that it applies to all content searches, including those executed by people that might legitimately have reason to preview content found in the sensitive mailboxes.

Users cannot preview items found by a content search in the designated mailboxes, but they can preview documents and other items (like PDFs) found in sites covered by searches. To ensure full confidentiality for the Senior Leadership Team, you need to define a site filter to protect these locations. This filter restricts access to documents found in the document library. In this context, "All" means members of the eDiscovery manager role group rather than all users.

```
New-ComplianceSecurityFilter -FilterName NoSLTPreviewDocs -Users "All" -Filters "Site_Site -ne
'https://tenantname.sharepoint.com/sites/SLTGroup'" -Action Preview
```

You can create a filter with clauses for multiple workloads (a filter list). Here is a filter with two clauses: one for U.S.-based mailboxes and the other for a specific SharePoint site:

```
New-ComplianceSecurityFilter -FilterName CountryFilter -Users annb@contoso.com -Filters
"Mailbox_CountryCode -eq '840'", "Site_Site -eq 'https://tenant.sharepoint.com/sites/Confdocs'/"'
-Action All
```

The Effect of Filters on Content Searches

In its documentation, Microsoft explains that:

*"The permissions filter is added to the search query when a Content Search is run. The permissions filter is essentially joined to the search query by the **AND** Boolean operator."*

and:

*"In a Content Search query, multiple permissions filters are combined by **OR** Boolean operators. So results will be returned if any of the filters are true. In a Content Search, all filters (combined by **OR** operators) are then combined with the search query by the **AND** operator."*

If you use multiple filters, the filters are joined with the query (AND) and then combined (OR). This allows the search to find all the content per the query and then apply each filter to arrive at a combined set of results. The exact results that any action (search, preview, or export) produces depend on the actions specified in each filter. The ability to combine filters with content searches creates a great deal of flexibility in what you can do to control searches, even if it might take some time and effort to arrive at the filters needed to generate the desired result.

Note that you cannot exclude specific public folders using a search filter. The filters only work for user and group mailboxes and SharePoint and OneDrive sites.

Auditing of Search Activities

Administrators and eDiscovery managers access and view user content through content searches. Being able to access messages, documents, and other potentially sensitive user content is necessary as otherwise, you'd

never be able to perform a compliance search and export its results. Because searches use privileged access to user data, the Microsoft Purview Compliance portal captures audit records when investigators create and run content searches and eDiscovery cases, and for search actions against results like preview, export, and purge. Having audit information to hand enables organizations to ensure that they meet their requirements to protect confidential user information under regulations such as GDPR.

You can review the audit records for search activities through the audit log search in the Microsoft Purview Compliance portal. This is a reasonable approach when you know the time and date when an activity occurred, and you only need to review a small number of activities.

If you want to process a lot of audit records, perhaps to verify that administrators are not abusing their access to user information, it is better to use PowerShell to interrogate the audit log and extract the records you might be interested in analyzing. This example (see the Auditing and Reporting chapter for a more extensive discussion of using audit log data) extracts records captured when users view, export, or preview the results of content searches, and outputs a CSV file. The CSV file can be opened and reviewed in Excel or imported into Power BI.

```
$StartDate = (Get-Date).AddDays(-7) ; $EndDate = Get-Date
$Records = Search-UnifiedAuditLog -StartDate $StartDate -EndDate $EndDate -Operations
"SearchExportDownloaded", "SearchViewed", "ViewedSearchPreviewed" -ResultSize 1000 -SessionCommand
ReturnLargeSet
If (!$Records) {
    Write-Host "No audit records for content search activities found." }
Else {
    Write-Host "Processing" $Records.Count "audit records..."
    $Report = [System.Collections.Generic.List[Object]]::new()
    ForEach ($Rec in $Records) {
        $AuditData = ConvertFrom-Json $Rec.Auditdata
        $ReportLine = [PSCustomObject]@{
            TimeStamp = Get-Date ($Rec.CreationDate) -format g
            User      = $AuditData.UserId
            Action     = $AuditData.Operation
            Exchange   = $AuditData.ExchangeLocations
            SharePoint = $AuditData.SharePointLocations
            Query      = $AuditData.Query }
        $Report.Add($ReportLine)
    }
}
$Report | Export-Csv c:\temp\SearchAuditRecords.csv -NoTypeInformation
```

Microsoft Purview captures audit records for many other content search and eDiscovery activities, and it is easy to modify the PowerShell code shown above to include multiple other activities and export those records for later analysis.

Microsoft Purview eDiscovery

Content searches are useful in a variety of situations. Sometimes it is to find information that a user has “lost,” and sometimes it is to find information for more serious reasons, such as looking for evidence of corporate or personal malfeasance needed to prove a point for internal or external purposes. If the information exists in an indexed location, content searches will find it.

Good as content searches are at finding information, searching is only part of the eDiscovery lifecycle. And while the results of an individual search might be critical to proving or disproving a point, many eDiscovery projects involve teams of investigators using multiple searches looking for different sets of information. eDiscovery cases deliver the structure needed by investigators to organize their work, including searches, holds, and exports.

Microsoft Purview eDiscovery functionality divides into standard and premium. Standard eDiscovery is available to tenants with E3 licenses; you need E5 licenses or the Microsoft 365 E5 Compliance license to use Premium eDiscovery.

Standard eDiscovery

To access the cases created by standard eDiscovery, go to the **eDiscovery** section in the Microsoft Purview Compliance portal and select Standard. This reveals the set of eDiscovery cases available to the signed-in user. Some of the cases are “Active,” meaning that investigators might still be working on these cases. Closed cases are still available, and investigators can reopen them if necessary.

eDiscovery Case Components

If you open an eDiscovery case, you see that its major parts are:

- **In-place holds to ensure that users cannot remove information.** Holds ensure that Microsoft 365 workloads retain information needed for an eDiscovery case in their original location. A hold covers a set of locations (Exchange mailboxes, SharePoint and OneDrive for Business sites, and Exchange public folders) and criteria to specify the items in those locations that come under the scope of the hold. A hold can be as broad as to include all items in all available locations within a tenant or as specific as to hold just one or two items found with a highly-specific phrase in a selected mailbox.

All items that fall under the scope of the hold stay in the specified sites and mailboxes (including those used by Microsoft 365 Groups). Users can try to remove items that come under the scope of the hold, but if this happens, the workloads keep a copy of the item until the hold expires. In-place holds on Exchange mailboxes include both the primary and archive mailboxes. Standard content searches do not include the ability to place holds on sources. Note that a user account must have at least an Exchange E3 license before you can place it on hold. The license must stay assigned to the account for the duration of the case. An eDiscovery case can include multiple holds, each of which has its own target set of locations and hold criteria.

- **Searches are used to gather** information of interest to the case. The searches in an eDiscovery case behave very much like content searches. An eDiscovery case might only have one search, but it might equally deploy multiple searches, each of which focuses on different material. Each search covers a different aspect of the case and might look for content based on different queries, various locations, or even content created in different languages. The intention is that multiple searches allow investigators great flexibility in how they approach looking for information because they can create a series of searches to interrogate information with different criteria. The searches created for eDiscovery cases do not appear along with other content searches because they belong to an eDiscovery case. Both types of searches use the same technology to find information using the content indexes populated from Exchange Online and SharePoint Online data. The names assigned to searches belonging to eDiscovery cases must be unique and not clash with standalone content searches.

One difference between regular content searches and those executed within an eDiscovery case is that in a case, you can specify the special *“Locations on hold”* target for a search, meaning that you want to search the held content in all the locations included in a case. For example, assume two holds exist for the case. The first covers two mailboxes and two sites and the second spans a further twelve mailboxes. In this instance, *“Locations on hold”* means searching the held content in the fourteen mailboxes (including their archive mailboxes if these exist) and two sites. If the scope of any of the holds belonging to a case changes (for example, the addition of new locations), the scope of *“Locations on hold”* changes to match the holds when you refresh the search results. Searching against

on-hold content is a current workflow scenario in eDiscovery situations where investigators place locations such as mailboxes or sites on hold before starting to search those locations.

- **Exports of information gathered by the searches.** An eDiscovery case might use several searches to find different sets of information. You can export results from a single search using the same steps as for exporting results for a normal content search, or you can combine the results of multiple searches belonging to a case into a single set of data to give to external investigators.

When you combine results from multiple searches, the search combines the queries using the OR operator to form an overall query and runs the query against the locations to generate the search results. In other words, the search results created for export come from a single search instead of manually combining the sets generated for the individual content searches. The results of the searches are deduplicated so that the export includes only a single copy of an item found in a location. Because of the way that a combined search brings multiple search queries into one, the overall keyword limit for a query (500) might be met. If so, you will see an error and the search will end. To achieve the desired result, you must combine fewer searches or simplify the queries.

Case Members

Each case has one or more members, each of whom must be a member of the eDiscovery Manager role group. The members are the only people who can access the results of the searches associated with a case. The eDiscovery Manager role group divides into two sub-groups:

- **eDiscovery Managers** deal with specific cases. They only have access to the content belonging to those cases. When a user accesses the Microsoft Purview Compliance portal, they can only see the cases where they are the eDiscovery Manager. They cannot see the cases belonging to other eDiscovery Managers.
- **eDiscovery Administrators** have oversight over all eDiscovery cases and can view and edit any case within the tenant regardless of who is the eDiscovery Manager for the case. To access a case, an eDiscovery administrator adds themselves as a member of the case.

Logically, a very small set of users within a tenant should be eDiscovery Administrators.

Case Management

When you open the eDiscovery section, the Microsoft Purview Compliance portal shows you all the cases that your account manages or has access to. You can then select an existing case or **Create a case** to initiate a new case. When you open an existing case, you can use the **Settings** tab to access the properties of that case, including the members working on the case and its status. Figure 17-10 shows that the selected case has three members plus anyone who is a member of the Senior Investigators role group.

Access & permissions

Users

		+ Add	Remove	3 items	Search
Name	Email				
Tony Redmond	Tony.Redmond@				
Kim Akers (She/Her)	Kim.Akers@office365itpros.com				
Ben Owens (DCPG)	Ben.Owens@office365itpros.com				

Role groups

		+ Add	Remove	1 item	Search
Name	Description				
Senior Investigators	Senior Investigators				

[← Close](#)

Figure 17-10: Viewing members for a Standard eDiscovery case

You can use the same form to manage the status of the case by closing or removing the case. Due to the nature of corporate investigations, eDiscovery cases are often long projects that span several years. It is not unknown for cases to last five years or more.

Creating a New eDiscovery Case

From the eDiscovery section of the portal, click **Create a case** to begin. You can then input the name of the new case and some details to describe the need for its creation. Make sure that the name of the case clearly indicates what it does while the description gives additional information to anyone reviewing the case about its purpose and who authorized the investigation. Click **Save** to continue and be returned to the portal.

Creating a new case creates the eDiscovery case container for searches, holds, and other activities. Nothing much exists in the case at this point, so we should select and open the case to begin adding these elements. The case screen then displays to allow us to access the different components.

eDiscovery Case Holds

The next step is to create one or more holds to preserve the content needed for the case. You can use multiple holds for an eDiscovery case but in most cases, one hold that applies to Exchange mailboxes and SharePoint and OneDrive for Business sites is enough. Click **Holds** to access that section of the case and then **Create (+)**. The steps to create a hold are:

- **Name the hold.** Assign a unique name for the hold along with an optional description. Ideally, the description should tell an eDiscovery manager the intention behind the hold and link the hold to the eDiscovery case. For instance, if the case name is "Investigation 2020-003," then you might call the holds in the case "Investigation 2020-003 #1," "Investigation 2020-003 #2," and so on, following whatever naming convention makes sense.
- **Define the locations** the hold will cover. The locations divide into:
 - Exchange mailboxes (user, shared, and group mailboxes). Group mailboxes include group conversations and calendars for Microsoft 365 Groups and the compliance records created for Teams and Viva Engage conversations. Compliance records for Teams personal chats and

- private channel conversations come from user mailboxes. If you select a distribution list, Exchange expands the membership and adds valid mailboxes to the hold.
- SharePoint Online sites (including those used by Teams and Microsoft 365 Groups) and OneDrive for Business accounts.
- Exchange public folders. You can include or exclude all public folders, but you cannot select specific public folders.
- **Define the search criteria** to find items to hold. The criteria are like those used for content searches and include keywords and conditions.

A hold does not have to include a query, and if it does not, it means that you want to apply a hold to every item in the selected locations. You do this when you want to preserve complete mailboxes or sites because you are unsure of the material that you want to hold. Figure 17-11 shows the summary for the creation of a new hold.

New Hold

The screenshot shows the 'Review your settings' step of the 'New Hold' wizard. On the left, a vertical checklist indicates steps completed: 'Name your hold' (checkmark), 'Choose locations' (checkmark), 'Query' (checkmark), and 'Review your settings' (blue circle). The main pane displays the following settings:

- Name:** Finance Trading Hold LD-2021 17-15
- Description:** Hold on executive mailboxes
- Choose locations:**
 - Exchange email:** Jessica.Chen@office365itpros.com, Chris.Bishop@office365itpros.com
 - SharePoint sites:**
 - Exchange public folders:**
- Query:**
 - Query:** "Trading Profits"
 - Edit query:**

At the bottom are 'Back', 'Submit' (highlighted in blue), and 'Cancel' buttons.

Figure 17-11: Creating a hold for a Standard eDiscovery case

After creating the hold, the Microsoft Purview Compliance portal publishes its details to the workloads for the selected locations. It can take some time to synchronize across all workloads to make the hold effective everywhere, but it should certainly be in place within a few hours.

To view information about a hold, select it to reveal a details pane. Here you find the current hold statistics provided by the relevant workloads to show how many items come under the scope of the hold, the date and time of the last modification for the hold, and some statistics about the items which come within the scope of the hold. If a change is needed for the hold parameters, you can edit the hold settings.

Applying Holds to Teams Private Channels: Two steps are necessary to apply a hold to information belonging to a Teams private channel. First, you assign the hold to the SharePoint site for the private channel by specifying the URL of the site. Second, you add at least one mailbox of a member of the private channel to the hold. Compliance records for messages posted to private channels are copied to the

mailboxes of all members, so messages for the private channel come within the scope of the hold when you add a member's mailbox. The hold might lapse if that member's account is removed from Microsoft 365, so it's best to add at least two member mailboxes.

eDiscovery Case Searches

After applying a hold to make sure that users can no longer remove any content that we might need for our eDiscovery case, we move on to searching. The simplest eDiscovery case has just one search, but more complex cases might use multiple searches, each of which takes a different approach to look for material of interest. The idea is that an investigator can use different searches to home in on the information they need. Apart from the ability to use different queries to focus on different material in each search, the searches in a case might target different locations. One search might focus on a set of mailboxes and look for a specific item. A second search might look for some documents in a SharePoint Online site and a third might concentrate on a single user and retrieve a much wider range of content from their mailbox. Like other searches, you can reiterate several times to refine the results retrieved by search criteria until you find the desired content.

Click **Searches** to go to the search page and then **New search** to create a new search. The same steps to create a regular content search occur when creating a search in a Standard eDiscovery case. These are:

- Name the search.
- Identify the target locations from Exchange mailboxes, SharePoint sites, and Exchange public folders. Select all locations or choose individual mailboxes or sites. If you want the search to apply only to locations on hold for the case, select **Locations on hold**.
- Enter the keywords and conditions for the search to find items.
- Review the search parameters and submit them for processing.

The Microsoft Purview Compliance portal goes ahead and launches a preview search. When the preview search finishes, you can review sample items to understand if the search finds the right items.

eDiscovery Case Exports

After investigators run searches to find the information they need, they can then export the search results. This process works like exports for content searches, with the notable exception that you can select to export the results for multiple searches in the same operation. The same general approach is used:

- Access the search whose results you want to export.
- Click the **Actions** button and select **Export Results**.
- Set the export characteristics:
 - Decide what items the search finds to include in the export (all items, all items except those that are in an unrecognized format, encrypted, or indexed, or just the items in an unrecognized format, encrypted, or unindexed).
 - Decide what PST structure to use for mailbox items (one PST per mailbox, one PST for everything, one PST with all messages in a single folder) or to use individual MSG files.
 - Decide whether to deduplicate the search output.
 - Decide whether to include versions (if available) for SharePoint and OneDrive for Business documents.
- A background job named "Search Name_Export" then exports the search data to a secure Azure location.
- When the search data is available, you download it to a workstation using a secure key generated by Microsoft 365 as credentials to access the data.

- Investigators use the downloaded PSTs, MSG files, and documents to review the information and assess its content.

Closing eDiscovery Cases

Eventually, when the investigation for an eDiscovery case winds down, the case manager can close the case by selecting the **Close case** option. When you close a case, the underlying workloads release the holds for the case. It can take some time for workloads to process the hold release commands. After the workloads respond to confirm that they have removed the holds, the case status is set to closed, and the time and date of closure and the user who invoked the closure are captured in the case properties. Later, if the case records are not needed, you can remove the case after first releasing any holds belonging to the case. These holds are inactive, but they exist in case someone wants to reopen the case and reestablish the holds, so they must be removed before you can remove the case.

Warning! Depending on the age of the data involved, closing a case could result in background maintenance processes removing the items that are no longer on hold. Exchange Online keeps mailbox items until the deleted items retention period expires while SharePoint Online and OneDrive for Business keep items for 30 days after the hold terminates to avoid any inadvertent data loss. Even so, closing a case is not something to do on a whim. If you make a mistake and need to reactivate a case, the case manager can reopen the case. However, reopening a case does not reestablish the holds that were previously in place and they will have to be recreated by going to the Holds section of the case, selecting each hold, and then taking the **Turn It On option** in the action pane. The gap in time between removing the original holds and reapplying new holds creates the potential that data will be removed from the sources during this period. The exact amount of data that might be lost is unpredictable because it depends on whether the background processing to remove data from sources has run and removed data.

Premium eDiscovery

The cost of large-scale eDiscovery actions can be staggering. It is expensive enough to retrieve all the items necessary to satisfy a discovery order handed down by a judge. It can be extraordinarily expensive to individually process each piece of information delivered in response to a discovery order. The number of individual messages or documents can easily mount into the low millions and, when very large companies are involved, quickly grow into tens or hundreds of millions of items. The problem then becomes how to locate the proverbial needle in the haystack.

In the early days of eDiscovery, it was common to print off copies of emails and documents for lawyers to review. This process was tedious, paper-bound, and expensive. Lawyers are paid by the hour and lots of IT effort was necessary to generate the material. However, the technique worked reasonably well then because a small volume of email or electronic documents was involved, and the major focus was on paper documents and communications such as faxes and telexes. Today, the situation has changed because paper files are no longer the focus of business documentation and the volume of items stored and available to be discovered has grown massively. If a discovery order turns up 50,000 items, you don't want to incur the cost of having a professional check each item.

Basics of Premium eDiscovery

Although the standard approach to eDiscovery (hold, search, and export) is suitable for investigations that generate tens of thousands of items, human examination of every item retrieved by a search is a time-consuming and expensive exercise. To address the problem, Premium eDiscovery applies algorithms to refine very large sets of search data retrieved to make it easier for investigators to find what they are looking for. Premium eDiscovery is currently capable of ingesting data sets spanning up to several million items. Microsoft

expects that they will be able to lift the limit and at that point, Premium eDiscovery will be able to process as much data as any organization might need.

Consider a situation where a search uncovers a hundred thousand items. The choices are then to:

1. Refine the criteria for content searches to return the most precise set of discovered information and then review all the found items to decide which are useful and which are not. This is an acceptable tactic for relatively targeted searches where the desired material can be accurately described in terms of search criteria. For instance, looking for evidence that a specific phrase was discussed in an email sent between four known individuals.
2. Ingest the output of content searches, use analysis to parse the set of discovered files, and home in on the material that needs close examination, followed by a review of sample items by expert investigators to find items that are of relevance and those that are not. The items deemed to be of relevance are then fed through machine learning algorithms to construct filters (think of them as very complex search queries) that are used to interrogate the complete set of files to locate the desired information.

The first choice described above is roughly what's possible using the Standard eDiscovery features. The second is what becomes feasible with Premium eDiscovery.

The current implementation of Premium eDiscovery uses a workflow described in the [Electronic Discovery Reference Model](#) (EDRM). The stages in the workflow are:

- **Identification:** Knowing whose data should be searched is essential to an investigation. People who might own information needed by the investigation are called **data custodians** or **people of interest**. These are Microsoft 365 accounts that you might want to add to a Premium eDiscovery case and search for data (Figure 17-12). The mailbox and OneDrive for Business site (custodial locations) for each custodian can be included in the case along with other locations they access, such as Teams, shared mailboxes, and SharePoint sites.
- **Preservation:** After you add custodians to a case, you can create **in-place holds** to preserve selected data needed for the case. You can also add holds that cover people who aren't custodians. Premium eDiscovery includes the ability to **send notifications** to custodians by email to tell them that their accounts are under hold and then track responses from the custodians.
- **Collection:** After identifying relevant data sources, you collect information from those sources by using a **special form of content search**. Information remains in the data sources and users can continue to work with it as usual.
- **Processing:** Once searches have located relevant data for the case, you process the data. Like when you export results from a content search, the eDiscovery case **copies data found by searches** to an Azure storage location called a review set. The review set is a static view of the case data that can be analyzed and reviewed for relevance.
- **Review:** Investigators can now look at specific items in the review set to decide if they have the right information or need to query the data to reduce the set to what is most relevant to the case. Investigators can annotate and tag items during this phase. If necessary, case managers can [load data from outside Microsoft 365](#) for inclusion in the review.
- **Analysis:** Premium eDiscovery includes a set of tools to help reduce the data from the review set down to the most relevant information. Reducing the amount of data for investigators (and lawyers) to consider limits the costs of eDiscovery.
- **Production and Presentation:** When the final set of most relevant items is identified, you can export them from the review set. Export can be in the native format of documents or an EDRM-specified format suitable for ingestion into third-party review applications used by external experts.

Source name	Source type	Locations	Source status	Indexing status	Hold status	Index date
Sean Landy	Data location	1	Active	Fully indexed	On hold	Nov 2, 2023 6:50 PM
Microsoft Graph Gurus	Data location	1	Active	Fully indexed	On hold	Nov 2, 2023 6:50 PM
R&A Projects	Data location	1	Active	Fully indexed	On hold	Jun 22, 2023 12:28 PM

Figure 17-12: Custodians for a Premium eDiscovery case

Premium eDiscovery can process exports involving up to 5 million documents or 500 GB (whichever is smaller). To deal with such large amounts of data, the export splits processing across multiple ZIP files, which investigators can later combine in a single location to reform the complete set. One thing to be aware of is that Premium eDiscovery processing is slower than many people expect. It takes time to perform the complex background processing performed by many actions. Patience is certainly an advantage when dealing with these cases.

Premium eDiscovery is a specialist activity and apart from assigning the necessary permissions to accounts used by investigators, it is unlikely that most tenant administrators will need to become involved in these cases. Instead, it will probably be specialized compliance managers that create and run the cases. For more information, see [Microsoft's documentation](#).

Premium eDiscovery Licensing: While the accounts of users who create the input set for a Premium eDiscovery search only need Office E3 licenses, every user included in the scope of a Premium eDiscovery analysis needs an Office E5 license or Microsoft 365 E5 compliance license. This might sound like Premium eDiscovery is an expensive proposition, but the purpose of the content search is to refine the set of content for Premium eDiscovery to analyze. Refining the input set should mean a reduction in the number of users covered by the set too, so the number of Office E5 licenses you need is probably less than you think. From April 16, 2021, users need an appropriate license to create new Premium eDiscovery cases. Cases created before that date remain accessible to administrators without a license.

Data Search Cases

Article 15 of the European Union's General Data Protection Regulations (GDPR) grants a data subject (a person) the right to have a data controller (the organization owning a tenant) provide them with a copy of their data. According to [Microsoft's Data Subject Guide](#), 90% of an organization's data stored in Microsoft 365 is in Word documents, Excel spreadsheets, PowerPoint presentations, OneNote files, and Outlook messages. The data are indexed and searchable. Some data cannot be found by content searches, so the information you can find through a DSR case is not necessarily all the personal information belonging to a data subject existing in a tenant. For instance, videos featuring the user stored in Stream cannot be found through eDiscovery, so extra effort is needed to review and retrieve this information if necessary.

To help tenants respond to data subject requests, the Microsoft Purview Compliance portal supported the creation and management of special eDiscovery cases, called user data search cases under *User data search* in the eDiscovery section. On August 30, 2023, Microsoft retired the User data search tool. The replacement is

eDiscovery standard. Existing User data search cases and searches appear in eDiscovery Standard and can be processed using that solution.

To create a new eDiscovery standard case for the same information as a user data search, first create a new case. In the new case, create a search and access the KeyQL editor. Copy the query shown below into the search, replacing the example user name shown here with the user principal name of the person to search for:

```
participants:"Kim.Akers@office365itpros.com" OR author:"Kim.Akers@office365itpros.com" OR  
createdby:"Kim.Akers@office365itpros.com"(ItemClass=IPM.Document)(ItemClass=IPM.Note)(ItemClass=IPM.  
Note.Microsoft.Conversation)(ItemClass=IPM.Note.Microsoft.Missed)(ItemClass=IPM.Note.Microsoft.Conve  
rsation.Voice)(ItemClass=IPM.Note.Microsoft.Missed.Voice)(ItemClass=IPM.SkypeTeams.Message)
```

Make sure that the query runs against all Exchange Online and SharePoint Online locations. eDiscovery standard is not a prerequisite. A standard content search also works.

Things to remember about processing the results found by the search include:

- The target locations defined for searches are static. If new mailboxes or sites are added to the tenant after you create the case, the search will ignore those locations. However, given that most user data searches are backward-looking, the need to include new locations in the search is not usually an issue.
- Searches can only find information in cloud locations. If you run a hybrid organization, you must run separate searches to find relevant information in the on-premises locations. The current versions of Exchange Server and SharePoint Server include the ability to run eDiscovery searches to find and export information.
- Searches interrogate more than the relevant individual's mailbox and OneDrive for Business account. It finds items created by the data subject in other mailboxes (user, group, and shared) and SharePoint Online and OneDrive for Business sites. Because of the way Exchange Online delivers individual copies of email to recipients, it is likely that many duplicate messages exist in mailboxes.
- When you export protected email (with sensitivity labels), the export decrypts the messages. This doesn't happen for content search exports in eDiscovery standard (it does in eDiscovery premium). Some other arrangement must be made to remove sensitivity labels from protected documents before the files are examined and eventually handed over to the data subject.
- [Article 15 of the GDPR](#) says that organizations must respond to data subject requests within a month of the request. It is therefore important to keep an eye on the progress of cases and highlight instances when the finalization of search results are delayed.
- Running a search to find and export information is only the start of a response. Searches do not address the need to remove information about a data subject (the right to be forgotten defined in [Article 17 of the GDPR](#)). However, the reports generated for a search tell you where data matches are found and act as a guide for checking individual locations and items to decide whether items are relevant and what content should be removed. Remember, not all data found for a data subject needs to be removed from locations as it is legally permissible to keep data under certain circumstances, such as the requirement to comply with a legal obligation.

When you are happy that a user data search finds the information necessary to satisfy the data subject request, you can export the information as normal and prepare the content (usually PSTs and documents) to give to the data subject. A further check is always needed to exclude anything in the exported data that is unrelated to the data subject. For instance, if the name of the data subject is common (like John Smith), some of the matches returned by a search probably do not refer to the data subject. It is also possible that some of the information is commercially sensitive and should be reviewed by the business and potentially by legal advisors before its release.

Priva Subject Rights Requests

The Priva Subject Rights Requests solution is part of the [Microsoft Priva privacy management suite](#). It is a more developed and comprehensive version of DSR processing which Microsoft licenses on a per-request basis. Organizations can run a free trial of Priva Subject Rights Requests for up to 90 days or 50 requests (whichever limit is reached first). Priva Subject Rights Requests include:

- Customized content searches to find information relating to a data subject.
- Retrieval of information to an Azure blob storage container for review (annotation, tagging, redaction, etc.). During retrieval, Priva attempts to identify high-priority items for reviewers to consider.
- Generation of reports.
- Integration with Teams for collaboration (by default, each request creates a team for those working on the request to use with the person who creates the request being the team owner).
- Workflow based on Power Automate (customizable by the organization).
- Processes requests in line with compliance regulations including GDPR, the California Consumer Privacy Act (CCPA), UK Data Protection Act (UDPA), U.S. State Breach Notification Laws (USBNL), and U.S. Patriot Act (USPA).

Using PowerShell with Content Searches

Many compliance operations are quite complex, and it is usually best to execute eDiscovery and search operations through the portal. The information about running searches with PowerShell offered here gives some insight into what happens in the background so that you have a starting point for further investigation, if necessary. Remember that to run these cmdlets, you must connect a PowerShell session to the compliance endpoint. In addition, the account used must have the required Compliance permissions to perform whatever action you wish to take. If the account does not have the right permissions, not all cmdlet parameters are available. For example, if the account does not hold the eDiscovery Manager role, you cannot add the export action to a search.

Creating and Running a New Content Search

To create a new content search, run the *New-ComplianceSearch* cmdlet, followed by the *Start-ComplianceSearch* cmdlet to start the search with the specified query to find items. For example, let's assume that we are interested in finding out whether any items exist in user mailboxes that have a specific phrase in their subject delivered in a certain period. Perhaps these items belong to a potential phishing attack. This command creates a simple content search to look for items based on some subject text delivered in a certain date range.

```
New-ComplianceSearch -Name "Look for Phishing Items" -Description "A search to locate suspicious phishing items" -PublicFolderLocation A11 -ExchangeLocation A11 -ContentMatchQuery '(Subject: "Phishing") AND (Received:06/01/2016..04/05/2021)' -AllowNotFoundExchangeLocationsEnabled $True
```

Setting *AllowNotFoundExchangeLocationsEnabled* to \$True means that the search will check the cloud-only mailboxes used to hold data for hybrid (on-premises) and guest accounts.

After creating the search, we use the *Start-ComplianceSearch* cmdlet to execute the query. Over the lifetime of a search, any time it has been longer than seven days since the search was run, you should run *Start-ComplianceSearch* to scan the target locations and refresh the results.

```
Start-ComplianceSearch -Identity 'Look for Phishing Items'
```

The *Get-ComplianceSearch* cmdlet fetches information about the search. For instance, this command checks the status of the search:

```
(Get-ComplianceSearch -Identity 'Look for Phishing Items').Status
```

The search status begins with "Starting" as the search engine initializes and evaluates the search parameters. It moves to "InProgress" when the search processes items in the target location. The search status reaches "Completed" when search results are ready for review. The number of items returned by the search is always interesting, so we can see this data with:

```
(Get-ComplianceSearch -Identity 'Look for Phishing Items').Items
```

Although content searches are much faster than their on-premises counterparts, a search across many locations can take some time to complete. Inside a script, we might want to have a loop to check the search status and then continue to some other processing once the search completes. Here is a simple loop that checks the search status every five seconds.

```
$Search = "Contoso Review of Patent Information for Project Alpha"
Start-ComplianceSearch -Identity $Search
do
{
    Write-Host "Searching..."
    Start-Sleep -s 5
    $Test = (Get-ComplianceSearch -Identity $Search).Status
}
While ($Test -ne 'Completed')

Write-Host "All done. Items found:" (Get-ComplianceSearch -Identity $Search).Items
```

The full output of the `Get-ComplianceSearch` cmdlet includes more detail than the search status and the number of found items. For example, the information returned about this content search shows the number of items found by the search in different mailboxes:

```
Get-ComplianceSearch -Identity 'Search for Phishing Items' | Format-List Items, Size,
SearchStatistics
```

The information delivered in the `SearchStatistics` property is in JSON format. To see the essential statistics, do the following:

```
$Stats = Get-ComplianceSearch -Identity "Contoso Review of Patent Information for Project Alpha" |
Select-Object -ExpandProperty SearchStatistics
$data = $Stats | ConvertFrom-Json
$data.ExchangeBinding.Search

Name      :
Sources   : 12
SourcesRaw : 12
ContentItems : 684
ContentSize : 154.32 MB
ContentSizeRaw : 161813705
HasFaults  : False
```

To see the search results for each location, examine the `SuccessResults` property:

```
Get-ComplianceSearch -Identity 'Contoso Review of Patent Information for Project Alpha' | Select-
Object -ExpandProperty SuccessResults
```

```
Location: Kim.Akers@office365itpros.com, Item count: 34, Total size: 24165076
```

There can be many lines of information detailing locations where a search finds items, including the special mailboxes used to store compliance records generated by Teams and Viva Engage by guest and hybrid accounts. To report the set of locations where a search finds information, we can use [regular expressions and the special \\$Matches hashtable](#) to capture results. For example:

```
[array]$Results = Get-ComplianceSearch -Identity "Project Derrigimlagh" | Select-Object
-ExpandProperty SuccessResults
$RecipientList = [System.Collections.Generic.List[Object]]::new()
```

```
$Data = $Results -Split '[\r\n]+'
ForEach ($Item in $Data) {
    If ($Item -match 'Location: (\S+),.+Item count: (\d+)' -and $Matches[2] -gt 0) {
        $RecipientDetails = [PSCustomObject]@{
            "Recipient"      = $Matches[1]
            "Items found"   = $Matches[2]
        }
        $RecipientList.Add($RecipientDetails)
    } # End if
} #End ForEach Data

$RecipientList

Recipient                                Items found
-----
Tony.Redmond@office365itpros.com          489
Deirdre.Smith@office65itpros.com           160
Ben.Owens@office365itpros.com              11
Customer.Services@office365itpros.com       9
```

A content search with a broad search query is likely to return hundreds or even thousands of items. The easiest way to validate that the search finds items of interest is by reviewing the sample items retrieved by the search through the GUI. Apart from anything else, this allows you to examine the items carefully to ensure that the search is working as expected. The next step is then to export the items for closer examination or to refine the search keywords and conditions to focus on a more refined set.

Searching SharePoint and OneDrive for Business

The locations searched by the example query used above are user mailboxes and public folders, including the cloud-only mailboxes holding compliance records for non-tenant users. We can add OneDrive for Business and SharePoint sites to the set of search locations, but only if the target resources support the query. In this case, if we try to add non-Exchange locations to the search by running the *Set-ComplianceSearch* cmdlet, we will see a warning message because the search query is based on email-specific properties (Subject and Received date) that OneDrive for Business and SharePoint Online don't support.

Here is how to create a content search that specifically targets SharePoint and OneDrive for Business sites. In this case, we search for any item stored in any site (the *SharePointLocation* parameter is set to "All") that includes some credit card information (the search uses the sensitive information type to find these files – see the Data Loss Prevention chapter for more information). We can further refine the search query by only looking for items created on or after 1 January 2015:

```
New-ComplianceSearch -Name "SPO and OD4B search for credit card data"
-Description "A search of SharePoint and OneDrive to locate files containing credit card data"
-SharePointLocation "All" -ContentMatchQuery '(SensitiveType:"Credit Card Number:2..") AND
(created>=01/01/2015)'
```

Once again, after creating a new content search, we start it with the *Start-ComplianceSearch* cmdlet to retrieve some results.

The example query searches all sites. If we try to refine the set of sites that we want to search, we can do so by specifying the URL for each site as shown below. In this instance, we also add a couple of Exchange Online mailboxes to the search locations. This will cause an error because the search properties we are trying to use are not available for all locations.

```
Set-ComplianceSearch -Identity "SPO and OD4B search for credit card data" -SharePointLocation
"https://office365itpros.sharepoint.com/sites/0365ITPro/", 
"https://office365itpros.sharepoint.com/Projects/" -ExchangeLocation "Tony Redmond", "Paul
Cunningham"
```

PowerShell allows you to go ahead with the content search even though the problem with search properties is flagged. It is a mistake to do this as the net effect is usually to find everything in the search location that does

not support the properties used in the search query. In this example, because we use search properties specific to SharePoint and OneDrive for Business but have included some Exchange mailboxes, the search returns every item in those mailboxes, which is probably not what you intended.

See this [blog post](#) and this [support article](#) for tips about how to format KeyQL queries to interrogate SharePoint and OneDrive for Business sources.

Content Search Actions

Behind the scenes, many of the actions you take after a search runs use the `New-ComplianceSearchAction` cmdlet to add a new action to the search. For example, when you export data from a search, the cmdlet runs to add an export action to the search. The following parameters are the most used:

- *SearchName*: The name of the search to add an action.
- *NotifyEmail*: The email address(es) of users to receive a notification when an action is complete.
- *NotifyEmailCC*: The email address(es) of CC recipients for notification messages.
- *Scope*: Specifies what kind of items (indexed, unindexed, both indexed and unindexed) the search will process.
- *Preview*: Add an action to preview items found by the search.
- *Export*: Add an action to export items found by the search to a PST or folder.
- *EnableDeDupe*: Removes duplicate messages during exports of search items.
- *IncludeSharePointDocumentVersions*: Input `$True` to include all versions of discovered SharePoint documents or `$False` to include only the most recent version. Remember that SharePoint Online captures many versions of Office documents during edit sessions due to the autosave feature.
- *RetryOnError*: Retry the search if an error occurs. Do not specify this parameter when using a content search action to remove items from mailboxes as it will stop the action.
- *Purge*: Add a search action to remove items found by the content search. Exchange Online is the only workload to support purging items. Because the search depends on the content indexes, it cannot remove [unindexed items](#) (like encrypted messages that aren't protected by sensitivity labels) from mailboxes. Users who don't hold the compliance Organization Management role cannot use the purge action.
- *PurgeType*: Specify how the content search should remove items. Items can be soft-deleted by passing the *SoftDelete* value. Users can recover soft-deleted messages during the deleted items retention period (default 14 days). You can also specify *HardDelete* to force hard deletion, which makes the items irrecoverable by the user.

You cannot add a new action to a search if the search is in progress or the search results are stale. For export operations, a search is stale if it is more than seven days old. For destroy or purge operations, a search stays usable until it is more than ten days old.

Using a Content Search to Purge Mailbox Items

Administrators often need to purge items from mailboxes to eliminate problem messages. Common reasons include:

- Phishing messages before users have the chance to read them and activate the harmful links.
- Messages that hold malicious attachments (viruses or other code).
- Messages sent in error and hold information that the organization would like to withdraw (insofar as is possible). You cannot retrieve messages that users send outside the organization or when delivered by Outlook to a PST.

In these circumstances, the usual approach is to create a search targeting the mailboxes holding the problem messages. The easiest way to do this is to create the search in the Microsoft Purview Compliance portal and

refine it by tweaking search criteria until you are happy that the search finds the right messages. Because you are going to remove data from user mailboxes, the search must be as precise as possible. Think of keyhole surgery rather than a massive incision with the aim of finding just the right messages to remove rather than casting a wide net that finds hundreds of items. To focus the search, you should capture the essential characteristics of the targeted message in a content query to limit the search as tightly as possible. If you plan to remove items from mailboxes with a purge action, it's essential that the search query limits what it finds to just the targeted items. For instance, you could include these criteria:

- An exact word or phrase that occurs in the message subject. For example: "Great Opportunity to Purchase." You can use this phrase for the Subject property in the search query. Note that when Microsoft Search processes message subjects, it finds any message that includes the search term rather than an exact match.
- The sent date for the message, or a limited date range. Use this date as the Received property in the search query.
- The SMTP address of the sender.
- A keyword containing some unique value found in the message body.

Combining several properties will generate a more precise search. For instance, if you use a broad term such as "Office 365" to search the message subject, the search will find messages with subjects like "Welcome to Office 365" and "The best Office 365 book" or even "How to send spam to Office 365 recipients." Adding the email address of the sender and a limited range for the email sent date will hone the search and adding a keyword phrase that you know is in the body of the messages you want to find will make the search very precise.

After running the search, you can use the search preview facility in the Purview portal to examine the items found by the search to verify that the search criteria are correct and working as expected. This is a critical step to take before you apply a purge action to remove mailbox items. Make sure that all the items selected by the preview match the criteria you used and that no unexpected results are present. Another thing to consider is that because a purge action works against search results, it cannot remove any items that search has been unable to index for whatever reason.

A purge action works for a maximum of 50,000 mailboxes. If you need to purge items from more mailboxes, you must split processing across multiple searches. In addition, a purge action can only remove ten items at a time from a mailbox, which is a good reason to refine search criteria until the query finds no more than ten items per mailbox ([the Graph API for eDiscovery premium](#) supports purging for up to 100 items for both Teams and mailbox locations). You cannot create a purge action for a search covering data held in SharePoint Online or OneDrive for Business.

Litigation and in-place holds affect the removal of items. If holds are in place for mailboxes, it might not be possible for a hard delete purge action to remove items. The search can find the items, but any attempt to remove the items fails because they are on hold. Soft delete purges will work because the items remain in the mailbox. The golden rule is that if you want to hard-delete mailbox data, make sure to first remove any holds covering the mailboxes. However, in many cases, it's enough to remove problematic messages from user view, so it's acceptable if the purge action moves the items into the Recoverable Items Purges folder and keeps them there until the retention hold lapses.

Look before you leap: No one wants to remove items from user mailboxes in error. Before committing a search to remove items, it is best to check that the search completes successfully and finds the right items. Use the Preview function to verify that the items you expect to find are present and that no unanticipated items have turned up. You might need to refine the search query several times before the search does exactly what you want it to do and is ready to go ahead and remove the items.

Using the Purge Action

When you are happy the search finds the correct results, add the *Purge* action to the search. Note that you can only do this if you are a member of the *Compliance Organization Management* role group. For example, this command invokes the search called "Look for Phishing Items" and instructs it to soft delete any items matching the search criteria. Before the cmdlet starts the purge, you must confirm that the action should proceed.

```
New-ComplianceSearchAction -SearchName "Look for Phishing Items" -Purge -PurgeType SoftDelete
```

After a few minutes, check the status of the purge operation by running the *Get-ComplianceSearchAction* cmdlet. The purge reports its progression in percentage terms from zero to 100. The name of the action is formed by combining the search name and a *_Purge* suffix. Given that the name of the search referenced above is "Look for Phishing Items," the name of the action is "Look for Phishing Items_Purge." The following command retrieves the progress of the purge action.

```
Get-ComplianceSearchAction -Identity "Look for Phishing Items_Purge" | Format-Table SearchName, JobStartTime, JobProgress, Status -AutoSize
```

SearchName	JobStartTime	JobProgress	Status
Look for Phishing Items_Purge	18/08/2024 19:04:38	100	Completed

To see how many items were purged, look at the *Results* property of the purge action.

```
(Get-ComplianceSearchAction -Identity "Look for Phishing Items_Purge" -Details).Results
```

```
Purge Type: SoftDelete; Item count: 4; Total size 104080; Details: {Location: Jack.Smith@office365itpros.com; Item count: 2; Total size: 20443; Failed count: 0; , Location: Kim.Akers@office365itpros.com; Item count: 1; Total size: 54554; Failed count: 0; , Location: Sue.Best@office365itpros.com; Item count: 1; Total size: 29083; Failed count: 0; }
```

If you need to remove more than 10 items from a single mailbox, let the purge job complete, remove it and its parent search, and then resubmit the search followed by another purge action. Do this until all the items are removed:

```
Remove-ComplianceSearchAction -Identity "Look for Phishing Items_Purge" -Confirm:$False
Remove-ComplianceSearch -Identity "Look for Phishing Items"
New-ComplianceSearch -Name "Look for Phishing Items"
Start-ComplianceSearch -Identity "Look for Phishing Items"
New-ComplianceSearchAction -SearchName "Look for Phishing Items" -Purge -PurgeType SoftDelete
```

If you find that more than 10 problematic items exist in user mailboxes, it's a bad situation to be in. Microsoft didn't design the compliance search action mechanism to clear mailboxes out. It is more of a precision removal tool for specific items.

You can purge items with content search actions in two ways:

- The *HardDelete* action moves items into a non-user-accessible folder in Recoverable Items. Depending on the holds that exist on the mailbox, the items might end up in the Purges or DiscoveryHolds folders, neither of which are available to users. The items remain in the mailbox until the Managed Folder Assistant processes the mailbox and discovers that the items are awaiting removal (see below).
- The *SoftDelete* action moves items into the *Deletions* subfolder of Recoverable Items. Users can recover items from Deletions using the Recover Deleted Items feature in Outlook and OWA.

The Managed Folder Assistant processes items held in Recoverable Items and removes the items after all retention mechanisms expire. These include:

- The mailbox's deleted items retention period (the time allowed to users to recover deleted items; this can be from 14 to 30 days). If the Single Item Retention feature is set on the mailbox, the Managed Folder Assistant leaves the messages in the Recoverable Items folders until the deleted items retention period lapses.
- The item has a personal retention tag or retention label.
- Retention policies (Microsoft 365 or Exchange Online) are in force for the mailbox.

Purged items remain available for eDiscovery. It's important to remember this because contents search will continue to find items in mailboxes even after their removal to an inaccessible folder in Recoverable Items. In other words, even after you run a content search and purge its results, the messages remain until the removal of all holds on the items. However, mailbox owners can no longer access or recover these items.

Of course, software being software, it is wise to verify results when a risk exists that a malicious email might wreak havoc on mailboxes. After running a purge action to remove items, you can review the properties of the search action to check the mailboxes where the action processed items, or (if you have permission), sign into a mailbox that you know held a problem item to check that the items are gone.

You can download an example script to create and run a search to find mailbox items before using a search action to purge the discovered items [from GitHub](#).

Be Sure About Removal

The removal of items from a user mailbox through a search generates a *SearchResultsPurged* audit record in the audit log, including details of the query used for the search. Neither this audit record nor the *Get-ComplianceSearchAction* cmdlet reports the locations where it found items to purge, but (using the *Search-UnifiedAuditLog* cmdlet) you should also find a matching *HardDelete* or *SoftDelete* record in the audit log that contains details of the purged items. The lack of obvious feedback on what the search action did is a good reason why you need to make sure that the content search returns the items you want to purge. To validate the results of the content search, use the preview function and then, if necessary, export the items to a PST before going ahead with the purge. You might need to export the items anyway to keep evidence about the data removed from user mailboxes.

Limit any possible damage: Removing data from user mailboxes is an operation that is fraught with error. The potential of making a mistake and removing something that you should not delete is always there. To reduce the potential for harm, purging based on a content search will only remove a maximum of 10 items from a mailbox per run (if the search covers multiple mailboxes, more than ten items can be removed in a single run). The purge function is an "incident response" feature to remove small amounts of problematic data from user mailboxes. Limiting removal to ten items should not be a problem unless malware floods mailboxes through multiple attacks over a short period. Purges should use a precise, focused search to find data. The ideal situation is to find and remove a single item. In addition, by limiting deletion to 10 items per mailbox, search and destroy operations finish much faster (Microsoft reckons on being able to process 100,000 mailboxes in 30 minutes). Using soft deletes rather than permanent removals allows users to recover items if the search removes them in error. If you need to purge more than 10 items from a mailbox, you must run a purge action multiple times, removing the purge action and recreating it each time.

Exporting Search Data

When a content search is tuned to find the right data, the next step is usually to export the data to allow expert examination and review. For email, the export can be to PSTs or as individual messages while exports from SharePoint or OneDrive are as individual documents, including earlier versions if necessary.

You can use PowerShell to automate the export to Azure part of an export operation. After that, things become trickier to call the tool used to download results from Azure and pass the necessary access token to the tool (see [this discussion for a suggested solution](#)). The example below shows how to start the export process for search results. In this case, we want to export messages in PSTs (the format is "FxStream") with messages for each mailbox stored in a separate PST. A loop tracks the progress of the job. When complete, the data is ready in Azure to be downloaded.

```
$Search = "Investigation LD-17166"
New-ComplianceSearchAction -SearchName $Search -EnableDedupe $True -Export -Format FxStream
-ArchiveFormat PerUserPST -Scope BothIndexedAndUnIndexedItems
$ExportJob = $Search+"_Export"
Write-Host "Export started at" (Get-Date)
do
{
    Start-Sleep -s 3
    $ExportStatus = (Get-ComplianceSearchAction -Identity $ExportJob -Details)
    Write-Host "Current status:" $ExportStatus.Status "% progress:" $ExportStatus.JobProgress
}
While ($ExportStatus.Status -ne 'Completed')
Write-Host ""
Write-Host "Export ended at" (Get-ComplianceSearchAction -Identity $ExportJob).JobEndTime
```

To download the exported results, select the search in the Microsoft Purview Compliance portal, followed by **Download exported results**. The export key is visible. Copy the export key to the clipboard. Later, you will paste the key into the download tool to authorize it to copy data from Azure to the export target destinations (such as PSTs or individual files).

If you want to restart an export, run the *Remove-ComplianceSearchAction* cmdlet to remove the exported data from Azure. Remember to append "_Export" to the end of the content search name to create the name of the export action.

```
Remove-ComplianceSearchAction -Identity "Investigation_#2_Export"
```

Using PowerShell to Manage eDiscovery Cases

PowerShell cmdlets are available to create and manage eDiscovery cases. For instance, the *New-ComplianceCase* cmdlet creates a case.

```
New-ComplianceCase -Name "Stock Trading Case Reference 2017-001"
```

The *Get-ComplianceCase* cmdlet returns details of an eDiscovery case. However, because an eDiscovery case is a wrapper around content searches and holds, it does not return much information as no members or sources have yet been added.

```
Get-ComplianceCase -Identity "Stock Trading Case Reference 2017-001"

RunspaceId      : 883d2fb0-ef1b-484f-918d-bedf1930ef11
TenantId        : b662313f-14fc-43a2-9a7a-d2e27f4f3478
Identity        : 2fd9411c-3fd4-4293-a6f1-8fca699f51ed
Name            : Stock Trading Case Reference 2017-001
Description     :
CaseType        : eDiscovery
Status          : Active
ClosingStatus   : Unknown
CreatedDateTime : 11/01/2017 18:13:32
LastModifiedDateTime : 11/01/2017 18:13:32
ClosedDateTime  :
LastModifiedBy  : Tony Redmond
ClosedBy        :
ObjectState     : New
```

Different types of compliance cases are supported. You can fetch the different types by specifying the case type when running the `Get-ComplianceCase` cmdlet. For instance, this command retrieves eDiscovery (premium) cases:

```
Get-ComplianceCase -CaseType AdvancedeDiscovery
```

Other case types include:

- eDiscovery: eDiscovery standard.
- PrivacyManagementDSR: Microsoft Priva case.
- DSR: Data subject request case.
- InsiderRisk: Insider Risk case.

After finding the case to work with, we can update its details. For instance, we can add some members to the case with the `Update-ComplianceCaseMember` cmdlet, specifying the user principal name or display name for each member in a comma-separated string. For example:

```
Update-ComplianceCaseMember -Case "Stock Trading Case Reference 2017-001" -Member "Tony Redmond", "Kim.Akers@Office365ITPros.com"
```

The `Update-ComplianceCaseMember` cmdlet replaces the existing member list for a case. If the user who runs the cmdlet does not specify their name in the member list, the cmdlet includes it automatically. If you want to add a specific user to an existing member list, use the `Add-ComplianceCaseMember` cmdlet.

To make sure that no one can remove information needed by the case, we must set up a hold to retain information. A hold includes a rule and a policy. We create the rule with the `New-CaseHoldRule` cmdlet. The simplest form of rule has no query, in which case all content in the search sources is covered. For instance:

```
New-CaseHoldRule -Policy "Stock Trading Case Reference 2017-001" -Name "Stock Trading Case Reference 2017-001"
```

It's more usual to include a query, defined in KeyQL syntax. This example sets up a condition to look for any item where the words "stock" and "trading" occur near each other.

```
New-CaseHoldRule -Policy "Stock Trading Case Reference 2017-001" -Name "Stock Trading Case Reference 2017-001" -ContentMatchQuery "Stock NEAR(10) Trading"
```

We now use the `New-CaseHoldPolicy` cmdlet to add the hold policy for the case. The hold policy defines the locations that the case covers. Sources are:

- Exchange mailboxes.
- Public folders.
- SharePoint and OneDrive sites.

You can include either individual mailboxes or distribution lists. The membership of groups is expanded into individual mailboxes and added to the policy. You can also include public folders by passing the "All" value to the `PublicFolderLocation` parameter. SharePoint sites are specified with the site URL. For example:

```
New-CaseHoldPolicy -Case "Stock Trading Case Reference 2017-001" -Name "Stock Trading Case Reference 2017-001" -ExchangeLocation "Nancy Anderson", "Sanjay Patel" -SharePointLocation https://office365itpros-my.sharepoint.com/personal/ben_owens_office365itpros_com -PublicFolderLocation All -Enabled $True -Comment "Search sources added programmatically"
```

To check that the hold exists, we can run this command:

```
Get-CaseHoldPolicy "Stock Trading Case Reference 2017-001"
```

Or, to see all holds in place for all eDiscovery cases:

```
Get-ComplianceCase | % {Get-CaseHoldPolicy -Case $_.Name}
```

After you create an eDiscovery case, you probably want to create one or more content searches and link the searches to the case. We discussed the creation of content searches earlier. This example is like those reviewed then with the exception that we use the *Case* parameter to associate the search with the case.

```
New-ComplianceSearch -Name "Stock Trading Case Reference 2017-001 – Search 1" -Description "Search associated with Case Reference 2017-001" -ContentMatchQuery "Stock NEAR(10) Trading" -Case "Stock Trading Case Reference 2017-001" -ExchangeLocation "Nancy Anderson", "Sanjay Patel"
```

Once the search is available, you can start it in the normal manner by calling the *Start-ComplianceSearch* cmdlet.

The queries and search locations used in the content searches for eDiscovery cases do not have to match the hold rule or policy. This is because a case might span multiple searches, each of which looks for different information from different sources. The combination of all those results constitutes the information for case investigators to review.

Removing Cases

You can remove a case by running the *Remove-ComplianceCase* cmdlet, but only after removing any holds associated with the case. For example, let's assume that we want to remove the Contoso Alpha Case July 2015 case. To remove the holds, we issue the command:

```
Get-CaseHoldPolicy -Case "Contoso Alpha Case July 2015" | Remove-CaseHoldPolicy
```

The command to remove the holds is published to the workloads. It takes some time for the workloads to process the removals. When this process finishes, and no holds show up when you run the *Get-CaseHoldPolicy* cmdlet for the case, you can run the *Remove-ComplianceCase* cmdlet:

```
Remove-ComplianceCase -Identity "Contoso Alpha Case July 2015"
```

Adding eDiscovery Managers

Although it is usually best to manage the membership of sensitive role groups through the portal, you can add or remove users from the eDiscovery role groups through PowerShell. To do this, connect to the compliance endpoint and run the *Add-RoleGroupMember* (to add an eDiscovery Manager) or *Add-eDiscoveryCaseAdmin* cmdlet (to add an eDiscovery administrator). For example, these cmdlets add a user to the eDiscovery Managers role group and then check that the user is in the group:

```
Add-RoleGroupMember -Identity eDiscoveryManager -Member "James Abrahams"  
Get-RoleGroupMember eDiscoveryManager
```

Only an eDiscovery administrator can add another user to the eDiscovery Administrators role group. If you hold this status, you can run the cmdlets to add a user and check that the add worked as follows:

```
Add-eDiscoveryCaseAdmin -User "James Abrahams"  
Get-eDiscoveryCaseAdmin
```

Reporting Holds for eDiscovery Cases

The [Office 365 for IT Pros GitHub](#) repository contains a modified version of [a Microsoft script](#) to report the holds that exist for eDiscovery cases. You can use it as an example of how to navigate through eDiscovery cases to unpick and report on components.

The expected output is something like shown below, with cases organized by status and the holds described for active cases. The result of the analysis is held in the \$Report variable, so it is very possible to create different reports from the data without changing the script.

```
EDiscovery Cases found: 9
```

Active Cases:	7		
Closed Cases:	2		
Active Holds:	11		
<hr/>			
Case	Status	Created	HoldCreated
-----	-----	-----	-----
Board Minutes	Closed	28/04/2017 19:14	
Contoso Investigation	Closed	28/04/2017 19:14	
Improper management transactions (LD-2018-002)	Open	04/04/2018 18:03	04/04/2018 18:19:55

In-place Holds and Litigation Holds

An eDiscovery case can include one or more in-place holds to ensure that workloads retain information even if someone tries to remove or edit it. Each hold has a search query to find the information, which stays in the source location until something happens, like a user trying to remove or edit the content. At this point, Exchange Online captures a copy of the original content. Holds applied by Exchange and SharePoint or by retention policies and eDiscovery cases all keep content in place. It is an efficient mechanism that avoids the need to duplicate information unnecessarily.

Litigation or legal hold is a somewhat cruder but very effective mechanism available for Exchange Online mailboxes. A litigation hold places the entire mailbox on hold for a set period or indefinitely. Again, all items stay in place, but every deletion means that Exchange keeps a copy of the deleted item. As you can imagine, many of the items contained in mailboxes fall into the banal category and are of no interest whatsoever to discovery actions. However, there are instances where it is necessary to keep everything so that there is no chance of missing anything which might remotely be of interest. A litigation hold keeps everything in a mailbox, as will an in-place hold that has no search criteria. You can use litigation holds alongside in-place holds.

Placing a mailbox on litigation hold is easy. First, select the mailbox owner's account in the Microsoft 365 Admin Center, go to the **Mail** tab, and select **Manage litigation hold**. If a hold is already in effect on the mailbox, you'll see when it was set and by whom. To enable litigation hold for a mailbox, check *Turn on litigation hold* and enter values for the optional properties.

- **Hold duration:** How long the hold will last in days. Leave blank to set an indefinite hold.
- **Note visible to user:** Text entered here to explain the reason for the hold is visible to the mailbox owner in the Account Settings section of Outlook's "backstage."
- **Web page with more information:** A URL to a web page that should contain more information for the user to know why the organization puts mailboxes on hold and what it means to them. It might also include relevant citations of local laws governing user privacy and the steps taken by the organization to ensure that user privacy is respected. If present, Outlook displays a *More information* link in Account Settings. No check is made to ensure that the URL is reachable.

Click **Save changes** to make any changes to hold settings effective.

To make a litigation hold effective, Exchange Online updates several mailbox properties:

- **LitigationHoldEnabled:** Set to *\$True*.
- **LitigationHoldDate:** Set to the time and date when an administrator applies the hold to the mailbox. For example, 2-Feb-2022 19:45:50.
- **LitigationHoldOwner:** Set to the account that placed the mailbox on hold.
- **LitigationHoldDuration:** Set to the retention period. For example, 90.00:00:00, or 90 days. This is a notional period only because the litigation hold remains effective until *LitigationHoldEnabled* is set to *\$False*.
- **RetentionComment:** The free-text note to inform the user that their mailbox is on hold. You don't have to enter this comment if you do not want to.

- **RetentionUrl:** The URL pointing to a page holding additional information.

You can also set litigation hold on by setting mailbox properties in EAC or with PowerShell. Here is an example of putting a mailbox on litigation hold using PowerShell is:

```
Set-Mailbox -Identity "Ben Owens" -LitigationHoldEnabled $True -LitigationHoldDate (Get-Date -format 'dd-MMM-yyyy HH:mm') -LitigationHoldOwner "Administrator" -LitigationHoldDuration 90.00:00:00 -RetentionComment "Your mailbox is on hold" -RetentionUrl "http://www.contoso.com/compliance.html"
```

A hold can be indefinite. If you want to pass a duration in days, Microsoft's documentation states that the limit is 2555 days (7 years), but the cmdlet is happy to accept 100,000 days (>273 years). I doubt anyone now alive will be worrying if such a hold expires before its due date.

Chapter 18: Managing Data Loss Prevention

Tony Redmond

It would be nice if users handled confidential or sensitive information correctly all the time, but that is not how things happen in real life. It is human nature to err, and a common mistake is including confidential or sensitive information in emails or via a document shared with external people. Data Loss Prevention (DLP) is a technology designed to prevent users from sharing sensitive information inappropriately. Policies encapsulating rules to dictate the sharing of sensitive information are how organizations deploy DLP. First introduced in Office 365 for Exchange Online, DLP covers Exchange Online, SharePoint Online, Teams, and OneDrive for Business, with plans in place to extend coverage further to protect data drawn from across Microsoft 365.

This chapter describes:

- Data Loss Prevention concepts.
- How Microsoft Purview implements DLP.
- How to build suitable DLP policies to help applications prevent the loss of sensitive information.
- How to know whether your DLP policy is effective.

Data Loss Prevention is not a magic bullet and its capabilities do not extend to every method that someone can use to share data with another person. For instance, someone could post sensitive information like a credit card number in a Facebook conversation. You can handle that issue through third-party monitoring software, but user education might be equally effective. DLP is just another part to fit into the compliance puzzle that contributes to the overall security of information within companies.

Leak Prevention with Software

The need to prevent the loss (or leakage) of sensitive information such as credit card numbers, personal information like passport numbers, and so on is well understood, possibly because there have been many instances in which company or personal information has been compromised by being made public deliberately or accidentally. Graphic examples exist where large public companies have lost millions of records. The result can be brand erosion, legal expenses, customer loss, and an almost guaranteed public relations disaster. It is easy for a user to attach a document and send it to someone else; it is also easy to make a mistake that ends up with information leaking outside the organization. For example, you might not notice that Outlook has auto-completed an address with the wrong recipient and end up sending a confidential attachment outside the company. The speed of modern email systems makes any attempt to recall messages futile, so if someone realizes that they have made a mistake, all they can do is call the recipient and ask them to remove the content from their system.

Companies devote enormous effort to protecting IT systems. Much of the focus in the past has been on erecting traditional security barriers to stop attackers from penetrating internal systems. This approach might keep out hackers and scammers, but it does nothing to prevent employees from causing data loss, usually by accident. DLP is not new, and vendors have offered solutions for well over a decade. Microsoft enjoys certain advantages over third-party solutions because of its ability to deeply integrate DLP checks into clients and services:

- Integration of DLP functionality to detect policy matches in email into Outlook clients, including OWA, Outlook Classic, and the new Outlook. The integration analyzes message text using a mixture of algorithms including pattern matching and [regular expressions](#) as users type into a message body to detect possible sensitive information considered to be of concern to the company. Clients display policy tips to users when they detect sensitive information to help users become more aware of the kind of data that they are dealing with before including sensitive content in messages.
- Inclusion of DLP functionality into other Office applications such as Word, Excel, and PowerPoint. Enabling DLP checks throughout the Office suite means that users have less chance of making mistakes.
- The ability to implement checking at points where data is guaranteed to pass through. For Exchange Online, checking happens in the transport system as all messages must pass through it before leaving the system or are delivered to internal recipients. Sensitive information can therefore be intercepted in messages by integrating DLP checks into the transport flow. For documents stored in SharePoint Online and OneDrive for Business, a crawler to detect sensitive information checks files in document libraries as users add or share content. The crawler is already indexing all content stored in SharePoint and OneDrive for Business sites, so adding a check for sensitive content there creates the desired oversight. When DLP policies are deployed to protect Teams, the examination happens in the chat service.

The need to protect against the disclosure of confidential data does not exist in a vacuum. To be effective, it is important to incorporate DLP into an overall corporate compliance strategy alongside other tools to protect data both inside and outside the organization. For example, the strategy should consider how to use sensitivity labels to encrypt and protect the most confidential content so that even when this material circulates outside the organization, it continues to be protected and cannot be accessed except by authorized people. It's also important to consider how to protect data created before the introduction of the compliance strategy as old documents and messages can contain highly confidential information.

DLP-enabled clients can display policy tips when a DLP violation is detected to help users understand why a potential DLP violation exists and what they need to do to fix the problem. For instance, if a DLP policy exists to combat [oversharing of sensitive information via email](#), Outlook and OWA monitor the contents of new messages (including any attachments added to messages) to make sure that users don't share confidential content with external recipients. If DLP detects a violation, the client displays a policy tip to warn the user that they're not allowed to share confidential material externally and the user must take action (like removing the external recipient or choosing a different sensitivity label) before DLP allows them to send the message. Because users might see policy tips in clients, it's obvious that user education and policy communication is very important. People must know why the policy tips appear and what they should do next. It is also important to stress that DLP is not a guaranteed block against users sharing sensitive data. If someone wants to send information externally, they will be able to find another way to do so.

DLP policies to process Exchange Online, SharePoint Online, and OneDrive for Business items require an Office 365 E3 license (or, for Exchange Online only, an Exchange Online E2 license). In general, DLP policies that process emails will block messages in violation of policy no matter what license a user has, but users must have Office 365 E5 or Microsoft 365 E5 Compliance licenses before DLP will process Teams chats and channel messages.

Teams DLP Policy Licensing Checks: From May 30, 2023, Teams checks for the necessary licenses and will not process DLP policies for Teams messages. While the policies no longer operate, they remain available in the Microsoft Purview compliance portal in case the organization buys some licenses.

Microsoft Purview Data Loss Prevention

Microsoft Purview implements a common DLP service across multiple workloads based on checks evaluated against common conditions and data types (including retention and sensitivity labels) for target objects. DLP currently covers:

- Exchange Online.
- SharePoint Online and OneDrive for Business.
- Teams chats and channel conversations.
- Windows and Mac devices (endpoint DLP).
- Power BI.
- Microsoft Defender for Cloud Apps.
- On-premises repositories ([based on the Microsoft Information Protection scanner](#)).

Not all locations support the same DLP functionality, and some (like Teams and Windows devices) come with specific licensing requirements.

Microsoft Purview DLP policies are managed through the Microsoft Purview compliance portal. From August 2023, Exchange Online does not support DLP processing in Exchange transport rules (ETRs). The Exchange transport service ignores DLP conditions and actions in ETRs and treats the rules as if they are disabled. ETRs in this category are highlighted in the Rules section of the Exchange admin center. Organizations should remove any such ETRs and migrate their processing, if still required, to Microsoft Purview DLP policies.

Conversion from ETRs to Microsoft Purview DLP policies is not automatic. Effort is needed to plan the conversion, to create and test the new policies, and ensure that the combination of old and new policies function together during the conversion period. To ease the transition, Microsoft has developed [a playbook to help tenants move to Microsoft Purview DLP policies](#).

Sensitive Information Types

The basis for a DLP policy is understanding what kind of sensitive data you want to protect and how you want to protect the data. Several common data types come to mind when you consider what kind of information you prefer users to not mishandle. Credit card numbers or passport numbers are obvious examples of data usually regarded as sensitive. Although credit cards use a worldwide format, personally identifiable information (PII) and other sensitive information types differ from country to country.

It would not make much sense if Microsoft required tenants to analyze the essential characteristics of data types like credit card numbers and passport numbers to create custom definitions to match these types. Mistakes would happen, and inconsistencies in definitions would abound. Fortunately, Microsoft Purview includes [over three hundred sensitive information types](#) for use in DLP policies and other solutions. Some of the data types are like other types (for example, the definition for passport numbers or driving licenses often does not vary much between countries). Among the set of standard sensitive information types are:

- ABA routing numbers.
- Credit card numbers.
- U.S. Social Security numbers.
- Canada bank account numbers.
- European Union debit card numbers.
- Australian passport numbers.
- German driver's license numbers.
- European Union tax identification number.

- Various credentials used in Microsoft, Google, and Amazon cloud services like an OAuth 2.0 access token.

Over time, Microsoft has expanded the inventory of sensitive information types to increase coverage for data loss prevention and other capabilities. Many of the sensitive information types added recently are to detect country-level data like passports, identity cards, and bank numbers. In addition to new types, Microsoft also tweaks the patterns and definitions of existing sensitive information types to improve their accuracy.

You can see the current set of sensitive information types available in Microsoft Purview by running the `Get-DlpSensitiveInformationType` cmdlet (after connecting to the compliance endpoint):

<code>Get-DlpSensitiveInformationType Format-Table Name, Description</code>	
Name	Description
Canada Driver's License Number	Detects Canadian driver's license number.
EU Debit Card Number	Detects European Union debit card number.
Israel National ID	Detects Israeli national identification number.
Credit Card Number	Detects credit card numbers for American Express, Diner...
U.S. Social Security Number (SSN)	Detects formatted and unformatted US social security nu...
German Passport Number	Detects German passport numbers or Reisepass.

Sensitive information types break down into bundled and unbundled entities. An unbundled entity is a sensitive information type that stands on its own. It can be used in a DLP policy to detect specific information, or it can be used as part of a bundled entity. Each sensitive information type is defined by describing its characteristics in the form of some recognizable pattern, often captured in a regular (regex) expression. For instance, a social security number is a nine-digit number usually formed in three groups of three, two, and four digits separated by hyphens. Many passports have some alpha characters followed by seven digits, and so on.

A bundled entity is simply a collection of sensitive information types managed as a single type. For example, if you use the *All Medical Terms and Conditions* type to detect content in a DLP policy, DLP finds any medical term or condition found in SharePoint, Exchange, and Teams content to which the policy applies. Microsoft also has a bundled entity for credentials called *All Credential Types*.

The use of sensitive information types is not restricted to DLP. You can use sensitive information types in:

- DLP policies.
- Communication compliance policies.
- Insider risk policies.
- Auto-labeling policies (retention labels by background processes).
- Auto-apply retention labels (by applications).
- Auto-apply sensitivity labels (by applications).
- Find items with specific sensitive data types in content searches and eDiscovery cases.

Later we cover how to create custom sensitive information types. You can use custom sensitive information types in the same way as standard sensitive information types.

A simple number is never enough: A sixteen-digit number is not by itself enough evidence to prove that it belongs to a credit card. DLP applies several tests to ensure that data contained in message bodies or attachments are sensitive. In the case of credit cards, the first check compares the number with the Luhn algorithm to ensure that it matches the rules set down for credit card numbers. DLP looks for further evidence such as the presence of a card expiry date (like 11/26), a name, or a CVC/CVV (card verification value). If these elements exist near the credit card number, it lends weight to the argument that the data matches the policy, and enough confidence exists to invoke the policy actions. The same is true of nine-digit U.S. social security numbers that do not have a checksum. If DLP applied a test of just looking for nine-digit numbers, the likely result is that many false positives would be signaled. In this case, the extra

evidence is the presence of the word "SSN" in conjunction with nine-digit numbers. Different validation rules are employed to process the various sensitive information types so the thing to remember is that DLP must be reasonably confident that a violation exists before it will signal a policy tip to the user or block a message.

Bypassing DLP Checks

It's important to recognize that scanning based on sensitive information types will only detect instances where data matches the patterns defining the data type. If someone wants to get around DLP checking, they can by disguising text to avoid the pattern being detected. For instance, if you use a DLP policy to block email going outside the organization if messages contain credit card numbers, people can get around the block by spelling out the numbers (for example, use "six" instead of 6) or by including a picture of a credit card number. Messages with these variants of credit card numbers will be passed by the policy because the detection routines don't examine graphic data or look for blocks of text that might be a credit card number. In other words, DLP policies can catch most occurrences when people misuse sensitive data, but DLP checks will not detect disguised data.

Microsoft Purview DLP Policies

To understand how Microsoft Purview DLP policies work across multiple workloads, we'll go through the process of setting up a new policy and see what happens when the policy is operational. First, some broad concepts:

- A DLP policy is composed of rules, locations, and actions. The locations are where the DLP service checks for policy violations. DLP supports the use of administrative units to restrict policy processing to specific user accounts and groups.
- Each rule defines conditions that the DLP service applies against data to decide if any violations exist. DLP policies don't need many rules to be effective. For example, the [DLP policy to prevent users from sharing Teams meeting recordings outside the organization](#) uses one simple rule.
- The rules tell the DLP service what actions to take if it detects a violation. For instance, a rule violation could stop users from sharing a document.
- A rule can allow a user to override an action.
- For [some conditions](#), rules can display policy tips to users to help them understand why the organization considers it to be a problem if they share certain types of sensitive information. Some of the conditions are deemed to be premium functionality. Users require Office 365 E5 or equivalent licenses before Outlook displays a policy tip based on a premium condition.
- Rules can also generate incident reports to inform compliance administrators when violations occur.

Now that we understand the basics, let's discuss some differences which exist when the DLP service processes different forms of content.

Checking Documents for Sensitive Data

Despite the obvious differences that exist between processing email and documents, the same need exists to find a single point in the system to apply policies reliably. Using transport rules for Exchange DLP policies guarantees that the transport system will apply policies to all messages as they pass through the transport pipeline. Microsoft Purview DLP policies do not use Exchange transport rules. Instead, DLP policy checking occurs during the indexing of Exchange messages. This happens quickly enough to ensure that violations are detected and stopped before messages leave the organization.

A similar natural chokepoint does not exist for SharePoint Online, so Microsoft needed to take a different approach to offer protection for SharePoint and OneDrive for Business libraries. To detect DLP violations in

documents, SharePoint Online uses a mixture of real-time policy evaluation together with a special "crawler" process and a background timer job to find documents containing sensitive data. Microsoft refers to this as a mixture of synchronous and asynchronous checking that applies equally well to new documents as users upload files to document libraries and to existing documents as users update their content.

Crawlers create content indexes by scanning all the document libraries in sites to look for new or changed material to index. The DLP crawler looks for sensitive information types in new or changed documents and can detect them soon after an update occurs (as fast as indexing occurs). Background processes are subject to throttling and DLP checks might not happen if servers are under a heavy processing load. When system load reduces, the crawler detects any lingering violations as it processes items for content indexing. Excel posed a difficulty in terms of how it stored data in spreadsheets and Microsoft had to create a special file handler to ensure that DLP could detect sensitive information types in these files.

Synchronous or real-time evaluation does not mean the kind of in-place checking that occurs in Outlook when the body of messages is examined for matches against applicable DLP policies as the user updates the message body. Nor is it like the OWA implementation where message content is sent to the server for examination periodically. Real-time checking for SharePoint and OneDrive documents means that the content is examined when documents are added, changed, or shared.

When SharePoint detects a violation, it applies the rules specified in the DLP policy. If the policy rules block access to items containing restricted data outside the organization, SharePoint and OneDrive for Business incorporate the check into the file-sharing dialog so that users cannot commit DLP violations (Figure 18-1). The idea is that prevention at the outset is better than fixing a problem after a violation occurs. If the policy calls for the generation of an incident report, this is when the DLP service creates and sends it.

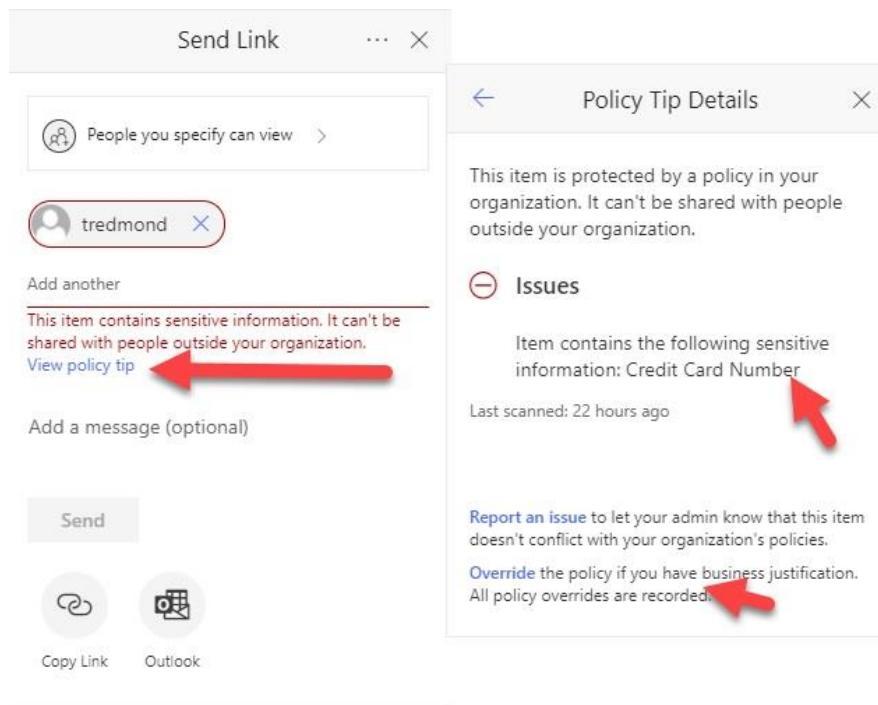


Figure 18-1: DLP blocks a user from sharing a file

Detection of a violation can also cause the display of a policy tip defined in the policy, but only in applications that support the necessary user interface, like SharePoint's browser interface. Policies might allow users to override the blocks imposed on documents holding sensitive information. If so, users can do this through the browser by opening the document properties, viewing the policy tip, and clicking **Override**.

SharePoint does not generate and send incident reports when the crawler detects a violation in content that existed before a rule became active. If SharePoint generated incident reports when it scanned content after an administrator adds a new rule or updates an existing rule, it is easy to imagine how the results might be a mail storm of thousands of incident reports. In a practical sense, it would be impossible to go through all the incident reports and resolve all the newly-detected violations. DLP still enforces any blocking actions contained in the rules; suppression occurs only for the incident reports.

Sensitive by Default

Because DLP policies are not processed immediately for new files created or uploaded to SharePoint Online and OneDrive for Business libraries, the risk exists that external users can access sensitive data before DLP scans the content of new files. Normally, DLP scanning happens within a few minutes, but if the organization considers the small time gap to be an issue, you can configure SharePoint Online to treat all new files as sensitive by default until they have been checked by a DLP policy. In effect, this means that SharePoint Online blocks external access to documents until DLP scans the contents to identify if any sensitive information is present. If guests attempt to access a document before it is scanned, they see a page to tell them that scanning is in progress. Any DLP policy that has a "contents contains" condition to process information in SharePoint Online sites can perform the check, even if the policy doesn't subsequently perform an action or flag content for follow-up.

To implement the Sensitive by default control, you:

- Implement at least one DLP policy to scan the SharePoint Online sites that store information intended for external access.
- Run the `Set-SPOTenant` cmdlet in the SharePoint Online PowerShell module to block access to new files. It can take up to 15 minutes before the change is effective. The block applies to all sites in the tenant, and you can't exclude sites from its effect.

`Set-SPOTenant -MarkNewFilesSensitiveByDefault BlockExternalSharing`

With the block in place, users can still share documents externally (if not blocked by the sharing settings for the tenant), but external people with a sharing link cannot access the content until the document is scanned by a DLP policy. Scanning either passes the document for external access (because DLP doesn't detect a policy violation) or blocks it (because DLP detects some content that violates the policy if shared externally).

To revert the block, run `Set-SPOTenant` to allow sharing without waiting for DLP processing:

`Set-SPOTenant -MarkNewFilesSensitiveByDefault AllowExternalSharing`

Applying the Sensitive by default control is an effective way to stop external sharing from SharePoint Online. However, it's a broad-brush policy that covers all sites in a tenant. Using sensitivity labels to restrict access to documents containing important information might be a better approach, especially when auto-label policies are used to find and apply labels to documents at rest.

Policy Tips

Overriding a policy tip through the **Override the policy** link allows a user to go ahead and share a document when a DLP policy would otherwise block this action. SharePoint records user overrides in the audit log in a "`DLPRuleUndo`" audit entry. The `ExceptionInfo` section of the audit entry captures the override text:

```
{  
  "Reason": "Override",  
  "Rules": [  
    "413957f5-c3ab-4765-9322-33d2983dabfe"  
  ],  
  "Justification": "This document is authorized for sharing!"  
}
```

Mobile Policy Tips: The OneDrive for Business mobile apps for Android and iOS support DLP policy tips. The clients download the DLP policy from Microsoft Purview when it connects, and the application is then able to scan text input into documents for sensitive information types and, if detected, display the correct prompt. The Teams mobile clients also support DLP policies in that they report violations in the activity feed, show when messages are blocked, and allow authors to override a block if allowed by policy.

Teams DLP Policy Processing

Teams clients don't scan for DLP violations as users enter text or when items are indexed. Instead, Teams checks messages against DLP policies after users send messages and clients submit those messages to the Chat service. Both personal chats and channel conversations (including private channels) are monitored. Teams DLP policies only work for users with an Exchange Online mailbox. Teams DLP policies can be scoped to cover all users or to include or exclude up to 1,000 selected accounts.

Note: Because all Teams messages pass through a message aggregator, DLP policies applied to the host team also apply to messages posted to conversations in Teams private and shared channels and the documents stored in the SharePoint sites belonging to the private channels. Because private channels don't have a unique identity within the tenant, you can't add a private or shared channel as an explicit inclusion or exclusion in a Teams DLP policy.

Teams messages remain inside the company, so the division between internal and external users is less obvious than in SharePoint or OneDrive, where it's obvious when a document is shared with an internal or external account. When you create a DLP policy for Teams, remember that guest users and federated external users (including those who join meetings) are considered external to the organization; tenant users are inside. Because of this separation, it might be easiest to create separate DLP policies for Teams for external and internal users. In this respect, Teams is different from Exchange and SharePoint. DLP policies applied to email and documents usually focus on external sharing rather than internal communications.

Checking Teams Messages

As messages flow through the chat service, Teams compares message content against the criteria defined in DLP policies covering Teams locations. The normal matching procedure is used to identify sensitive data specified in the policies by comparing values like credit card numbers together with accompanying information. If a violation is detected, Teams generates a block signal to a "Rethook" (a mechanism used by Teams to flag actions to clients) to instruct clients to block the message. After receiving the signal, the client used by the person who sent the blocked message tells them that the block is in place (Figure 18-2) and, if the policy allows, offers them the chance to override the block (through the *What can I do* link). Users who received a blocked message might see its content momentarily but once the block is in place, the message is hidden, and they can't see it any longer.



Figure 18-2: Teams blocks a message containing credit card numbers

Users receive a notification in their Activity Feed when Teams blocks one of their messages. In addition, if the user is logged into Teams with a mobile device, they'll receive a notification on the device that their message is blocked.

Teams DLP Policy Recommendation: Organizations that use Teams but don't have any Teams DLP policies see a Microsoft recommendation in the Microsoft Purview compliance portal that a policy should exist to protect Teams messaging. Accepting the recommendation creates a pre-packaged Teams DLP policy to protect against the sharing of financial data, passport and social security numbers, and credit card numbers. You don't have to accept the policy settings as defined and can edit them before making the policy effective. Remember that you might need extra licenses to use Teams DLP policies.

Default DLP Policy

It is always good to have a building block to start with when approaching the introduction of new technology. To help tenants start with DLP, Microsoft includes a default DLP policy to protect credit card information for tenants where DLP is not already in use. Credit cards are the most common data protected by active DLP policies, so they are a natural choice for companies to start their DLP journey. If your tenant has a default DLP policy, you must edit and enable it to make the policy active.

Creating Microsoft Purview DLP Policies

After becoming used to DLP policy structure and operation, the next step is to create a policy tailored for your organization. You can edit the default DLP policy or create a new one. To create a new DLP policy, go to the Data loss prevention section of the Microsoft Purview Compliance portal and click **Create policy**.

Before you go ahead and create a new policy, it is worthwhile to chart out what kind of sensitive data you want to protect and where is that data kept. Every DLP policy follows the same basic structure:

- **Locations:** What workloads to protect. You can choose from Exchange Online, SharePoint Online, OneDrive for Business, and Teams. Coverage extends to messages posted to Viva Engage communities if the tenant network operates in Microsoft 365 mode. DLP policies do not currently cover Planner but do cover the SharePoint content associated with this app. You can scope the policy to include or exclude specific mailboxes, sites, or teams. The account pickers for Exchange Online, Teams, and OneDrive for Business support distribution lists and security groups to make it easier to apply policies to large sets of people without having to select each account individually. DLP evaluates distribution lists periodically to detect membership changes.
- **Optional Locations:** DLP is spreading its ability to analyze content to detect violations in different places. For example, you can [use DLP to monitor non-Microsoft apps like DropBox via Microsoft Defender for Cloud Apps](#), [Windows devices via EndPoint DLP](#), [Power BI](#), or [scan on-premises resources](#). Microsoft deems these to be advanced capabilities, so you'll need appropriate licenses like Microsoft 365 E5 Compliance.
- **Rules:** What kind of protection do you want to achieve. Rules specify what kind of sensitive data you want to protect, conditions that say what must happen before a violation occurs, and actions that the policy takes afterward. Actions include user notifications and the creation of incident reports.

Basic DLP Policy Settings

You can then start to flesh out the policy by creating the different sections of the policy. The policy creation wizard is divided into these parts:

- **Choose the information to protect:** To make it easier for customers to create DLP policies, Microsoft Purview includes many DLP templates, each of which defines a set of sensitive information types that organizations commonly need to protect in certain fields of activity. For instance, if you want to avoid the loss of personal data, you can select **Privacy** to see templates such as "U.S. Personally Identifiable

Information (PII) Data" or "U.K. Privacy and Electronic Communications.". When you select a template as the basis for a policy, the wizard automatically creates the necessary DLP rules to protect the information defined by the sensitive information types defined in the template. If none of the standard sets work for you, select **Custom**, which allows you to construct your own rule set.

- **Name your policy:** If you select a template, the policy name inherits the template name. You can overwrite the name with your own choice. You can also enter a description for the policy. Some organizations used this to refer to internal documentation for the policy, including information about who created the policy.
- **Choose Locations:** The policy wizard displays a set of supported locations with a slider for each location. If you leave the slider on for a location, the policy applies everywhere in the location (for instance, every SharePoint Online site in the tenant). Alternatively, you can select to include or exclude specific:
 - Exchange mailboxes. Specify all mailboxes or select mailboxes to include or exclude. You can use distribution lists to include or exclude sets of mailboxes covered by a policy, but you can also add or exclude individual mailboxes by typing their names into the search field. Dynamic distribution lists can scope DLP policies for mailboxes based on properties of user accounts.
 - SharePoint sites. Specify all sites or enter the URL for the sites that you want to protect (up to a maximum of one hundred sites) or choose to include or exclude specific sites. If you need to include or exclude more than a hundred individually-specified sites in a policy, consider using an org-wide policy.
 - OneDrive for Business accounts. Specify All or select accounts using distribution lists or individual accounts for inclusion or exclusion. The limit of a hundred accounts also applies.
 - Teams. Choose all to cover all teams or select individual accounts by name or using a distribution list to include or exclude in a policy.

The above are the Microsoft 365 locations. Depending on the licenses you have, DLP policies might extend to locations like Power BI workspaces, on-premises repositories, and endpoint devices.

Because of our Microsoft 365 focus and the optional nature of software that covers the non-Microsoft 365 locations, this book does not cover those locations.

- **Policy settings:** Each policy contains at least one rule used to match items with potential violations. If you create a policy from a template, you can accept the default processing settings for the rules copied along with the template. For instance, a rule might be set up to block content when shared outside the organization. If the default rule settings don't do what you want, you can customize the rules or create new rules from scratch. A policy created from a template is likely to have at least two rules, each of which should be checked to ensure that the settings in one rule cannot interfere with settings in other rules. We will discuss rule settings in more detail later.
- **Enable policy:** Define whether the policy is on or off, or if it is in test mode.
- **Review your settings:** Before you save a policy, you can review its settings to ensure that everything is as you expect. Click **Create** to continue.

When you create a new DLP policy or update an existing policy, Microsoft Purview checks the policy to ensure that it is valid. For example, you might have input the URL for a subsite instead of a site. If this happens, the error is flagged, and you must fix the problem before you can save the policy. Once everything is satisfactory, Microsoft Purview publishes the new policy to the various workloads to enact the policy. A certain amount of complexity is involved to publish a policy to all the workloads as multiple servers are involved. Microsoft's SLA is for a new or updated policy to be effective within an hour of publication, but the experience of many is that this SLA is often breached and that you might have to wait up to a day before everything settles down and new DLP rules are active.

A further delay occurs before workloads begin to detect violations. SharePoint relies on the crawler within the content indexing process to detect sensitive data within documents. SharePoint does not index content

immediately after an item is updated and (depending on system load) the crawler might take between ten minutes to an hour before it processes an updated document. It can take up to an hour before a new DLP policy for Teams or an update to a DLP policy for Teams is effective. The exact time varies depending on the current load on the Teams infrastructure.

Resolving Multiple Potential Violations

Large organizations or those with complicated DLP requirements will likely use several DLP policies. This creates the possibility that an item will match several policies. In this situation, the following applies:

- DLP policies have a priority order for evaluation from 0 (most important) downwards. Policies are evaluated in this order.
- Rules within DLP policies also have a priority order.
- DLP rules can be set to stop the processing of other rules when a match is detected.
- In general, DLP applies the most stringent policy on the basis that it is better to be safe rather than sorry.
- The exception is where a rule in a high-priority policy stops the processing of other rules. In this case, the violation flagged by this rule is used and any other potential violation which might be detected by rules in lower-priority policies is ignored.

With this guidance in mind, organizations should:

- Order DLP policies so that the most important policy is assigned the highest priority.
- Order rules within DLP policies so that the most important rule is assessed first.

Default Rule Settings

If you don't customize the rules in a DLP policy, the rules inherit some default settings, including:

- **Who can receive sensitive content:** DLP can apply the policy inside or outside the organization. People with email addresses belonging to a domain registered for the tenant in the Microsoft 365 admin center are internal; those with addresses belonging to other domains are considered external.
- **How DLP protects content:**
 - **Display policy tips:** It is usual to display policy tips to users to tell them that a problem exists with a document.
 - **How many instances of sensitive data exist in an item before DLP flags a violation:** The default for a rule is that 10 instances of the same sensitive information type (for example, a credit card number) must be present in a file or message before a violation occurs. You can reduce or increase the number of matches to change how the rule works. If you want to make a rule easier to match, reduce the instance count (for example, from 10 to 7). Likewise, to make it harder to match, increase the count.
 - **Who receives the incident report and what is in the incident report:** Typically, incident reports go to a DLP administrator, who checks the incident to assess whether it is valid and if a violation is present, decides what action to take to resolve the violation.
 - **Restrict or encrypt access:** Should sharing the information in a detected item be blocked or encrypted? Encryption is only supported for Exchange Online messages. For SharePoint and OneDrive content, you can restrict access to content after detecting a DLP violation. As shown in Figure 18-3, the normal situation is to block external access to the content while allowing internal users continued access. The options are:
 - Block everyone from accessing the content.
 - Block people outside the organization. Anyone with a tenant account can access the content, including guest users.

- Block only people with access to content granted through an *Anyone* shareable link. This option only appears in policies applied to SharePoint Online and OneDrive for Business locations.

Actions

Use actions to protect content when the conditions are met.

Restrict access or encrypt the content in Microsoft 365 locations

Restrict access or encrypt the content in Microsoft 365 locations

Block users from receiving email or accessing shared SharePoint, OneDrive, and Teams files.
By default, users are blocked from sending Teams chats and channel messages that contain the type of content you're protecting. But you can choose who is blocked from receiving emails or accessing files shared from SharePoint, OneDrive, and Teams.

Block everyone. ⓘ

Block only people outside your organization. ⓘ

+ Add an action

Figure 18-3: Customizing access to content setting for a rule in a DLP policy

When you opt to block external users from seeing sensitive content that violates a DLP policy, the SharePoint and OneDrive for Business sharing dialog includes a warning to users if they try to share sensitive content outside the tenant. The warning appears in real-time and helps to educate users about the need to protect sensitive content.

Advanced Rule Settings

To have full control over the rule settings, select **Create or customize advanced DLP rules** when creating a new policy. You can then use the full rules editor to edit rules copied from the template (or created from scratch) to meet your exact needs. The settings for rules are:

- **Rule name:** Free-text name assigned to the rule.
- **Description:** A brief description of what the rule does.
- **Conditions:** The type of data present in the content and the context surrounding the data (for example, the number of instances of some sensitive data) to cause the rule to fire. For example, a rule might ignore content where a single credit card number is present but fire when it finds more than three instances of credit card numbers. Figure 18-4 shows where to change the number of detected sensitive data instances for a policy to check (in this case, at least one credit card number must be present in an item to fire the rule).
DLP conditions can include aspects of documents or messages that must be present for the rule to fire. These conditions might only apply to a single kind of data. For example, a rule might check for email messages sent from a specific IP address or email with attachments that cannot be scanned or can only partially be scanned, or a rule could look for attachments of a specific type or those that are password protected. Another example of a condition is when you use a document property to identify documents that come within the scope of a policy. Any managed property supported by SharePoint search can be used in this manner. Finally, if sensitivity labels exist in the tenant, a DLP rule can include a condition that a certain label must be present for the rule to fire.
- **Exceptions:** Define whether any conditions exist that will cause the rule not to fire. The exceptions include if the content has a specific form of sensitive data (or label) or file extension, and the sharing of content inside or outside the organization. Exchange Online policies can focus on a characteristic of email (IP address, attachment type, and recipient domain). Exceptions used to be a separate section. Now they are set as a NOT group within policy conditions.

- **Actions:** What happens when a violation occurs. The action is to restrict access to the content by removing permissions for everyone except the primary site administrator (or global administrator), site owner, and the person who last changed the item. Microsoft Purview automatically restores the original permissions when the owner or person who last changed the document acts to remove the offending content and bring the document back into compliance. Encryption is available to protect email with sensitive content, but only for policies scoped to apply to Exchange content. See the note below.
- **User notifications:** DLP supports two forms of notifications. First, it can send email notifications to the site owner (or other designated users) and whomever last changed the item to inform them that a problem exists and why (for instance, someone shares the item with external people and includes a debit card number). A link in the message allows the recipient to open the document and fix the problem detected by the policy. The second method is to flag the problem visually with a policy tip. You can customize the text of the policy tip to add organization-specific advice to users.
- **User overrides:** The rule can allow users to override the block because of a false positive. In other words, the user (who knows the content and can put it into a business context) says that the rule is incorrect to flag an item for a policy violation. When this happens, DLP removes the block and records the text given by the user to justify the override for auditing purposes.
- **Incident reports:** You can arrange for email notifications to go to one or more people when a policy detects problems. These notifications are known as incident reports. Each report has enough information about the problem to allow an administrator or compliance officer to understand whether a problem exists and if so, whether they need to take further action.

You can also set rule priority to have DLP execute the rules in a certain order and terminate processing after a rule matches conditions and is executed.

Edit rule

Conditions

We'll apply this policy to content that matches these conditions.

Content contains

Default	Any of these
---------	--------------

Sensitive info types

Credit Card Number	High confidence	Instance count 1 to 9
U.S. Bank Account Number	Medium confidence	Instance count 1 to 9
ABA Routing Number	Medium confidence	Instance count 1 to 9

Add ▾

Create group

AND

Content is shared from Microsoft 365

Detects when content is sent in email message, Teams chat or channel message, or shared in a SharePoint or OneDrive document.

with people outside my organization

Save **Cancel**

Figure 18-4: Defining settings for an individual rule in a DLP policy

When you finish working with the settings for a rule, click **Save** to return to the rule set so that you can edit the next rule. When all the rules are to your liking, click **Next** to return to the policy. Remember that if you make a mistake or want to change something, you can always edit the policy and then update settings for individual rules or the policy.

Email message type conditions and exceptions: DLP supports exceptions based on the message type. These are used in cases where you might not want to apply rules to read receipts or automatic replies. Care should be taken with the three types which cover encrypted email. Encrypted means S/MIME encrypted; Signed means S/MIME signed; and Permission Controlled means that a sensitivity label or OME template protects the message. The latter is the type usually required to process Exchange Online messages.

Confidence Levels and Match Accuracy

DLP policies match data found in documents and emails against sensitive information types by looking for patterns and other forms of evidence. The primary element (like a regular expression) in a pattern for a sensitive information type defines the basic match for that type. Secondary elements (like keyword lists) add evidence to confirm that a match truly is an example of a sensitive information type. The more evidence is gathered, the higher the match accuracy and the more confidence exists that the data found is an instance of the sensitive information type. Microsoft refers to the match accuracy as the confidence level. Policy rules use the confidence level to decide whether action is necessary when matches are found.

The higher the percentage confidence level specified by a rule, the more evidence DLP must find before it can match a rule. Three confidence levels are used:

- Low (65% match accuracy).
- Medium (75% match accuracy).
- High (85% match accuracy).

For instance, to meet the bar set for a low confidence match for a credit card number, text must be in the right format (sixteen digits) and pass [Luhn's algorithm](#) to establish that the number could be a credit card. To increase the confidence that the number is a credit card to 85% confidence, the rule looks for other evidence like a keyword (such as "Visa" or "Amex") or an expiry date in the MM/YY format.

If a policy includes multiple rules that check for the same sensitive information type, the suggestion is to:

- Set the minimum and maximum confidence level for the rule that takes the least aggressive action when a low-confidence match is found.
- Set the confidence level range for the rule that takes more aggressive action when a match is detected with higher confidence.

The idea is that content with lower confidence matches receives an action with less impact on the user (like displaying a policy tip) while content with higher confidence matches gets a more restrictive action (like being blocked).

Rule Priority

Each rule in a policy receives a priority number in the order in which it is created. When DLP evaluates content against a policy, it processes the rules in priority order; if the content matches multiple rules, DLP applies the most restrictive action. For example, if rule 1 displays a policy tip to users and rule 6 restricts access to the content, DLP applies the settings from rule 6. In addition, the policy tip for the most restrictive rule is displayed to the user.

Protecting Sensitive Email with Encryption

If DLP detects outbound emails containing sensitive content, you can have Exchange apply encryption to the messages before they leave your tenant. You can choose to apply any of the Microsoft Information Protection templates (not sensitivity labels, because a label might not include encryption) available in the tenant to messages, including the default Encrypt Only and Do Not Forward templates. See the Information protection chapter for more information about how to create and use sensitivity labels to protect documents and email.

If you choose to apply encryption to messages in a DLP policy, that policy can only cover Exchange. You can't apply encryption to documents through a DLP policy.

Outlook (Classic) Pause to Evaluate Outgoing Messages

By default, the Outlook (classic) and OWA clients transmit message content to Microsoft Content Services to check whether it violates DLP policies. During an edit session, the clients send content and receive back notifications if a problem is present. Receiving a notification about a policy violation prompts clients to display policy tips to warn the user, if these are configured in policy rules.

It is possible for a user to input text containing sensitive information and send the message before Outlook has had a chance to transmit the content to Microsoft Content Services. If this happens, Outlook submits the message to the Exchange Online transport service, which applies DLP policies to email as messages pass through the transport pipeline. If the text contains a policy violation, it will be detected in the transport pipeline. Depending on the rule configuration, Exchange will either reject the message or send it to the destination server. Exchange can also inform the sender that their message contained some problematic content.

Obviously, it is better if users learn about potential issues before the transport service rejects their messages. To solve the problem, administrators can enable the *specify wait time to evaluate sensitivity content* cloud policy setting for Microsoft apps to implement a delay before transmission. Along with enabling the setting, the administrator sets a delay to allow the evaluation to complete. Usually, the delay is between ten and twenty seconds.

With the setting in place, Outlook (classic) pauses before sending the message to allow Microsoft Content Services to complete its evaluation of the content. The user sees a pop-up message to inform them that the organization requires every email to have a sensitive content evaluation before transmission. If the evaluation passes, Outlook sends the message as normal, and if a problem is detected, it displays a pop-up dialog policy tip configured for the rule where the violation occurred and implements the action defined in the rule. Normally, the action is to block the message because it contains sensitive content that shouldn't leave the organization. Depending on the rule configuration, the user might be able to override the block and send the message. The setting only applies to Outlook (classic). You can't change the way that Outlook mobile or OWA work.

Although effective, Outlook doesn't know if an outbound message contains sensitive information and therefore pauses for evaluation for each message. The subsequent delay to each message can infuriate users if they don't understand why it happens, so some user education is necessary before implementing the feature.

For more information, see this [Microsoft Technical community post](#).

GDPR Support

Tenants that come within the scope of the European Union's General Data Protection Regulation (GDPR) need to meet specific requirements for the protection and use of personal data. To help, Microsoft Purview includes six common sensitive information types for use in DLP policies or to classify sensitive data. The information types include:

- EU Debit Card Number.
- EU Driver's License Number.
- EU National Identification Number.
- EU Passport Number.
- EU Social Security Number (SSN) or equivalent ID.

- EU Tax Identification Number (TIN).

In addition, Purview includes many country-specific sensitive information types like the Estonia Driver's License Number.

Microsoft Purview includes a General Data Protection Regulation DLP template. If you create a DLP policy using this template, DLP adds the six EU-wide sensitive information types listed above to the policy. You can edit the policy to include other sensitive information types or include the EU data types in other policies.

An example of the difficulties involved in detecting content using sensitive information types happened when emails imported into SharePoint Online caused DLP to flag violations for the EU TIN sensitive information type because eight- and nine-digit numbers in the email headers resembled tax identification numbers. Microsoft resolved the problem by adjusting the data definition to look for more proof that a number was a TIN before flagging a violation.

Sample Test Data

When you start working with DLP, the issue of how to generate good test data to use to check policies always arises. The [DLPtest site](#) offers several different sets of sample data, including social security numbers and credit card numbers, that you can use for testing.

DLP Audit Records

When a DLP policy blocks an item, it records that fact in an audit entry in the audit log. You can see these entries in the audit log (search for the *DLPRuleMatch* operation). Alternatively, you can view DLP events in the report viewer. Click the *DLP policy matches* widget in the dashboard to be brought to the report viewer and then click *View details* table to see information about the DLP matches for all services covered by DLP policies.

DLP events are also accessible via the [Office 365 Management Activity API](#), a REST-based API covering audit information gathered from Exchange Online, SharePoint Online, OneDrive for Business, and Entra ID that's intended for ISVs to develop analysis and reporting products. Two types of DLP events are logged. One is a non-sensitive event and contains data such as the document or email that triggered a violation, the user, the policy rule, actions taken, and the type of sensitive data involved. The other is a sensitive event and returns all the data for non-sensitive events plus the value of the data, such as a credit card number.

Alerts

If configured in policies, matches against possible rule violations can generate alerts for administrators. DLP alerts are available in the Microsoft Defender XDR dashboard, under Alerts in the DLP section of the Purview compliance portal (Figure 18-5), and in the Activity Explorer. An alert doesn't necessarily indicate a problem. There might be an issue with the policy conditions that generated an alert in innocent circumstances. For that reason, it's a good idea to monitor alerts to check what policies are generating alerts and why. If your tenant has Security Copilot licenses, it can be used to summarize a set of alerts to detect if any trends are present.

Another policy setting dictates if administrators receive email copies of alerts. DLP can generate messages each time an activity matches a rule or when alerts reach a certain threshold, such as more than 20 matches during the last hour. The matches can be for all users in the tenant, or the threshold can apply to a single user. In other words, an email is sent when the activity for everyone in the tenant generates 20 matches in an hour or if an individual user (who must be very prolific) generates the same number by themselves. Obviously, appropriate reporting thresholds vary enormously based on the size of the tenant, the maturity and awareness of users about DLP, and the effectiveness of DLP policies.

Alert name	Severity	Status	Time detected	User risk level
DLP policy match for email with subject 'More imp...'	High	Active	Jun 18, 2024 10:56 AM	
DLP policy match for document 'Credit Card Test.d...'	High	Active	Jun 17, 2024 3:00 PM	
DLP policy match for document 'Credit Card Test.d...'	High	Active	Jun 17, 2024 2:22 PM	

Figure 18-5: DLP alerts

PowerShell support for DLP policies

DLP policies use several cmdlets (included in the compliance module) to work with policies and rules. The cmdlets include:

New/Get/Set/Remove-DlpCompliancePolicy: Create, access, manipulate, and delete DLP policies. For example:

```
Get-DlpCompliancePolicy -Identity 'Confidential Patent Information DLP Policy'
```

New/Get/Set/Remove-DlpComplianceRule: Create, access, manipulate, and remove the rules used in DLP policies. For example, here is how to check the settings for a rule (edited output shown):

```
Get-DlpComplianceRule -Policy 'Check for SSN Data' | Format-List

ParentPolicyName      : Credit Card data check
ContentContainsSensitiveInformation: {System.Collections.Hashtable, System.Collections.Hashtable, System.Collections.Hashtable}
AccessScope           : NotInOrganization
ContentPropertyContainsWords : {}
Workload              : Exchange, SharePoint, OneDriveForBusiness
BlockAccess            : True
GenerateIncidentReport : {DLPIncidents@Office365ITPros.com}
IncidentReportContent : All
NotifyUser             : {SiteAdmin, LastModifier, Owner, Tony.Redmond@office365itpros.com}
NotifyAllowOverride    : WithJustification
NotifyEmailCustomText  : You can't keep this kind of information in documents!
NotifyPolicyTipCustomText : Whoops - bad SSN data found here
ReadOnly               : False
Priority               : 0
Comment                : A rule to detect SSN data in documents
Disabled               : False
CreatedBy              : Tony Redmond
```

We can tell that this rule:

- Is associated with the DLP policy "Credit Card data check".
- Looks for three types of sensitive data (the hashtable references in the *ContentContainsSensitiveInformation* property – the names are not shown).
- Checks information shared with users outside the tenant (scope is "NotInOrganization").

- Scans for three supported workloads (Exchange, SharePoint Online, OneDrive for Business).
- Blocks access to content deemed to contain sensitive data.
- Generates a DLP incident report.
- Generates an email notification to the site administrator, the last user who modified the content, its owner, and a nominated other user.
- Allows the policy tip to be overridden with a business justification.
- Is active (*Disabled* is False).

Given that DLP policies can be reasonably complex to set up, it is best to manage DLP policies and rules through the Microsoft Purview Compliance portal and only use PowerShell to check individual objects as needed.

The Test-Message Cmdlet

The *Test-Message* cmdlet (from the Exchange Online management module) allows administrators to test the processing performed for an email by:

- Exchange Transport Rules.
- DLP Policies.
- Purview auto-label policies.

You can run *Test-Message* without creating a test email, but it's a good idea to create some messages with a variety of message subject, body, and attachments to test with. Ideally, the messages should reflect the kind of email that you expect rules to run against. The easiest way to create a test message is to create it with Outlook, populate its properties, and then save the message to a file. To pass the message to *Test-Message*, it must first be encoded and stored in a variable, which is then specified in the *MessageFileData* parameter. We can then call *Test-Message* to process the file. This example tests a message sent to a recipient from a single sender and directs the output to another address.

```
$EncodedText = ([System.IO.File]::ReadAllBytes('c:\temp\TestMessage.msg'))  
  
Test-Message -MessageFileData $EncodedText -Sender Terry.Jones@office365itpros.com -Recipients  
TestUser@outlook.com -SendReportTo Jim.Flynn@office365itpros.com -TransportRules -UnifiedDlpRules  
  
Server -----  
PAXPR04MB8095.EURPRD04.PROD.OUTLOOK.COM 626b8a86-c262-4457-911b-  
641a027989d7@DB9PR04MB8445.eurprd04.prod.outlook.com
```

The server information reported by the cmdlet is the Exchange Online mailbox server where the transport rules run. Given the massive pool of Exchange Online servers, it's likely that *Test-Message* will use a different server each time it runs.

Exchange Online creates the output for the test in messages delivered to the address specified in the *SendReportTo* parameter. In my case, the test generated three messages (DLP, auto-label, and ETR). Each message tells you the processing performed by the rules engine to allow you to see what each rule did and the effect it had on the message.

DLP and Insider Risk Management

Insider Risk Management is a Purview solution designed to detect the signs that internal users might engage in risky behavior that can lead to data compromise, mostly actions that could be data exfiltration such as sharing files with people outside the organization or downloading an unusual number of SharePoint files. When a scan identifies a user of concern, the account is assigned a risk level (elevated, moderate, or minor). Adaptive protection, an Insider Risk Management feature, includes a quick setup option to automatically create a DLP policy to protect against the actions being taken by accounts that are assigned a certain risk

level. Two automatic policies are created. The policy called *Adaptive Protection policy for Teams and Exchange DLP* covers Teams and Exchange Online. The other policy is called *Adaptive Protection policy for Endpoint DLP* and covers devices. Each policy includes two rules – one for elevated risk, the other for moderate and minor risk, with more restrictive limits placed on users deemed to be at the elevated risk level. For more information, including the settings used by the automatic DLP policies, see the [Insider Risk Management documentation](#).

Alternatively, organizations can manually configure DLP policies and use the *Insider risk level for adaptive protection is* condition and a risk level to block user actions, just like any other DLP policy. The accounts covered by Insider Risk Management require Microsoft 365 E5 licenses.

Endpoint DLP

[Microsoft Purview Endpoint DLP](#) is a solution that uses signals generated by actions performed on Windows 10/11 and Mac workstations to evaluate against DLP policies. Supported actions include copying files to removable media like a USB or to a network share, printing files, uploading to a cloud app, or copying data to the clipboard. The code necessary to detect actions and submit them for evaluation is in Windows 10 and 11 and the Edge or Chrome browsers. No additional agent is necessary to monitor activity on a workstation.

Create rule

File activities for all apps

Decide whether to apply restrictions for file related activity. Unless you choose different restrictions for restricted apps or app groups below, any restrictions you choose here will be enforced for all apps.

Don't restrict file activity

Apply restrictions to specific activity

When the activities below are detected on devices for supported files containing sensitive info that matches this policy's conditions, you can choose to audit the activity, block it entirely, or block it but allow users to override the restriction

Copy to clipboard ⓘ Block

+ Choose different copy to clipboard restrictions

Copy to a removable USB device ⓘ Audit only

+ Choose different removable USB device restrictions

Copy to a network share ⓘ Audit only

+ Choose different network share restrictions

Print ⓘ Audit only

+ Choose different print restrictions

Copy or move using unallowed Bluetooth app ⓘ Audit only

+ Choose different bluetooth restrictions

Copy or move using RDP ⓘ Audit only

+ Choose different remote desktop restrictions

Save **Cancel**

Figure 18-6: Endpoint settings in a DLP policy

Before you can use Endpoint DLP, you need Microsoft 365 E5 licenses or either the Microsoft 365 E5 information protection and governance or compliance add-ons. Workstations used by licensed accounts can

be onboarded (enabled) through the Microsoft Purview compliance portal to start the flow of signals for DLP evaluation, unless administrators have already enrolled the devices for Windows Defender, in which case Endpoint DLP works without any further configuration.

Once a workstation is enabled, actions taken by the user are monitored for potential violations against policy using the same kind of conditions as used to monitor Office 365 activity. For example, attempts to upload documents containing credit card numbers can be detected and stopped. Supported file formats include Office documents, PDF, text, and source code.

Endpoint DLP settings for the organization can be adjusted in the Microsoft Purview compliance portal to reduce the amount of noise in signals by excluding certain folders like the recycle bin, temp folder, or folders used for non-work files. It's also possible to allow uploads to specific cloud services without generating a violation. Policy thresholds can be set to generate alerts when multiple events of the same type happen over a short period. For instance, a policy could alert administrators if someone prints more than twenty documents with the Confidential sensitivity label.

When Endpoint DLP is available in a tenant, DLP policies can cover a target location called Devices, just like choosing SharePoint or Exchange as policy locations. The normal approach is to separate device policies from those used with Office 365 workloads, but you can combine them. Device policies have separate settings for restrictions to enforce when DLP matches policy conditions (Figure 18-6).

Edge is the preferred browser because it understands how to respect endpoint DLP policies, and you can block other browsers from accessing files protected by policies. For instance, you could block Firefox from opening a Word document if a specific retention label is present.

Apart from being used by DLP, the signals generated by devices can be gathered and analyzed in a SIEM. An example using Azure Sentinel is [described in this article](#).

Creating Custom Sensitive Information Types

Although a large set of standard sensitive information types exists, organizations often have specific ideas about the characteristics of confidential data which are not satisfied by the set of standard sensitive information types. You can create your own custom sensitive information types through the **Classifiers** section under **Data Classification** in the Microsoft Purview Compliance portal. Custom sensitive information types can be used in DLP policies, retention policies, and auto-label policies. They can be created from scratch or by copying one of the standard types and altering the copy to meet requirements.

The basic need for any sensitive information type is a pattern to detect matches in messages and documents. The simplest patterns have a primary element to instruct how to detect a specific type of sensitive information and a confidence level when a match occurs. A pattern with just a primary element might define its confidence level as medium for any match, while patterns with supporting elements that add more evidence that a match exists might increase the confidence level as supporting elements are found near the matched element. The following methods can be used as a primary element:

- **Regular expression:** A Regex to detect certain patterns of data. Sites like [regex101.com](#) are useful to help form regular expressions. For example, a regular expression of `\s[A-Z]{3}-[0-9]{4}\s` can be used to match project numbers like "PRJ-1384" or "PRO-1847".
- **Keyword list or Keyword dictionary:** Both ways to define keywords (like "Finance" or "Funding") that you want to use for matching. Typically, these methods are used as supporting elements rather than for primary matching.
- **Function:** Microsoft publishes a [set of functions](#) for different types of data, such as an Alabama driver's license. You can use these functions to create custom sensitive information types.

Supporting elements add confidence that matched data is what you are looking for and not just a random collection of letters and numbers. For example, as noted above, a social security number is described by a number in the format 999-99-9999 with added evidence coming from the keywords "SSN" or "Social Security" near (in terms of characters) the number. The same is true for credit cards, where the 16-digit number is confirmed by words such as "credit card," "Visa," MasterCard," "expiry date," and so on.

The Password Sensitive Information Type

In general, it's bad practice to circulate passwords in messages, so let's see how we can stop people from sending passwords in email and Teams messages (Microsoft includes an Azure user credentials sensitive information type in its set, but this discussion still serves for teaching purposes). Some cases exist when sending passwords around is necessary, such as when an administrator resets a password for a user (a tenant can enable [self-service password reset](#) to let users reset their passwords). To detect passwords, we need a regular expression to detect passwords matching Entra ID password policies. By default, Entra ID password requirements are:

- A minimum of 8 characters and a maximum of 256 characters.
- Requires three out of four of the following:
 - Lowercase characters.
 - Uppercase characters.
 - Numbers (0-9).
 - Symbols (@ # \$ % ^ & * - _ ! + = [] { } | \ : ' , . ? / ` ~ " () ; and blank space)

Many suggested regular expressions to validate passwords are shared on the internet. When you input a regular expression to use with DLP policies, Microsoft validates the code to ensure that it works and will perform well (the [rules are documented here](#)). Most of the suggested expressions do not meet Microsoft's rules. Fortunately, MVP James Cussen [created an expression](#) that passes the test and matches passwords, which we can use to illustrate how to create a custom sensitive information type. Here's the expression:

```
((?=[$]*?[A-Z])(?=[$]*?[a-z])(?=[$]*?\d)|(?=[$]*?[A-Z])(?=[$]*?[a-z])(?=[$]*?[^a-zA-Z0-9])|(?=[$]*?[A-Z])(?=[$]*?\d)(?=[$]*?[^a-zA-Z0-9])|(?=[$]*?[a-z])(?=[$]*?\d)(?=[$]*?[^a-zA-Z0-9]))[^s]{8,256}
```

The regular expression matches strings in the right format for passwords. To provide additional evidence that a string is a password, we can add a supporting element in the form of a keyword list. Typically, when people send passwords in messages, they include some explanatory text. Therefore, if a keyword occurs close to the matched password, the likelihood increases that the term is a password. For instance, someone might send a message saying "Here's your new password: AzurePW123!@." The string AzurePW123!@ matches the regular expression and becomes the anchor for DLP to look for keywords within the window set for keyword proximity checks. The window extends to the left and the right of the match, which means that a match against "password" occurs because the keyword is within a few characters of the anchor. The confidence that a good match exists is therefore higher.

In Figure 18-7, a keyword list of terms that help to confirm passwords is visible. If an organization is multi-lingual, you should include terms from different languages as shown here. It is also a good idea to consider including some misspellings of terms in the keyword list, such as "passwrd" or "passwrod" as there's no guarantee that people will spell everything correctly when they send messages.

Edit keyword list

Keyword lists identify the words and phrases you want this info type to detect. For example, the keyword list to identify Netherlands VAT numbers is 'VAT number, vat no, vat number, VAT#'. [Learn how to create keyword lists](#)

Choose from existing keyword lists

ID *

Keyword group #1 * ⓘ

Case insensitive

password, pwd, passcode, passwd, wachtwoord,
mot de passe, Passwort, contraseña

Case sensitive

Enter keywords, separated by commas. Each keyword is limited to 50 characters, and exact casing is required to detect matches.

Word match String match

Figure 18-7: Defining a keyword list

The components used to define the pattern for the new custom sensitive information type are:

- The primary element is a regular expression to detect the pattern of a valid Entra ID password.
- The supporting element is a keyword list of password terms.
- The confidence level is medium to start. This level is set when a match occurs against the primary element. It will increase to high confidence if DLP also detects a keyword from the keyword list in the supporting element.
- The character proximity defines how close one of the password terms must be to the primary element. Purview usually suggests a proximity window of 300 characters, but in this instance, it is better to adjust the proximity window to around 80 characters because the likelihood is that any mention of a supporting term will be very close to the password. If policies using the custom sensitive information type generate too many false positives, you can consider reducing the proximity to 50 or 60 to see if that reduces false positives. The option to check for anywhere in the document is not suitable because it is likely to result in many false positives.

Figure 18-8 shows the components of the new pattern during the creation phase. The primary element is saved with a name for easy reference later as is the keyword list. After defining the pattern, we set the recommended confidence level to look for in policies. The final step is to save the new type.

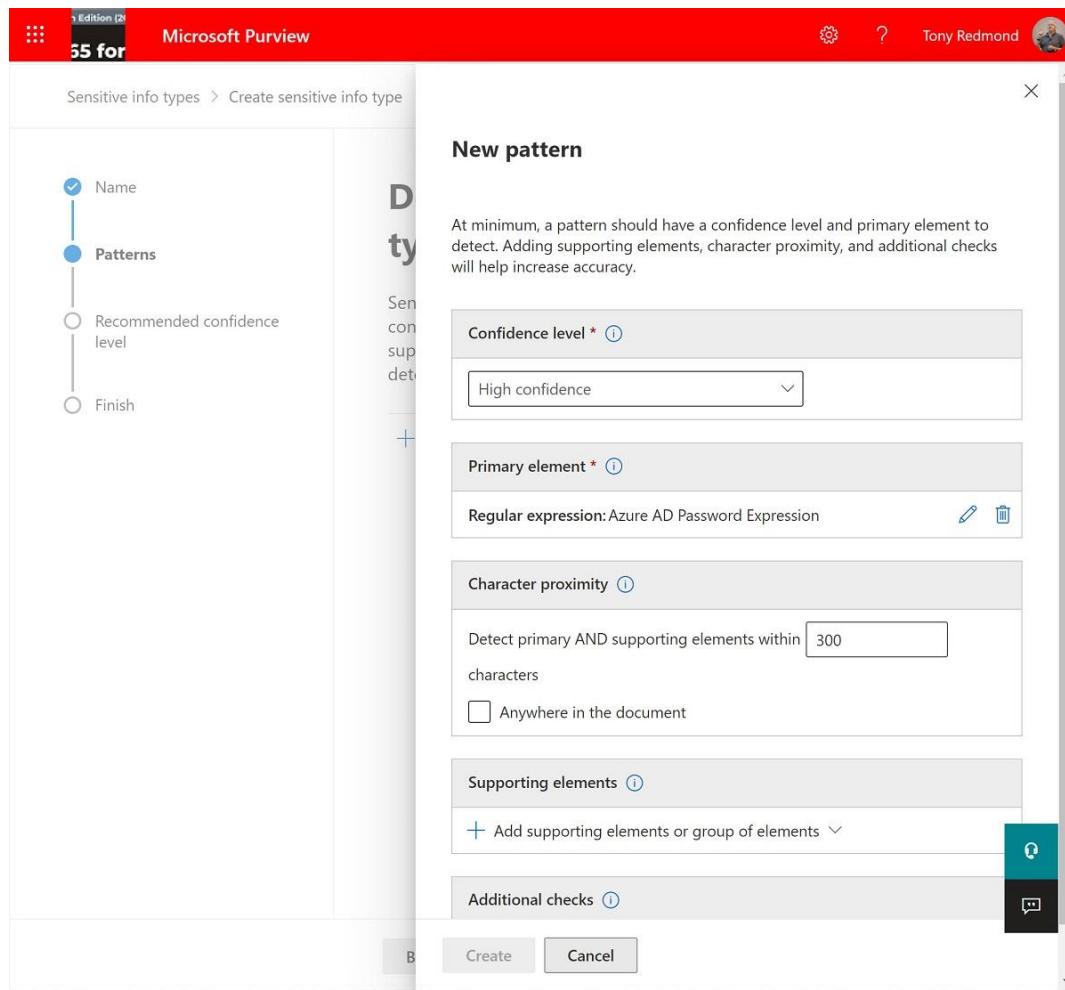


Figure 18-8: Defining a new custom sensitive information type

Testing a Custom Sensitive Information Type

After creating a new custom sensitive information type, it is wise to test it before attempting to use the new type in a policy. Select the custom sensitive information type from the set available in the tenant. Test is one of the available options.

At least two text files are needed for testing. One should contain a set of values that you expect the sensitive information type to detect; the other contains values that it shouldn't. For a more comprehensive test, you can create a suite of text files to check various combinations against the new type.

Click **Test** and browse to select a test file that you've prepared. Microsoft Purview uploads the file and tests its contents against the custom sensitive information type in the same way that a comparison occurs in a DLP policy. You'll then see the results of the test and the matches (Figure 18-9). We can see that the test made three matches using the primary element for three passwords found in the test file (65% confidence). The level of confidence increased to 75% because some of the keywords listed in the secondary element were detected within the defined proximity window.

The screenshot shows the Microsoft Purview interface for testing a custom sensitive information type. The left sidebar has a 'Sensitive info types' section with 'Azure Active Directory' selected. The main area shows a 'Match results' table with two sections: '1. Azure Active Directory password' and '2. Azure Active Directory password'. Both sections show four matches with supporting elements like 'Pwd' or 'Pwd', 'password'. Below the table are 'Back' and 'Finish' buttons.

Matches	Supporting elements
Mybestpassword	"Pwd"
NewThingtoTry56@	"Pwd"
GatheringDust12	"Pwd", "password"
Pwd!ForMe2	"Pwd"

Figure 18-9: Testing a custom sensitive information type

After the new custom sensitive information type passes its tests, you can go ahead and deploy it like any of the out-of-the-box types. It's important to test the custom sensitive information type in a variety of circumstances before you put it into production. For example, you should consider if it is necessary to exclude some email addresses from the policy (the easiest way to do this is to create a distribution list and use it to hold the accounts allowed to send passwords). Another thing to consider is whether a policy that works well for Teams (which mostly deals with internal communication) is equally effective for emails when you can exert less control over what external people might include in messages. The policy described here will, for instance, block email invitations for Zoom online meetings because the links to the meetings contain "pwd" and the string identifying the meeting looks like an auto-generated password. Finally, it's a good idea to consider how best to explain the rationale for the policy to end users so that people know what to do if the policy blocks their messages, including how they can override the policy (if policy settings allow an override).

The new custom sensitive information type can be managed in PowerShell. For instance, here's how to list all the custom sensitive information types in the tenant. The example we just defined shows up together with other types created by document fingerprinting (covered later).

```
Get-DlpSensitiveInformationType | ? {$_.Publisher -ne "Microsoft Corporation"} | Format-Table Name, Publisher
```

Name	Publisher
U.S. Tax Documents	Office 365 for IT Pros
U.S. Tax Form W-8BEN	Office 365 for IT Pros
U.S. Tax Form W-4 (2015)	Office 365 for IT Pros
U.S. Tax Form 1040 (2014)	Office 365 for IT Pros
U.S. Tax Form 1040EZ	Office 365 for IT Pros

Custom Keyword Dictionaries

In addition to defining custom sensitive information types, you can set up keyword dictionaries. A dictionary is a set of keywords that you want to check for in DLP policies. For instance, you could define a set of inappropriate words like *blast*, *damn*, and *bugger* that you don't want people using in internal email and Teams messages or a set of product code words that you do not want people to share outside the company.

The easiest way to create a keyword dictionary is with a simple editor like Notepad. Put each word on a separate line and save the file in Unicode format. You can then load the file into a PowerShell variable and use the variable to create the dictionary. In this example, we read the contents of a file called Codewords.txt and use it to create a dictionary with the *New-DlpKeywordDictionary* cmdlet.

```
$FileData = Get-Content c:\temp\CodeWords.txt -Encoding Byte -ReadCount 0
New-DlpKeywordDictionary -Name CodeWords -Description "Code Words for major projects"
-FileData $FileData

RunspaceId      : 3ab0f9ee-24ff-40c7-901c-c2bd8e43a830
Identity        : c1247f79-8cd8-4137-91a0-9c6dfb79192e
Name            : CodeWords
Description     : Code Words for major projects
KeywordDictionary : bitterball
                  : gandalf
                  : redsnark
                  : torchcraft
                  : x1050
                  : x1051
                  : x1052
                  : yellowplane

IsValid         : True
ObjectState      : Unchanged
```

To update a keyword dictionary, use the [Set-DlpKeywordDictionary](#) cmdlet. You can input a new set of terms interactively or load them from a file. After the keyword dictionary is created, you can use it as a primary or secondary element when creating a new custom sensitive information type.

Document Fingerprinting

Microsoft supports a comprehensive set of standard sensitive information types for use in DLP policies, but they cannot be aware of data that is uniquely sensitive to a company, like forms used in HR hiring processes, capital acquisition requests, employee review forms, and so on. Most companies would not like this information to be circulated externally and probably have security and privacy policies to govern external disclosure. DLP can help to educate users that confidential company documents should not be circulating in emails unless good business reasons exist.

Like the recognizable patterns that can be used to detect instances of data like social security numbers, documents have characteristics in terms of layouts, fields, and text blocks. You can use a process called fingerprinting to capture the characteristics of a document and create a digital signature in the form of a hash value. That signature, or fingerprint, then becomes a valid sensitive information type that can be used in DLP processing.

Microsoft Purview can create a digital fingerprint from a document in any of the formats supported by Microsoft Search. This includes any of the Microsoft Office formats plus Adobe PDF, so most documents used in corporations are candidates to serve as the basis of a digital fingerprint. It is always best to select a blank form rather than one that is filled in so that the resulting fingerprint is not affected by text or other markings

that will not appear in other copies of the form. Sample documents should not be password-protected or be graphic-heavy (text-based documents generate the best results).

[Document fingerprints](#) are used to create new sensitive information types usable across Microsoft 365.

After locating a suitable template file, use the *Get-Content* cmdlet to read the content of the file into a variable. In this case, I'm using the Irish Personal Tax Form 11.

```
$IrishTax11 = Get-Content "C:\Temp\Ireland Tax Form 11.pdf" -Encoding byte -ReadCount 0
```

Next, create a digital fingerprint from the variable generated by *Get-Content*:

```
$IrishTaxFingerPrint = New-DlpFingerprint -FileData $IrishTax11 -Description "Ireland Tax Form 11"
```

Finally, create a new sensitive information type from the fingerprint:

```
New-DlpSensitiveInformationType -Name "Ireland Tax Form 11" -Fingerprints $IrishTaxFingerPrint  
-Description "Ireland Personal Tax Form 11"
```

Microsoft 365 responds by listing the properties of the new sensitive information type. You can also check by running a command like:

```
Get-DlpSensitiveInformationType -Identity "Ireland Tax Form 11" | Format-Table Name,  
Type, Description
```

Name	Type	Description
---	---	-----
Ireland Tax Form 11 Fingerprint	Ireland Personal Tax Form 11	

The new sensitive information type is now usable anywhere in Microsoft 365 that supports sensitive data types.

Chapter 19: Managing Information Protection

Tony Redmond

This chapter discusses how to use information protection technology to protect email, documents, and other files. The topics covered include:

- The rights management service and Microsoft Purview Information Protection (MIP).
- Microsoft Purview Message Encryption (otherwise known as Office 365 message encryption, or OME).
- How to protect documents, email, and meetings with sensitivity labels.
- How to protect SharePoint Online document libraries and lists and OneDrive for Business sites.
- How rights management templates work and how sensitivity labels use rights management.
- Using PowerShell with protected content.

In some quarters, rights management enjoys a reputation of being a technology difficult to understand, implement, and manage. It is certainly true that deploying this kind of protection for on-premises infrastructures can take significant effort. Hopefully, we'll prove that although Microsoft Purview Information Protection uses many of the same concepts as found in on-premises deployments, it is easier to implement rights management-based protection in the cloud because Microsoft takes care of maintaining the infrastructure to issue and check user rights to access information.

The Need to Protect Data

We live in a world where encryption is pervasive for both businesses and consumers. It is unthinkable to consider conducting a banking transaction through a website not protected with encryption. Even so, an awful lot of email traffic still moves over unencrypted SMTP links (Exchange Online uses TLS to secure mail traffic in transit), perhaps because setting up reliable encryption for email has always run into the difficulties of agreeing on a common standard for external transmission and the cost of deploying and supporting an infrastructure to assure secure email internally. The earliest versions of Exchange Server included the Key Management Server (KMS) to manage the storage and distribution of keys for message encryption. At the time, the great hope was that the availability of KMS would encourage many organizations to adopt encryption to protect email. That hope never fully materialized.

Rights management delivers the capability to protect confidential messages or documents to control what recipients can do with the content (enforce usage restrictions). Without protection, an email recipient can forward messages they receive, print the messages, copy and paste message content, and so on. Rights management implemented through sensitivity labels allows an organization to define sets of rights that users apply to messages and documents to restrict what a recipient can do. The functionality protects companies by allowing them to circulate confidential or sensitive information under control and avoid situations such as "information leakage" which happens when, for instance, a disaffected employee forwards messages to journalists or other interested parties. Another example of similar functionality in a different context is the use of DRM to protect music downloaded from various sites. In addition, settings also control how long users can access information, after which the information becomes inaccessible. Microsoft offers several ways to deploy rights management to protect content:

- On-premises customers can deploy a Rights Management (RMS) server to manage the encryption keys used to protect data by both on-premises and hybrid users. [Hold your own key](#) (HYOK), which also uses keys managed by on-premises servers, extends the coverage to cloud applications. Because the complexities involved in using HYOK to protect data differ from customer to customer, we do not cover the topic here.
- Tenants can generate encryption keys and import the keys into Microsoft's data centers, where the keys are under the control of the tenants. This implementation is known as [Bring your own key](#) (BYOK) or HYOK.
- The most common method to implement rights management in the cloud is when Microsoft manages the encryption keys for tenants (a Microsoft managed key, or MMK). As with BYOK and HYOK, the keys issued to tenants protect information including Exchange Online messages and SharePoint Online and OneDrive for Business document libraries and lists.

Although the concept of rights management extends back to the early 1990s, Microsoft began implementing the technology for products like Exchange and Outlook in the middle of the decade. Rights management proved capable of protecting information, but customers did not take to the technology for a few reasons. Part of this was because of the culture shift needed inside companies to take the protection of information seriously, including strong executive leadership to champion the case for deploying the technology. Part of the reason was due to the extra infrastructure plus the time needed to deploy and run Active Directory Rights Management Services (ADRMS), the service underpinning protection within an on-premises environment. Because Microsoft delivers the required infrastructure and integration for cloud services, tenants need to dedicate less effort to secure protection.

The work to expand protection across Microsoft 365 is a journey. Newly-introduced capabilities include auto-application of sensitivity labels for Exchange Online messages in transit. We'll get to the new functionality as the chapter unfolds.

Rights Management

Microsoft 365 uses the Azure Rights Management protection service as the foundation for rights management and encryption to allow users to protect information through features like:

- **Microsoft Purview Message Encryption** (OME), a set of features to encrypt Exchange Online email including:
 - Out-of-the-box encryption for the Outlook and OWA clients through special *Encrypt Only* and *Do Not Forward* options. When OME encrypts a message, it places a special wrapper around the message that Exchange Online or Outlook.com recipients can automatically decrypt. Other recipients can access the content through the OME portal. OME's ability to protect email sent to any recipient using the Encrypt Only feature can replace the need to deploy S/MIME or other third-party tools. Outlook mobile clients can create and read messages protected by OME.
 - Recipients of encrypted messages outside the tenant can read the content in the OME portal by authenticating their access to the portal or using a one-time passcode. The same occurs when "unenlightened" clients (ones that don't understand rights-management based encryption) connect to Exchange Online. For instance, if someone uses an IMAP4 client to connect to Exchange, they must go to the OME portal to read any protected messages they receive.
 - Protection applied to outbound email by email transport (mail flow) rules. For example, a rule can ensure that any message sent to a partner domain is encrypted. Mail flow rules can apply the standard OME *Encrypted* and *Do Not Forward* protection as well as sensitivity labels defined in the tenant.

- Users and policies assign **Sensitivity labels** to messages and documents. While some labels only apply visual markings to content, others can invoke protection with rights management permissions. Clients that apply and process sensitivity labels use the MIP Software Development Kit. MIP is a framework or platform for developers inside and outside Microsoft to add protection to applications.
- **Information Rights Management protection** for documents downloaded from SharePoint document libraries. This form of protection is now obsolete, and tenants should migrate to sensitivity labels.

Some differences might exist in the capabilities depending on the data center region used by your tenant. For example, the [China](#) sovereign cloud region (operated by 21Vianet) have supported sensitivity labels only since May 2023.

Originally, Microsoft used the AES128-Electronic Codebook (ECB) cipher method with Office documents and messages protected by OME and sensitivity labels. Security researchers believed that it is theoretically possible for an attacker to amass many protected messages and search for patterns in the encrypted content to infer the meaning contained in that content. To address the criticism, Microsoft Information Protection uses AES256-CBC (Cipher Block Chaining) algorithm to protect all items created since August 2023.

Protection and Permissions

Rights management protects Items through a set of usage rights or permissions granted to a recipient. When a user applies a sensitivity label with encryption to a document, Purview writes the usage rights assigned to different users and groups into the document metadata. This ensures that the usage rights are available no matter where the document goes. It's important to understand that the usage rights written into a document are those that exist in the sensitivity label at the time. If the tenant subsequently updates the sensitivity label to modify the defined usage rights, the update doesn't affect files that are already labeled.

Logically, the author or originator of content always has full control over the content. You can compare applying a sensitivity label to a message as being analogous to registering a postal letter. The recipient is only able to open and access the content if the rights management service recognizes their access – the recipient gains access by having a known account (authenticated against Entra ID) with access rights defined by the sensitivity label that the application can apply to the item. If protected content ends up in the hands of an unknown user, they will not be able to access the content because it will stay within an encrypted "wrapper" that only intended users can open.

The set of available usage rights do not cover every possible circumstance or method that a recipient might use to interact with protected content. For example, if you don't grant the right, recipients can't take a screen capture of the content on Windows devices because Windows respects the denial of the right. iOS and Mac devices allow screen captures because those operating systems do not permit applications to restrict screen captures. This difference in behavior between operating systems illustrates the point that rights management can go so far in restricting deliberate attempts to share protected content. Taking a photo of a protected file open on a screen with a mobile device is another way around rights management unless the sensitivity label that protects the file uses dynamic watermarking. Rights management is therefore part of an overall solution to manage critical and sensitive information; it is not a complete answer if deployed without supporting user education, policies, and possibly other technology.

Other Ways of Using Protection

In addition to allowing authors to decide what level of protection to assign to their work by applying a label to a message or document, administrators can create mail flow rules to apply labels to messages that meet certain criteria as the messages travel through the transport pipeline. This is an excellent way to automatically protect confidential messages if you can create criteria to find those messages. For example, all messages that mention the word "Confidential" in the message subject or all messages sent to the "Corporate Planning"

distribution list. Mail flow rules protect messages without user intervention and users cannot override what they do. Best of all, this approach works for messages sent from any client.

Protecting messages through mail flow rules allows great control over information circulated through email. It also means that the content of any message sent externally is inaccessible because external recipients cannot retrieve the use licenses necessary for decryption. Fortunately, you can use encryption to protect messages sent to external recipients in a way that they can access the content securely.

While more difficult to manage, it is possible to use [an on-premises Active Directory RMS server](#) to deliver a Rights Management service to users. That setup is outside the boundaries of the discussion presented here.

Licensing Requirements for Microsoft Information Protection

Microsoft 365 has two Information Protection service plans. The standard service plan is included in [several Microsoft 365 licenses](#), including Office 365 E3. The premium service plan is in licenses such as Microsoft 365 Compliance E5 and Office 365 E5. These service plans govern the functionality available through sensitivity labels to protect email and documents in Exchange Online, SharePoint Online, and OneDrive for Business. The standard Information Protection service plan covers the use of sensitivity labels to manually classify and protect content stored in Exchange Online, OneDrive for Business, and SharePoint Online. The premium service plan enables functionality like automatic labeling at rest and label analytics. Tenants don't need licenses to apply sensitivity labels to items using Exchange Online mail flow rules. Some examples of functionality needing specific licensing requirements include:

- Apply sensitivity labels to protect Outlook meetings: Office 365 E5.
- Apply sensitivity labels to protect Teams meetings: Teams Premium.
- Define a default sensitivity label for a SharePoint Online document library so that new documents receive the label: Office 365 E5, Microsoft 365 E5, or Syntex-SharePoint Advanced Management.

All Microsoft 365 licenses include the ability to consume protected documents (in other words, to open protected documents). For instance, an account with an Office 365 E3 license could protect a document with a sensitivity label and circulate the document to users with frontline (F1) licenses who can read the content. Microsoft Purview Message Encryption is part of the Office 365 E3 and E5 plans (enterprise, academic, and government) plus Microsoft 365 Business Premium. For other plans like Exchange Online Plan 1 or 2, you'll need to purchase the Microsoft Compliance E5 license.

When you see references to premium licenses in this chapter, the feature under discussion needs a premium license. With the number of features, products (SKUs), and service plans available for Microsoft Purview, the issue of licensing can be quite complex and it's wise to check exactly what you need. Microsoft [publishes guidance](#) to help tenant administrators and licensing coordinators understand when premium licenses are required.

In some cases, a feature might not enforce the stated licensing requirement. This could be because the necessary code is not yet available. The code might or not appear soon. In any case, a tenant must have licenses to use functionality. It's a bad place to be in if features the business depends on suddenly stop working because Microsoft updates its license enforcement code.

Licensing the Protection of Content Stored Outside Microsoft 365

Your organization may want to protect files both inside and outside Microsoft 365. Office 365 E3 and E5 licenses cover the use of sensitivity labels and OME to protect documents and messages stored in Microsoft 365 repositories and to protect emails sent outside the organization. To apply sensitivity labels to files stored in external repositories (like network file shares) or to files belonging to applications that don't include native support for Microsoft Information Protection, you must:

- Deploy the Microsoft Purview information protection client to Windows PCs.

- Assign Information Protection licenses to accounts that apply protection to external files.

Licenses are available standalone or bundled in the Enterprise Mobility and Security and Microsoft 365 enterprise plans. The basic rule here is that using the information protection client to protect a file (or to change the protection on a file), requires a license. On the other hand, no license is necessary for someone who only opens and accesses the content in protected files.

The information protection client does not check licenses. If an organization has a Microsoft Information Protection subscription, all clients within the organization can download the policy and use labels.

The Flow of Protection

When a tenant activates rights management (the default state), clients use an automatic process to receive certificates from the rights management service to allow users to access protected content even when they work offline. The service keeps a copy of the user's Rights Account Certificate (RAC) so that it can issue it to another workstation if the user connects from there. Once authenticated, users can send and receive protected messages or apply sensitivity labels to protect files. When a user protects a message or document (for example, by applying a sensitivity label), the client embeds a unique key (the content key) in the item's header. To protect an item, the client encrypts it (and any attachments which support protection) using the AES 256-bit symmetric encryption algorithm. The content key persists with the item even if the author edits it to create an updated version. Rights management protects the content key with another key (the tenant key), which is common across all protected content. Either Microsoft or the tenant can manage the tenant key.

When it encrypts information, the client generates a certificate called the publishing license which includes a policy with the usage rights for recipients (individual users or groups) as well as any other restriction, such as an expiry date. Like all the licenses used by rights management, the publishing license is an [XrML certificate](#). The settings stored in the publishing license come from the sensitivity label selected to protect the content. The client signs the publishing certificate with a user certificate. The client also encrypts the publishing certificate and the content key using the tenant key. Finally, the client combines the encrypted content with the signed and encrypted publishing certificate to create the protected item. This step ensures that the publishing certificate always stays with the encrypted content. If necessary, the rights management service can use the information in the publishing certificate to create a use license in cases when the template used by a sensitivity label is inaccessible for some reason.

When a recipient reads protected content, the client extracts the publishing certificate from the protected item and sends it and the user certificates to the rights management service, which decrypts and evaluates the set of rights for the item. The service then extracts the content key from the publishing certificate and uses it to create an encrypted use license holding the set of rights allowed to the user and returns the license to the client. The client decrypts the use license with the user's private RAC key to extract the content key, which it uses to decrypt the content before displaying it to the recipient. The client also handles the enforcement of rights given to the user by policy, including limiting access if the license is valid for a certain period. When a use license for an item expires (usually after 30 days), the user must reauthenticate to get another license.

Mobile clients like Outlook for iOS use a simpler transactional flow. When mobile clients protect content, they send the selected policy to the server and receive a publishing license and symmetric key to protect the item. To consume protected content, the client sends the policy to the service and requests a use license. The service responds with the necessary keys and policy information to allow the client to open and display the content.

Access to Protected Content for External Users

Protection works on the basis that a recipient can authenticate themselves using an Entra ID account or a Microsoft Service Account (MSA) associated with an email address. People in other tenants and other email

domains can receive items protected by sensitivity labels, providing that the rights assigned in the sensitivity labels used to protect the items allows those recipients to access the content.

Entra ID federates with some other directories, such as Gmail and Yahoo, to allow users of those services to authenticate by signing into that service. Otherwise, the external user must sign in using an MSA account or a [one-time passcode](#) before they can access the document.

It's possible that configuration settings applied to your directory or to the directory of other tenants will stop users collaborating through encrypted email or documents. These settings include conditional access policies and cross-tenant access policies, which can stop the Azure Information Protection service decrypting protected content. An example is where a tenant applies conditional access policies to enforce multifactor authentication for all cloud apps. This configuration causes a problem for Outlook desktop users in other tenants who receive protected email because Outlook cannot satisfy an MFA challenge when it attempts to connect to the Microsoft Rights Management Services app to obtain a use license. The net effect is that the user cannot read the message through Outlook. Instead, they see the protected wrapper (RPMMSG) for the message and must read the content through the Office 365 Message Encryption Portal. Clients like OWA and Outlook Mobile aren't affected because of the way that the service fetches use licenses on their behalf. The solution is to exclude the Microsoft Rights Management Services app (*appid: 00000012-0000-0000-c000-000000000000*) from any policy that imposes MFA for all cloud apps.

For more information about conditional access and information protection, see [this article](#).

Enabling Rights Management for a Tenant

Before you can protect content, the rights management service must be enabled. Microsoft [enables rights management automatically](#) for eligible tenants. In other words, if you have an eligible plan like Office 365 E3 or E5 or buy the Azure Information Protection add-on for other plans, you do not have to enable Rights Management. Users with other Office 365 licenses can consume sensitivity labels applied to content but need to have an upgraded license to apply labels to content. See [this documentation](#) for information about enabling the protection service in a tenant.

Configuring Rights Management for Exchange Online

Although Microsoft configures Exchange Online so that you can use OME and sensitivity labels without doing anything else, you might wish to change some of the settings for the rights management configuration. This section explains how to make those changes. We'll discuss how to configure other relevant settings for how OME handles messages sent to other email systems and protection for SharePoint Online later.

Configure Exchange Online

The *Get-IRMConfiguration* cmdlet reports the current rights management configuration for Exchange Online while the *Set-IRMConfiguration* cmdlet is used to update settings. Microsoft configures rights management for all eligible tenants and sets the *AzureRMSLicensingEnabled* property in the IRM configuration to *\$True* to enable Exchange Online to use the Azure Information Protection service. See [this page](#) for more information.

Viewing the IRM configuration

Run the *Get-IRMConfiguration* cmdlet to check the rights management configuration. If any changes are necessary, you can make them with the *Set-IRMConfiguration* cmdlet. For example:

```
Set-IRMConfiguration -InternalLicensingEnabled $True -ClientAccessServerEnabled $True  
-EnablePdfEncryption $True
```

In most cases, you do not have to amend the default configuration to use start protecting email. If you want to, you can investigate settings such as:

- **AutomaticServiceUpdateEnabled:** Controls if new Information Protection features are automatically enabled in the tenant. The default is `$True` and it is best to leave this setting alone unless you have good reason to block the deployment of a new feature into your tenant.
- **AzureRMSLicensingEnabled:** This should always be True as it controls the ability of Exchange Online to connect to Azure Rights Management.
- **ClientAccessServerEnabled:** Default is `$True`. Controls whether OWA and ActiveSync clients (including Outlook for iOS and Android) can use IRM to protect and decrypt messages. When true, Exchange Online can fetch use licenses from the rights management service on behalf of these clients (see below).
- **DecryptAttachmentForEncryptOnly:** Controls if Exchange Online decrypts attachments for messages protected with the *Encrypt Only* feature. The default is `$False`, meaning that attachments remain encrypted, even when downloaded. If you change this control to `$True`, Exchange Online decrypts the attachments, and recipients have full control over the files. (Note: the older *DecryptAttachmentFromPortal* setting is deprecated).
- **EDiscoverySuperUserEnabled:** Default is True, which allows members of the Discovery Management RBAC management role group to access protected information found through (now deprecated) Exchange Online eDiscovery searches.
- **EnablePdfEncryption:** Set to `$True` to enable OWA and Outlook Mobile clients to apply sensitivity labels or standard OME templates to protect messages with PDF attachments. These clients include the necessary code to apply protection to PDF attachments, but Outlook desktop clients do not. To extend coverage to messages with PDF attachments sent from Outlook desktop clients, use an Exchange mail flow rule or DLP rules to apply a suitable sensitivity label to messages with PDF attachments. When users download protected PDFs, they can be opened with [an app that supports the ISO standard for PDF encryption](#), including the Edge browser.
- **InternalLicensingEnabled:** Default is `$True`. Controls whether licenses are automatically granted to internal recipients to allow them to access protected content.
- **JournalReportDecryptionEnabled:** Default is True. Controls whether the Exchange Online transport service uses its IRM super-user privilege to decrypt protected messages copied by journal rules to an external journaling system. When this happens, the journal recipient receives a journal report with two attachments. One holds the original message, the other the decrypted copy. Decryption works for both the default (Encrypt Only and Do Not Forward) options and custom sensitivity labels.
- **SearchEnabled:** Default is True. Controls whether OWA can search protected items in a mailbox.
- **SimplifiedClientAccessDoNotForwardDisabled:** Set to `$False` to make the *Do Not Forward* option available for messages in OWA.
- **SimplifiedClientAccessEnabled:** Controls if the Protect button is available in OWA. Set to `$False` if you don't want users to apply protection to messages. This control is now obsolete as the Protect button has been replaced by the Sensitivity button.
- **SimplifiedClientAccessEncryptOnlyDisabled:** Controls if the *Encrypt Only* option is available in OWA. Set to `$False` to disable the option.
- **TransportDecryptionSetting:** Default is Optional. Controls the access to protected messages for the transport service as they pass through the transport pipeline. Optional means that the transport service tries to decrypt protected messages so that the content is available for checking by transport and DLP rules or by anti-virus agents. Exchange Online will continue to process and deliver the message even if decryption is not possible. You can disable any attempt to decrypt messages by setting this value to *Disabled*. Setting it to *Mandatory* means that transport will reject any messages that it cannot decrypt and return a non-delivery report to the sender. The transport service automatically re-encrypts decrypted messages when they reach the end of the transport pipeline.

To make things easier for OWA users, if the *ClientAccessServerEnabled* setting in the IRM configuration is `$True`, Exchange Online imports keys from the Rights Management Trusted Publishing Domain (TPD) and is

thereafter able to decrypt content locally on behalf of clients so that OWA can display protected content inline within message windows. Some Exchange ActiveSync clients use the same approach, which is known as prelicensing.

The *Test-IRMConfiguration* cmdlet is available to test that everything is configured properly. For more information, see the [cmdlet documentation](#).

Bring Your Own Key (BYOK)

Microsoft 365 allows customers who need the highest possible degree of control over all aspects of security the ability to have full control over their tenant key, the element that serves as the root of trust for protection. The key is “pinned” or imported to a FIPS140-2 hardware security module (HSM), usually kept under tight control at a customer’s premises. In collaboration with Thales E-Security, Microsoft uses a secure process to transfer the key from a customer and import it into the Microsoft data centers into [Azure KeyVault](#) to make the key available to serve as the basis for protection. The process is free but needs a good deal of planning and coordination. Both SharePoint Online and Exchange Online support Azure KeyVault, so once a tenant imports its key to become the tenant key, that key becomes the base for encryption for SharePoint and Exchange content, except when encryption is applied through sensitivity labels as the rights management templates used by these labels are cloud-based. See [this link](#) for more information about BYOK.

Sensitivity Labels

The original implementation of cloud-based rights management followed the approach taken for on-premises deployments and used rights management templates to protect content. Microsoft Information Protection underpins the rights-management driven encryption side of sensitivity labels. Given the complex nature of anything to do with encryption, the deployment of sensitivity labels can take time to achieve, especially in large, complex companies. The basics of sensitivity labels are:

- Administrators manage sensitivity labels in the Information Protection section of the Microsoft Purview Compliance portal. Administrators must publish sensitivity labels to users through label policies before users can apply labels to content.
- The settings defined in sensitivity labels allow the labels to perform three major functions:
 - Apply visual markings such as headers and footers to Office documents and emails.
 - Protect the content of files with rights-management based encryption (Microsoft Information Protection). Encryption is persistent and remains until someone with the necessary rights removes the label. To gain access to protected content, users must authenticate.
 - Manage containers (Teams, Microsoft 365 Groups, and SharePoint Online team sites).

Labels don’t have to perform all functions. The scope set for a label establishes its use. Applications use the defined scope to decide if they should reveal a label to users. For instance, client user interfaces do not reveal labels used solely for container management when displaying the set available to users to protect files.

- Applications use the Microsoft Information Protection SDK to incorporate code to recognize and support the protection (encryption) applied through sensitivity labels. Within Office 365, support is available in Exchange Online, SharePoint Online, and OneDrive for Business. Users apply labels to email, meetings, and documents through the Microsoft Office apps. Other applications like Power BI use sensitivity labels to protect objects and when users export content. Teams uses sensitivity labels to manage team settings and meetings, but doesn’t currently use sensitivity labels to protect conversations and chats. Files protected by sensitivity labels are viewable in Teams. The capability exists to use [sensitivity labels to protect assets like SQL databases in Microsoft Purview Data Map](#).
- The Office 365 E3 and E5 plans include the license to apply sensitivity labels manually to items. All Office 365 users can consume (read) files protected by sensitivity labels.

- [Document unstructured models](#) generated by Microsoft Syntex can apply both retention and sensitivity labels files stored in document libraries.
- Sensitivity labels support manual (explicit assignment) by users or automatic assignment by policy (implicit assignment). A label assigned by an automatic process cannot replace a label assigned by a user.

The ability to apply labels to items is increasingly pervasive across Microsoft 365, meaning that it is very easy for information generators to apply appropriate labels as they create new content. Once applied, the labels are persistent and remain in place for the lifetime of items. Only administrators or people with author (including co-owner) rights can remove sensitivity labels from items.

Microsoft Endpoint Manager and Microsoft Defender for Cloud Apps support sensitivity labels. Policies can apply labels to ensure that users don't copy unprotected content to a third-party app like DropBox or removable storage like a USB drive.

Default Sensitivity Labels: Organizations starting with Information Protection can [create a default set of sensitivity labels and policies](#) to protect email, files, and meetings. The policies include client-side auto-labeling for Office documents and server-side auto-labeling to find and label files. While the default labels and policies are useful and can be tailored to meet tenant needs, it is often better to pause and think through the organizational requirements for information protection before deployment. That way you'll make sure that the best long-term choices for information protection are implemented.

Retention and Sensitivity

Some confusion might exist over the functions of retention labels and sensitivity labels, so let's summarize the differences and similarities:

- Documents and messages can have a single sensitivity label and a single retention label, but not multiple labels of either type. An exception exists where a document can have several sensitivity labels, but only when the document passes through multiple tenants and users apply a label without encryption in each tenant. Once a document receives a sensitivity label with encryption, that label becomes the document's sole and only sensitivity label.
- Retention labels are only valid within the Microsoft 365 tenant that owns the label. A sensitivity label is persistent and remains with an item until removed by someone with the right to do so.
- Both types of labels are applicable manually (by a user) or automatically by an auto-label policy. It's also possible to use the presence of sensitivity labels as a condition for the auto-application of retention labels.
- Sensitivity labels support container management. Retention labels can be the default for a container like a SharePoint site, but they have no management function.
- Sensitivity labels support different actions for data types. For example, a sensitivity label can include actions applying only to meetings.

Marking Important Content

Applying a sensitivity or protection label (think of a label as an adhesive sticker) to a document or email marks the item as having a certain level of importance to the organization. Usually, the higher the sensitivity of the content, the more stringent the protection invoked by the label. Some labels are purely visual indicators for a certain kind of content, like "Public." Others impose visual markings on documents and email to help users understand that the information is more sensitive; for instance, a label named "Confidential" might insert a footer and watermark in documents when applied. The most interesting type of label uses rights management to protect the most sensitive content. For example, a "Secret" label might use permissions to grant view-only access to anyone in the tenant while blocking access to anyone external.

Items and Containers

Sensitivity labels support:

- **Items:** The traditional use of sensitivity labels is to apply visual markings and protection to files, meetings, and email. Protection for items means that Purview encrypts their content (and attachments for email and meetings). Item metadata remains unencrypted. For documents, this means that users without the right to open an item can see document titles, dates, and authors. For email and meetings, it means that message subjects and metadata are unencrypted. This is a good thing because it allows clients like Outlook Mobile that rely on server-based decryption to use deeplinks to Teams meetings sent in meeting invitations.
- **Containers:** If configured for the tenant, labels can apply management settings to Teams, Microsoft 365 Groups, and SharePoint Online sites. Applying labels to containers does not protect the items stored in the containers. Microsoft is building out the set of controls settable through labels to make this capability more useful and powerful. Only administrators and container owners can apply labels to containers.
- **Schematized data assets (preview):** Users can apply sensitivity labels to files and schematized data assets like Azure SQL in Microsoft Purview Data Map. This chapter doesn't cover this application of sensitivity labels.

Labels and Applications

Assigning sensitivity labels to items for visual marking and protection through rights management-based encryption is known as information protection. Applying labels to containers is container management. The settings defined for a label sets its scope, which can be:

- Information protection only (file, email, meetings).
- Container management only (site, unifiedgroup).
- Both information protection and container management (file, email, meetings, site, unifiedgroup).

When the Microsoft Purview Compliance portal displays a list of labels, it shows the scope for each label as its content type (listed in parenthesis above). As discussed later, it is often easier to manage sensitivity labels when organizations create dedicated and separate sets of labels for the two purposes. Some advocate the case for creating a third set of labels exclusively for meetings. This becomes slightly complicated because a label configured for meetings must also include support for files and email.

Applications check labels to understand their scope and filter out the labels that they cannot use. For example, the set of labels available in the Office apps includes labels with information protection settings. The set displayed in the Teams client when someone creates a new team is those that have container management settings.

Container Management Labels

Microsoft is gradually extending the number of container management label settings, such as external sharing behavior for SharePoint or the visibility of private teams. A sensitivity label doesn't need to have container management settings. Any label without these settings is excluded by client applications when they display the list of labels available for assignment to a container. Information protection settings, such as encryption and marking, don't apply to containers.

Configuring a tenant to support container management labels is a one-time operation by updating the *EnableMIPLabels* setting in the Entra ID Groups policy. When the value of the setting is True, applications that support container management know that they should replace the older text-only classifications with sensitivity labels.

The Entra ID Groups policy can only be updated using PowerShell. This code uses a Microsoft Graph PowerShell SDK interactive session to update the tenant copy of the Groups policy. It assumes that a tenant-specific copy of the policy exists. If you haven't customized the groups policy before, see the instructions for how to create a tenant-specific copy in the Groups management chapter.

```
Connect-MgGraph -Scopes Directory.ReadWrite.All -NoWelcome
# Get Entra ID Groups Policy settings
$TenantSettingsId = (Get-MgDirectorySetting | Where-Object {$_['DisplayName'] -eq "Group.Unified"}).Id
$templateId = (Get-MgDirectorySettingTemplate | Where-Object {$_['DisplayName'] -eq
"Group.Unified"}).Id
# Update to enable sensitivity labels
Update-MgDirectorySetting -TemplateId $TemplateId -DirectorySettingId $TenantSettingsId -Values
(@{`'name`='EnableMIPLabels';`'value`='true'} | ConvertTo-Json)
```

For debugging purposes, you can check the set of container management labels by entering the following into a browser (replacing *tenant* with your tenant's name):

```
https://tenant.sharepoint.com/\_api/GroupSiteManager/GetGroupCreationContext
```

Gaining Rights to Access Content

When someone receives protected content, Microsoft Information Protection checks their signed-in account against the access granted to the users and groups specified in the sensitivity label. If the account is not present in the list of permissions, they won't be able to open the content. Whenever possible, it is best to grant rights to groups rather than individuals as this makes rights assignment easier to manage.

Microsoft Information protection depends on user accounts to authenticate access to content protected by encryption imposed by sensitivity labels. This isn't an issue if you share documents with people in another Microsoft 365 organization as the recipients authenticate against their home tenant directory. Likewise, it's not an issue if an external recipient has a Microsoft Services account because these accounts also authenticate against a Microsoft directory.

If you need to share protected content with people who don't have an Entra ID account, you can create guest accounts in your directory and the external people can sign in using those accounts, just like external recipients of SharePoint Online sharing links sign in to access shared documents. The [SharePoint Online and OneDrive for Business integration with Entra ID](#) creates guest accounts automatically for sharing. If you use this integration, guest accounts may well exist for the people with whom you share protected content.

If you assign access to an external user in a label, it's a good idea to check if their email address belongs to a Microsoft 365 organization, and if not, create a guest account. Remember to inform the person that they'll need to use the guest account to sign in to access protected content received from your organization. It's also wise to remind the external user that they must use a suitable application to access protected content, such as Microsoft 365 apps for enterprise or the standalone edition of Office 2022.

Double Key Encryption

For extra security, organizations can run a Double Key Encryption (DKE) service to manage encryption keys. Double key encryption is a form of protection where the customer holds one key and Microsoft holds the other. When a sensitivity label uses double key encryption, two keys are necessary to access a protected item's content. Microsoft Information Protection manages one key; the DKE service manages the other key, which remains under the control of the organization. If the DKE service is inaccessible, the content cannot be decrypted.

To configure double key encryption for a label, you must provide the URL of the DKE service. Because of the additional cost and complexity, most organizations don't use double-key encryption. [Double-key encryption](#) requires Office 365 E5 or Microsoft 365 E5 licenses. Since August 2023, the Microsoft 365 enterprise apps

(current channel) can apply and consume sensitivity labels configured to use double-key encryption, including for co-authoring of protected documents. Support for the semi-annual enterprise channel is available from late March 2024.

While deploying a DKE service on Azure is the fastest implementation method, it's also possible to [run the DKE service using an on-premises Windows server](#).

Native Support in Microsoft 365 Apps

Native support means that an app includes the necessary code (built using the Microsoft Information Protection SDK) to fetch policy and label information from the unified store and comply with policy settings, including encryption, as users assign sensitivity labels to items. Microsoft Office is a good example of an application that replaced the need to run a separate client with native support. Among the advantages gained by the integration are better cross-platform support, increased performance, lower memory demand, and avoiding problems that can happen when apps like Word or PowerPoint load add-ins. In addition, the regular updates issued for the Office apps include updates for sensitivity labels, so there's no need to update separate components.

Native support for sensitivity labels is available in the Office mobile apps, the desktop apps for Windows and Mac, and the Office Online apps. Table 19-1 summarizes the current support for sensitivity labels in different client platforms.

Client	Notes
Microsoft 365 Apps for Windows (Outlook, Word, PowerPoint, Excel)	Office desktop clients for Windows and Mac include native support for sensitivity labels as described in this section. The perpetual versions of Office don't include sensitivity labels.
Office online apps	Supported by Word Online, PowerPoint Online, and Excel Online.
Office mobile apps	Available for Word, PowerPoint, Excel, and Outlook mobile on iOS and Android.
PDF files	Export from protected Office files generate protected PDF files. Paid-for Adobe Acrobat DC versions can also generate protected PDFs.
Other non-Office files	Use the information protection client to apply labels to these files. You can then import the files into SharePoint Online or OneDrive for Business.

Table 19-1: Client support for sensitivity labels

The Sensitivity button in the menu bar allows users to apply, update, or remove sensitivity labels when working with Office files. The user's signed-in account appears at the top of the list of labels revealed by the Sensitivity button. Documents with a sensitivity label display the name of the label in the bottom information bar. A label icon appears when the applied label doesn't include encryption and a padlock icon when it does. In addition, the Office desktop apps include file information at the top of the document where the app displays the label name (and color, if defined). If clicked, a fly-out (Figure 19-1) appears showing the file name, location, sensitivity label name (and description) and a link to access the version history. The user can assign a different sensitivity label from this screen.

Objects that support sensitivity labels store metadata, including the label identifier (a GUID) and tenant identifier. When an application opens a file, it reads the metadata. If the tenant identifier stored in the metadata is the same as the user's tenant, the application displays the label name in the status bar. If someone shares a labeled item with another tenant that uses sensitivity labels, the application does not show the label because it doesn't come from that tenant. Nevertheless, the application respects the permissions set by the label from the original tenant and won't allow users to access the content unless they have the right to do so. Visual markings such as footers or watermarks applied by a label in the original tenant remain visible.

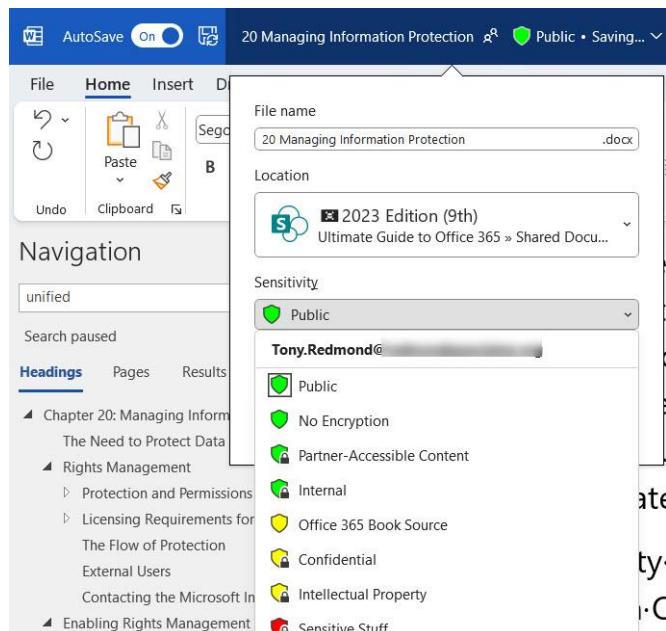


Figure 19-1: Sensitivity label information displayed in a Word document

Purview Information Protection Client

Those who don't use a version of Office that includes native support for sensitivity labels or want to apply sensitivity labels to files stored outside Office 365 can deploy [the Purview information protection client](#). The information protection client:

- Integrates with Windows File Explorer to allow users to assign sensitivity labels to files stored outside Microsoft 365 through the **Apply Sensitivity Label with Microsoft Purview** option in the right-click menu.
- Installs a viewer to allow the display of protected content when an application doesn't include the necessary Microsoft Information Protection code to process rights management and encryption.
- Installs the [Purview Information Protection](#) and [AIP Service](#) modules to allow administrators to interact with protected files and manage the AIP service.

The information protection client uses the Information Protection SDK to retrieve settings for labels and policies necessary to apply sensitivity labels to files stored in external locations like a Windows drive. The information protection client replaces the older unified labeling client, or AIP client. The big difference between the two clients is that the older client includes an integration with Office. That integration is no longer necessary because of the native labeling capabilities incorporated in the Microsoft 365 enterprise apps.

Third-Party Support for Microsoft Information Protection

The [Microsoft Information Protection SDK](#) is available to help ISVs develop integrated solutions based on MIP. Some examples include:

- Symantec DLP integration with MIP: decrypts protected content for DLP scanning.
- McAfee MVISION: applies labels to sensitive content discovered during scans.
- Relativity Trace: examines protected content during communication monitoring.
- VMware Boxer and Workspace ONE: apply labels to protect sensitive content.
- Adobe Acrobat (paid versions) supports in-app assignment and update of sensitivity labels.

Planning Sensitivity Labels

Before creating any sensitivity labels, it is sensible to chart out a plan for protection within the tenant. The plan should include a discussion of points such as:

- **Consider applying a default label:** The policies used to publish sensitivity labels to users can dictate a default label for documents and messages. One school of thought is that people are more likely to understand the use of labels if new documents and messages receive a default label. If you choose to go along this path, consider not using encryption with the default label. The argument against applying default labels is that the application of a sensitivity label should have some purpose, and rights management-based protection is a great way to convey the level of importance, confidentiality, or sensitivity of an item. Users should therefore make considered decisions about the right label to apply to a specific item. The decision as to which course to take is highly dependent on the organizational culture and the goals for the deployment of sensitivity labels. MIP applies default labels to new Office documents and to existing documents when a user modifies those files.
- **Restrict the number of labels.** Although an organization can deploy up to 500 labels, it's debatable if more than a small number of labels meet the needs of all but some corner cases. Using the keep it simple principle, the set of labels available to "the average user" shouldn't include more than ten labels to make it easy for the user to understand what label to apply when. It's easy to add extra labels to meet specific business needs to the general set of labels published to the entire organization.
- **Scope labels.** The scope of a label determines the applications where a label is available. The following scopes are available:
 - **File:** Apply labels to Office documents and PDFs (plus files stored outside Office 365 via the Purview Information Protection client). These labels are available in the Microsoft 365 apps for enterprise and the paid-for version of Adobe Acrobat.
 - **Email:** Apply labels to items in Outlook desktop, OWA, and Outlook mobile.
 - **TeamWork:** Apply labels to Outlook and Teams meetings.
 - **Container:** Apply labels to Microsoft 365 Groups, Teams, and SharePoint Online sites via administrative interfaces. The Microsoft Purview Compliance portal shows this scope as "*Site, UnifiedGroup*."

Although you can have "cross-over" or multi-purpose labels that apply to multiple scopes, such as a "General access" label that applies to files, email, meetings, and containers, it is often simpler and therefore better to restrict labels to a specific scope to reduce the number of labels presented to users to choose from. The smaller the number of labels, the more likely it is that users will select the most appropriate label.

- **Names and descriptions associated with company workflow and culture are more understandable.** For example, if the company uses "Confidential" to mark highly sensitive documents for years, it's a good choice to use it as the display name for a sensitivity label. Don't put confidential information (like "Company Merger") in label names – choose a code name instead. Test your label names with real users before committing to the final set of names. Include a description of the kind of information that you intend people to use the label to mark. For items, the description should tell the user about the level of sensitivity of the information considered appropriate for the label. For containers, the description should say something about the settings that the label will apply, such as privacy, guest access, and the site sharing capability. Display names can up to 64 characters long but cannot contain these characters: % \ & < > | ? : ;
- **Choose enduring label names.** Labeled items can exist for many years. Choose names that will last rather than those associated with one-time events. Give labels used for container management names different from those used for information protection. Assigning an appropriate color to a label can also help people understand the relative degree of sensitivity or confidentiality for files marked with the label.
- **Organize using Sublabels or a simple list.**: Two methods are available to organize the labels presented to users in applications: a simple list or labels organized into sets of parent and child labels (sublabels). No right choice exists for an organization. Factors influencing the choice depend on the

number of labels published to users and the complexity of the information protection scheme. For instance, a simple list is probably best when only five or six labels are in use. Above this number, you might find it better to organize labels into sets of parent labels and sublabels.

- **Protection and marking applied by labels.** Some labels serve solely as visual indicators of an item's sensitivity without taking any protective action. Other labels impose actions such as marking and/or encryption. The protection given by a label should match the expected sensitivity set by its name, and the rights assigned in the label must support its use within the organization (or outside, if users share labeled items with external people). Remember that a label can also apply visual marking to items (watermarks, headers, and footers), so consider whether to include this action in a label.
- **Involve more than IT.** It's unlikely that IT understands every business and legal ramification flowing from how people use information within the company, so involve other expertise before settling on a final design.

The goal is to create a practical set of sensitivity labels that make sense to people and meet business requirements without over-complicating matters. It's bad to have labels that people never use, and good when sufficient labels are available to allow users to select granularity in terms of confidentiality. In some cases, it might be possible to have a general-purpose label such as "Company Confidential" that allows full access to any tenant account while blocking external access. Such a label might deliver enough protection for a large percentage of use cases. In other circumstances, specific labels might be necessary to restrict access to certain sets of users or to grant rights to selected groups of users. In other words, the plan should define a set of labels to meet the needs of the business while limiting the number of labels to a manageable set.

A form like that shown in Table 19-2 is useful to describe a plan for sensitivity labels, ordering the set of labels used for information protection in order of sensitivity from least sensitive to most confidential. The Microsoft Purview Compliance portal organizes sensitivity labels in this order. Office applications use the order to know whether a user has replaced a label with one of higher or lower sensitivity.

Label Name	Description	Color	Marking	Protection	Extended Protection
Public	Content approved for sharing outside the company.	Green	Footer	None	None
Internal	Content that should remain internal but can be shared.	Yellow	Footer	None	None
Confidential	Content that should remain inside the company.	Yellow	Footer	Yes	None
Secret	Content that should never go outside the company.	Red	Footer and watermark	Yes	7-day expiry
Ultra	"Eyes-only" content for restricted circulation.	Red	Footer and watermark	Yes, restricted to certain groups	3-day expiry

Table 19-2: Planning Sensitivity Labels for Information Protection

Purview supports the use of colors to highlight different types of labels. For instance, you could use green labels to mark items for general access, yellow to mark those with more restrictive access, and red for the most confidential items. Administrators can assign colors to labels when configuring label settings in the Purview Compliance portal or by running the *Set-Label* PowerShell cmdlet. See [this article](#) for more details about how to apply a traffic light system for sensitivity label colors.

In addition to the set of general-purpose sensitivity labels, the plan might include labels for use by certain projects or departments. For instance, you could create a label for the Legal Department to mark documents associated with a patent application or other aspects of intellectual property.

Label names should leave users in no doubt as to the relative importance or sensitivity of the information in an item. After all, they have no idea of the position a label has within the list managed by Microsoft 365: all they see is the label name, so it's critical to give labels meaningful and understandable names. Because label names might appear in mobile applications on devices with limited screen estate, it's best if the names are short rather than long.

Changing Label Priority

Figure 19-2 shows a set of sensitivity labels displayed in the Microsoft Purview Compliance portal. Remember that the portal lists labels in priority order with the most important labels at the bottom of the list. The labels are in the order described above, with some of the labels created for use by projects and departments coming after the set intended for general-purpose use. The names of the labels appear rather than the display names, which is what users see in applications. Usually, the name and display name are the same for a label, but they can differ.

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose to encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

<input type="checkbox"/>	Name	Priority	Scope	Created by	Last modified
<input type="checkbox"/>	Public	0 - lowest	File, Email, Meetings	Tony Redmond	20 Feb 2023 14:23:43
<input checked="" type="checkbox"/>	No Encryption	1	File, Email	Tony Redmond	6 Feb 2023 16:56:52
<input type="checkbox"/>	Non-business use		Group	Tony Redmond	7 Jun 2021 16:26:44
<input type="checkbox"/>	Partner-Accessible Content			Tony Redmond	15 Feb 2023 10:56:28
<input type="checkbox"/>	General Access		Group	Tony Redmond	29 Nov 2023 08:44:55
<input type="checkbox"/>	Internal			Tony Redmond	12 May 2023 16:03:52
<input type="checkbox"/>	Internal Meeting		Meetings	Tony Redmond	12 May 2023 16:33:46
<input type="checkbox"/>	Office 365 Book Source			Tony Redmond	12 May 2023 16:26:00
<input type="checkbox"/>	Guest Access		Group	Tony Redmond	6 Dec 2023 12:39:24
<input type="checkbox"/>	Confidential			Tony Redmond	13 Jun 2023 14:19:42

Figure 19-2: Sensitivity labels listed in the Microsoft Purview Compliance portal

You also see the choices available in the ellipsis menu to reorder labels or to create a sublabel. When you move a label up in the order, its level of sensitivity decreases. For instance, the Public label, which is at the top of the list, is intended as a label for less sensitive information than the Confidential label further down the list. Conversely, if you move a label down, Office applications regard the label as being more sensitive. The compliance portal automatically assigns the highest level of priority to new labels, and it is important to adjust the priority of a new label to a more appropriate level afterward. Doing so through the portal is slower than running the *Set-Label* cmdlet in the compliance module to assign a priority to a sensitivity label. For example:

```
Set-Label -Identity "Internal" -Priority 5
```

Using the *Set-Label* cmdlet to change priority affects the priority previously assigned to other labels. In this example, the command moves the *Internal* label to priority 5. If the *Internal* label previously had a higher priority (which it will if the label is newly created), the label previously at priority 5 will move to priority 6. On the other hand, if you increase the priority of the *Internal* label, the label previously holding that position moves to priority 4.

Note: If you use different labels for container management and information protection, the position of the container management labels in the priority order affects the signaling of label mismatches as users upload documents. See the later discussion on this topic.

Sublabels

Sensitivity labels used for information protection can have sublabels. This means that you have a parent or group label that isn't used for labeling. Instead, the parent label is a container that serves as a logical collection of linked labels (child labels), each of which can have different marking and encryption settings. Although main labels appear in applications, you can't assign them to content. Instead, users can select one of the sublabels linked to the parent label, which is then assigned to the content.

To create sublabels in the Purview compliance portal, you first create the parent labels and then select the parent label to create the sublabels. The portal doesn't support linking a label to a parent label or unlinking a label from a parent label. However, both operations can be performed using PowerShell. See the PowerShell section later.

Labels Outside a Policy

Sensitivity labels become available by publishing the labels in a policy to all or some users in a tenant. The users included in the policy form the target set for the policy. Sometimes users will receive items with a sensitivity label that isn't available to them in the policy published to their account. In this case, because policies include all label definitions, including those unavailable to the user, the client can display the label, but the user cannot apply the label to items.

Planning for Container Management

If you use sensitivity labels for container management, a separate implementation plan should describe the set of labels for assignments to Teams, Groups, and Sites. Table 19-3 describes an example of what a container label plan might look like. Once again, the plan describes labels from least sensitive to most confidential.

Label Name	Description	Privacy	Guests Allowed	Sharing	Endpoint
General Access	Container for non-sensitive, general-purpose information.	Public	Yes	Anyone	Unrestricted
Guest Access	Container for restricted information.	Private	Yes	Existing guests	Web access
Limited Access	Container for restricted information.	Private	No	Existing guests	Web access
Secret Access	Container for highly confidential material.	Private	No	No external	Block Access

Table 19-3: Planning Sensitivity Labels for Container Management

Some organizations like to include a sensitivity label to mark groups and teams dedicated to non-business use, such as sports or other non-work activities. Such a label would have the same settings as the "General Access" label described above.

Given the more limited set of setting permutations available for container management, it's normally the case that fewer container management labels exist than the set of information protection labels. Restricting the set is good in any case because it makes it easier for container owners to choose and apply the right label.

Rescoping Labels for Container Management

Given that sensitivity labels started with a single scope (files and email), it is possible that an organization has labels used for both information protection and container management and now wishes to separate labels into two distinct sets. The suggested approach is:

1. Create a set of new labels specifically for container management. Make sure that these labels do not have information protection (items) settings. Give names to labels that reflect their use for container management and make sure that the descriptions used are informative and give guidance to container owners about the proper use of each label.
2. Publish the new labels to make them available to container owners. It's best to use a separate label publication policy for the labels used for container management. Optionally, you can choose to force users to assign a label to new containers and choose a label applied by default to new containers.
3. Unpublish the information protection labels that have container management settings. This must happen before you can remove the container management settings.
4. Remove the container management settings from the set of information protection labels. Within a few hours, these labels should no longer be available to assign to new containers. Existing labels and their settings will remain in place in the containers to which they are applied.
5. Republish the information protection labels to make them available to users again. Users can now only apply the labels to items.
6. Map the set of new container management labels to the set currently applied to containers. Some of the mappings will be 1:1, other labels might be able to replace multiple labels, and some new labels might not be used. For example, this mapping might be used:

New container management label	Current information protection label
General access	Public
Guest access	(None)
Limited access	Internal Employee confidential Market sensitive Financial data
Confidential access	Confidential Secret Ultra-confidential

7. Update the containers with new labels as defined by the mapping exercise. This won't take long to do manually if there are only a few containers to update. If not, it's easy to script it with PowerShell (an [example is available from GitHub](#)). The functioning of the containers won't be affected if the new labels have the same settings as the old labels. In some cases, it will be more appropriate to apply a new label to a container. These cases can be handled on an individual basis after the remapping exercise is complete.

As always, it's a good idea to test before you make a change like this in a production environment.

Tracking Label Changes for Containers

Organizations use sensitivity labels to apply policies to containers, but group, site, and team owners can change the label assigned to their containers, which might affect the settings applicable to the container. Microsoft doesn't support locked labels for containers (defined here as labels that group owners cannot change), so if organizations want to stop group owners changing assigned labels, they must implement some mechanism to monitor label changes and respond appropriately. This [article discusses an example of how to approach the problem](#).

In addition, Microsoft 365 doesn't have a way to report the set of containers and their assigned labels, so [here's an article](#) describing how to generate a report with PowerShell.

Creating a New Sensitivity Label

Management of sensitivity labels is through the Information Protection section of the Microsoft Purview Compliance portal. To be able to create and manage sensitivity labels, an account needs permission gained through membership of a compliance role group such as Information Protection ([see this article](#) for details).

Creating a new sensitivity label involves defining settings in these areas:

1. **Naming:** Define the label name that users see in applications. You can also add a tooltip that the apps display when users hover over the label name and an administrative description that can be whatever makes sense for your organization.
2. **Scoping:** Decide whether the label covers both items and containers or restricts its coverage to just one type. Some organizations like to define labels specifically for meetings.
3. **Encryption and marking:** Decide if the label invokes rights management. If yes, you need to decide what rights (permissions) to assign to different users and groups receive. A label used purely for marking purposes doesn't need to use encryption. You can also decide if the label inserts text in the header or footer of documents and messages, or as a watermark (documents only).
4. **Container settings:** If the scope of the label covers containers, it can control several settings for Microsoft 365 Groups, SharePoint Online sites, and Teams. The available settings include privacy, guest access, external sharing capability, and access from unmanaged devices. Settings inherited from sensitivity labels take precedence over tenant defaults.
5. **Auto-labeling:** Office apps can automatically apply a default label to emails and documents if their content matches a sensitive information type (like a credit card number) or classifier (like a resume).
6. **Endpoint data loss prevention:** Microsoft Endpoint Manager app protection policies check files to ensure that users do not move the files to unauthorized devices or storage. The definition of a managed device is one known to Entra ID through Intune. If a device isn't known to Entra ID, it is unmanaged and therefore liable for restriction if dictated by the label.

After going through the steps, you can review and change settings before finally saving the new label. In the following example, we create a new sensitivity label called "Employee Restricted" that protects (encrypts) and applies markings to items. To finish up, we create a label policy to publish the new label so that it shows up in applications for assignment to items by users.

Naming

As shown in Figure 19-3, creation of a new label starts with the population of four label properties:

- **Name:** The name must be unique. Internally, Microsoft Purview also creates an immutable GUID for internal use.
- **Display name:** Clients display this value to users. Unlike the label name, you can update the display name later by editing the label in the Microsoft Purview Compliance portal or with the *Set-Label* PowerShell cmdlet.
- **Description for users:** Clients display this text to users in a tooltip to help them understand how to use the label. Apps like Word display the information when a user hovers over a label in the list shown by the Sensitivity button.
- **Description for admins:** Users never see this text. It is for administrative purposes and intended to hold notes about the use and history of the label. Although it is mandatory to enter values for the other properties, you do not have to enter anything here.
- **Label color:** Optionally, you can select a color for the label. Organizations sometimes use colors to highlight the level of sensitivity for a label.

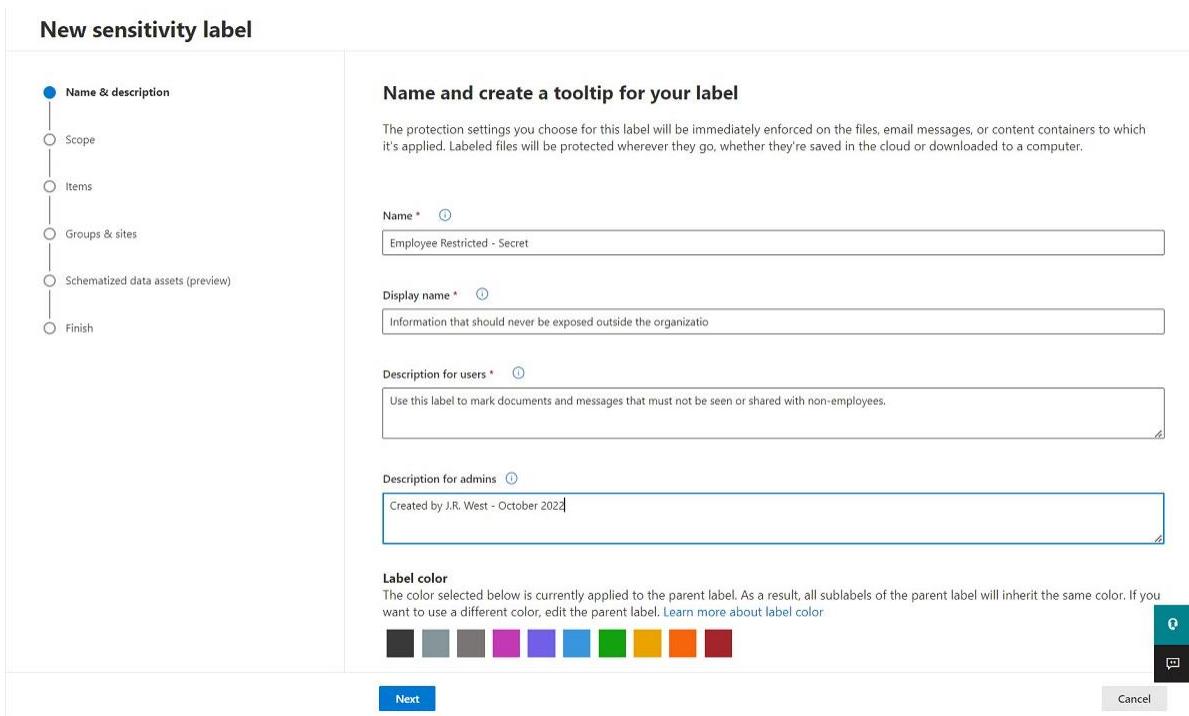


Figure 19-3: Providing display details for a new sensitivity label

Label Scope

As explained earlier, sensitivity labels have a scope that defines their use. In this instance, the label is available for both items and containers. To make things simple, we'll configure the scope for this label for just Items. Figure 19-4 shows that this label covers both Items and Groups and sites, so we'll uncheck the second box to reduce its scope to the desired level.

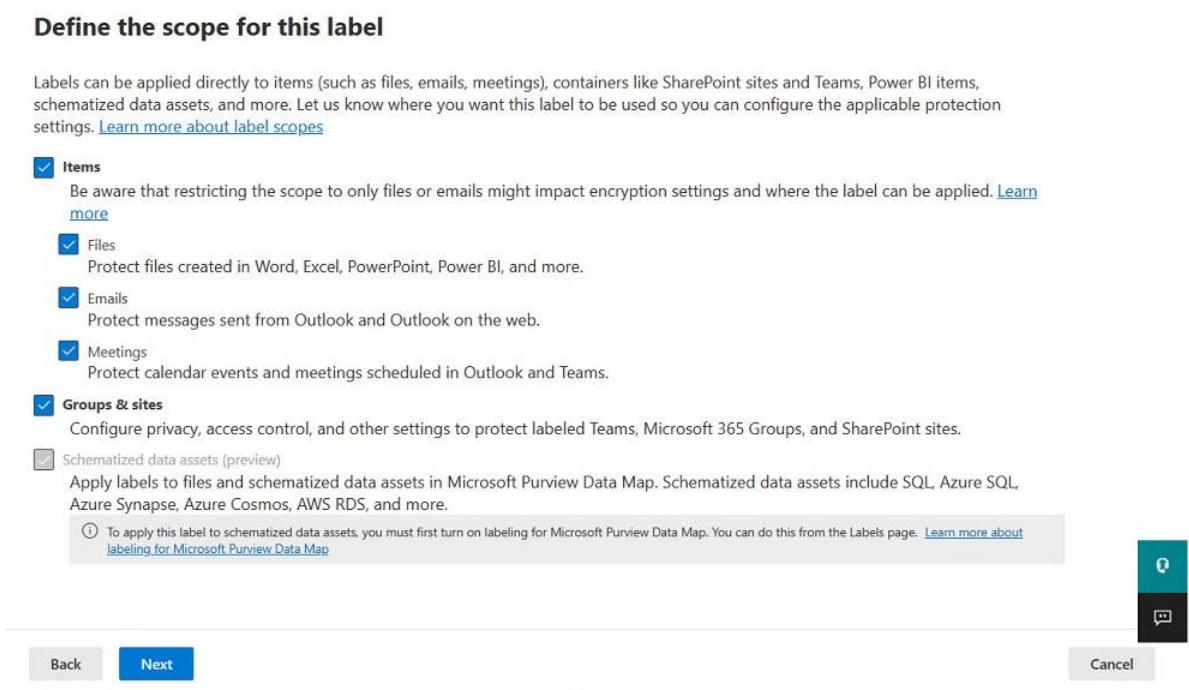


Figure 19-4: Setting the scope for a new sensitivity label

Under items, you can select:

- **Emails:** Labels are only available to Outlook clients.

- **Files:** Natively-supported labels are available for assignment to documents in Word, PowerPoint, and Excel (Online, subscription, and mobile). Apart from labels with user-defined permissions or which use DKE, labels are also assignable to PDFs:
 - Using the SharePoint Online and OneDrive for Business browser interfaces. This option requires that the *EnableSensitivityLabelforPDF* setting in the SharePoint tenant configuration is True:

```
Set-SPTenant -EnableSensitivityLabelforPDF $True
```
 - By the Adobe Acrobat paid-for products
 - Exported from Word, Excel, or PowerPoint
 - Applied to PDFs stored outside SharePoint Online and OneDrive for Business by the AIP extension for Windows Explorer.
- **Meetings:** Labels are available for meetings created in Outlook and OWA and the Teams desktop and browser clients. Because meetings include elements of email (meeting notifications and responses) and files (attachments), if you select this option, you must also enable the label for Emails and Files.
- **Groups and Sites:** If configured with these settings, the label can apply container management settings to Teams, Groups, and Sites. See the later section for more information.

If you [enable the schematized data assets feature](#), you can amend the scope of the label to support its application to items and Microsoft Purview schematized data assets, including SQL, Azure SQL, Azure Synapse, Azure Cosmos, and AWS RDS.

Because we've chosen to limit the scope of the label to items, the next step is to configure the protection and marking settings. The choices are:

- **Control Access:** Use rights management encryption to limit access to content. In most cases, sensitivity labels apply encryption, but it is useful to make a label available to allow users to remove encryption from encrypted items.
- **Apply Content Marking:** Apply custom headers, footers, and watermarks. Be aware that if a label applies a custom header or footer to a document, it overwrites any header or footer information already present. This is a replacement operation and the text applied by the label doesn't merge with whatever text might already be present.
- **Protect Teams meetings and chats:** This option is only available when the organization has Teams Premium licenses.

You don't need to choose any of these options. If you don't, the label becomes a visual indicator that users can assign to items.

Encryption and Permissions

The encryption settings allow you to configure the type of protection to apply to items or to remove encryption from items. Labels that remove encryption can only be applied by people who have sufficient usage rights (Export or Full Control) for the label currently applied to an item or be the owner of the message or document. Super-users (see later) can also remove encryption from items.

When a label applies encryption (Figure 19-5), rights management defines the protection given to items. The settings are:

- **Assign Permissions now or let users decide:** The heart of rights management is the permissions given to recipients of an item. The author grants permissions to individual accounts, groups, or collections of people (such as every authenticated user in a tenant). For sensitivity labels, administrators can decide to create a set of predefined permissions inherited by labeled items, or they can allow users to assign custom permissions when they apply a label to messages or documents. If

you assign predefined permissions, you must add permissions for at least one user or group. The Office browser apps do not support the assignment of user-defined permissions.

- **User access to content expires:** If never, the user can continue to access labeled content without hindrance. In some cases, like a draft for a plan, you will define an expiry date. In others, you know that content is only valuable for a certain period, so you can set access to expire a specific number of days after a user applies the label to an item.
- **Allow offline access:** When a label allows offline access, the use license obtained by the user and downloaded along with the content is used to access the content. The use license is a certificate that attests to the user's right to access content together with the encryption key used to decrypt the content. The normal validity of a use license is 30 days (you can choose any period between 1 and 100 days), during which the user does not need to reauthenticate to prove their access. You can block offline access completely (for very sensitive information) or allow access for limited periods when offline. You can further limit access by requiring the application to check with the rights management service after a set period to ensure that access is still valid and not revoked. Checking is only possible when the client is online. When checking, group membership is re-evaluated to ensure that someone who gains access through group membership is still a member.

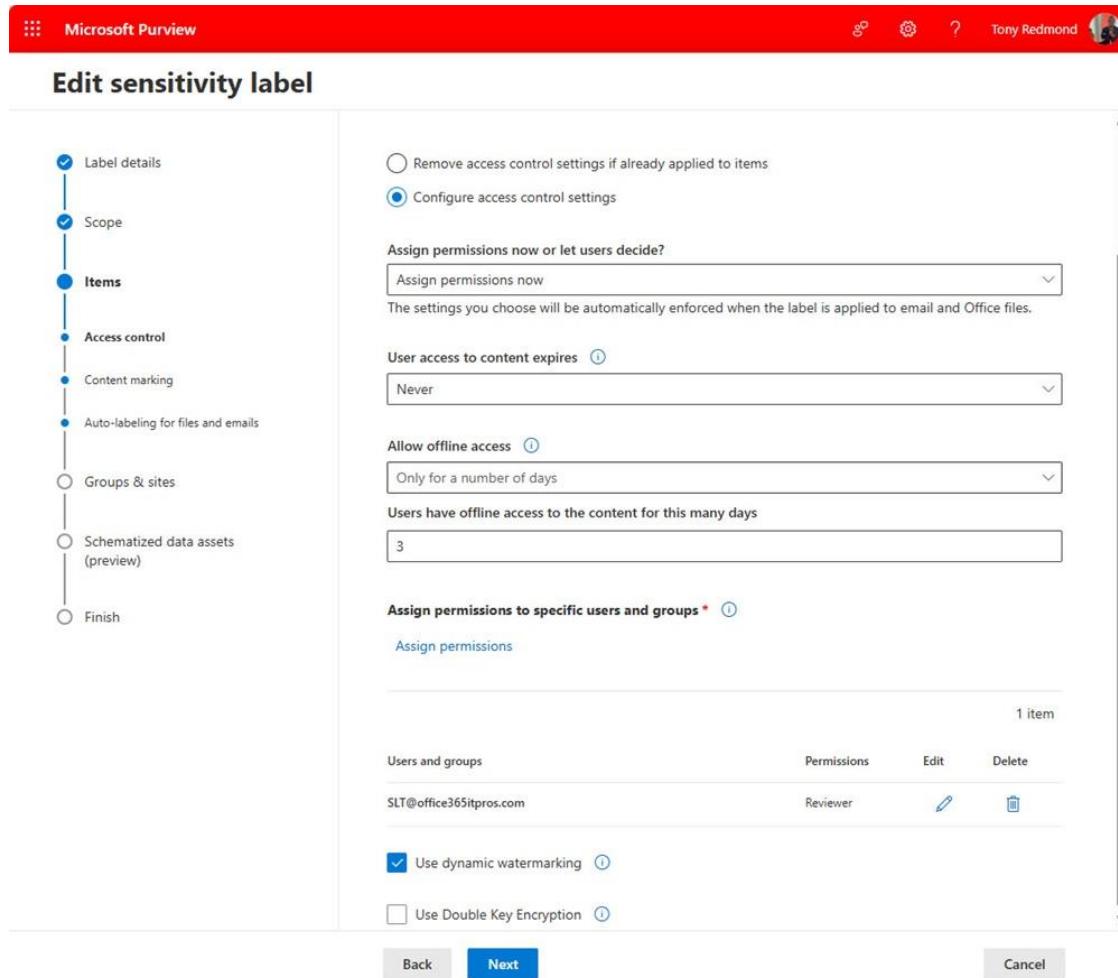


Figure 19-5: Configuring encryption settings for a sensitivity label

If you decide the label should have predefined permissions, assign them in the **Assign permissions to specific groups** section of the form. Click the *Assign permissions* link to display the form (Figure 19-6) and define the identities (such as users or a special identity like all authenticated users) and the rights (permissions) assigned to each identity. Be aware that:

- Purview Information Protection does not validate the email addresses entered when assigning rights. Be careful to use the correct addresses.
- Assigned rights do not expire. Even if someone leaves the organization and their email address is no longer valid, the assigned right remains in the label.
- Assigning rights to a domain, especially a consumer email domain like outlook.com, is seldom a good idea unless you explicitly want a form of protection that allows access to hundreds of millions of people. It's much better to assign rights to individual consumer email addresses.

Because assignments do not expire, it's a good idea to review the assignments periodically. Don't rush to remove an assignment without understanding that the consequence is that the rights assigned to access protected content are no longer available to the assignee.

It is common practice to grant the Viewer permission to **All users and groups in the organization** as a catch-all to ensure that any account belonging to the tenant can read files. This identity is especially true for sensitivity labels intended to protect information that circulates widely within a tenant such as confidential messages sent to large distribution lists or documents intended for internal consumption posted to intranet sites. The other types of permission are:

- **Any authenticated users:** Grants access to anyone with an authenticated identity. The item will be accessible to anyone who signs into a Microsoft 365 tenant or who has a Microsoft Services account. Depending on the federation configuration for the tenant, the definition of an authenticated user might be even wider, including users who authenticate using a one-time passcode. However, due to the authentication mechanism they use, these users can only access protected email. Because of the wide degree of access granted through this permission, it is unwise to include it in sensitivity labels designed to protect very confidential information.
- **Users or groups:** Used to restrict access to specific users or groups in the tenant. Use this option to assign specific rights to people who need it to interact with the content. For example, if you want a set of people to have full control over documents, assign the Co-author or Co-owner permissions to a distribution list or Microsoft 365 group (this can be a dynamic group) containing these people. It's always easier to use a distribution list or group than to specify permissions for individual users. The difference between the Co-author and Co-owner permissions is that an owner can remove or change encryption applied by someone else whereas an author cannot. Be careful not to assign broad rights to large groups because this can lead to Copilot unexpectedly being able to access and use confidential information.
- **Add all users and groups in your organization:** Some organizations include co-author rights for all tenant users in all labels except those used to protect the most sensitive information. The logic for this approach is that it ensures that documents created by someone who leaves the organization are available to other workers without the need for an administrator to intervene. Special arrangements, such as administrator-invoked decryption, might be necessary to unprotect highly sensitive documents authored by someone who leaves the organization. Be aware that granting the EXTRACT and VIEW rights to all users and groups means that AI tools like Microsoft 365 Copilot can access and reuse content protected by a label in the responses generated for user prompts.
- **Specific email address or domains:** Grants access to specific people outside your tenant (by email address) or complete domains. Use this option when you need to collaborate with protected content with people outside your tenant. For example, if you want to share protected information with Microsoft, add Microsoft.com as the domain and assign an appropriate permission (like Viewer). You cannot grant rights to the guest accounts used by applications such as Teams and SharePoint Online. Instead, you must add explicit assignments using the email addresses of the accounts (or grant access to Microsoft 365 Groups containing the accounts). External users must authenticate before they can access the content. In practice this means:
 - Using an Entra ID account (probably belonging to another tenant).

- Using a Microsoft Services account, like Outlook.com.
- Using an account from a federated directory (Gmail.com or Yahoo.com). To access protected Office documents and PDFs, these accounts must create a Microsoft Services account using their email address. If they don't, they can access protected emails using a one-time password but won't be able to authenticate to open protected documents.
- Another email or identity service. These accounts need a Microsoft Service account using their email address.
- On-premises directories. These accounts need to register for [RMS for Individuals](#) using their corporate email address. RMS for Individuals is a free service for users who need to open files encrypted by Microsoft Information Protection.

X

Assign permissions

Only the users or groups you choose will be assigned permissions to use the content that has this label applied. You can choose from existing permissions (such as Co-Owner, Co-Author, and Reviewer) or customize them to meet your needs.

- + Add all users and groups in your organization
- + Add any authenticated users ⓘ
- + Add users or groups
- + Add specific email addresses or domains ⓘ

Permissions assigned to

.onmicrosoft.com Delete

Choose permissions

Viewer
VIEW,VIEWRIGHTSDATA,OBJMODEL

Save

Cancel



Figure 19-6: Assigning predefined permissions for a sensitivity label

Pay special attention to permissions for external users defined for the sensitivity labels used to protect meetings. If a meeting participant doesn't have the right to open the meeting invitation, they cannot access its contents. For this reason, consider assigning the Viewer right to *Any authenticated users* in labels used to protect meetings that are not ultra-confidential. If someone forwards a protected meeting invitation to someone else, they might not be able to access the content if the rights specified in the label do not include an entry matching their email address (or domain). One advantage gained is that if people forward meeting invitations without permission outside the organization, the external recipients won't have access to the meeting content.

Meetings protected with sensitivity labels can include Loop components. Loop does not support sensitivity labels and the default permissions assigned allow tenant members to edit Loop components.

Labels Without Encryption: Some labels are intended to be solely visual markers and don't apply encryption. If you create labels like this, make sure to configure the label to remove any existing encryption applied by a previous label. If you don't, a label that seems to be purely visual might continue to protect content, which isn't what you want.

Permissions and Usage Rights

Sets of individual usage rights form the permissions assigned by sensitivity labels to users. The usage rights are:

- View content.
- View rights.
- Edit content.
- Save.
- Print.
- Copy (extract) content. This right is particularly important when using Microsoft 365 Copilot. Users must be granted both the copy (extract) and view rights for documents protected by sensitivity labels before Copilot can access and use content from those documents in its responses.
- Reply.
- Reply all.
- Forward.
- Edit rights.
- Export content.
- Allow macros.
- Full control (note that the Full control or Export content rights are the only permissions that allow someone to remove existing encryption from a labeled item).

To make usage rights easier to manage and assign, information protection defines permission sets such as Co-Author, Reviewer, and Viewer. Each permission set consists of a set of usage rights. Assigning predefined permissions to someone is a convenient way of giving them all the usage rights defined in the permissions. If none of the predefined permissions meet your needs, you can choose to define custom permissions made up of appropriate usage rights.

User-Defined Permissions

If you don't assign preset permissions to a label, you can allow users to control the permissions assigned when they apply the label to an item. You can enable protection for Outlook or the other Office apps, or both (shown in Figure 19-7):

- **Outlook:** the permissions on the message can be set to either *Do Not Forward* or *Encrypt Only*. Unprotected Office attachments inherit the same protection from the message. Files that have protection (through another label) before being attached to a message keep the protection assigned by that label, even if the label assigned to the email is more sensitive than one assigned to an attachment.
- **Word, PowerPoint, and Excel:** the app prompts authors to define the permissions (like Viewer, Reviewer, or Co-Author) they wish other users to receive.

If you don't set the Outlook checkbox, the label doesn't appear in the set shown in Outlook clients. The same is true for Word, Excel, and PowerPoint if you don't select this setting.

User-assigned permissions is a premium feature limited to the Office apps on Windows and Mac. New documents with labels with user-defined permissions are automatically processed by SharePoint Online (the process takes a few minutes to resolve permissions before full functionality such as autosave and collaborative editing is available). SharePoint processes existing documents with labels with user-defined permissions the next time users edit these documents. Edits for existing documents must be performed using the Office desktop apps because the online apps cannot access the documents until after SharePoint processes their permissions.

Access control

Use encryption capabilities to control who can access labeled items. Depending on the scope you specified, items can include emails, Office, Fabric and Power BI files, and meeting invites. [Learn more about access control settings](#)

- Remove access control settings if already applied to items
 Configure access control settings

Assign permissions now or let users decide?

Let users assign permissions when they apply the label

(i) The labeling behavior for these settings varies depending on which operating system platform is used to apply the label. [Learn more](#)

- In Outlook, enforce one of the following restrictions

Do Not Forward (i)

Encrypt-Only (i)

- In Word, PowerPoint, and Excel, prompt users to specify permissions (i)

- Use Double Key Encryption (i)



Figure 19-7: Defining user assigned permissions for a sensitivity label

Encryption Applied by OWA and Outlook Mobile

Outlook desktop clients encrypt messages before submitting emails to the Exchange Online transport service for onward processing. Other clients do not include the necessary code to protect messages. These clients stamp outbound messages with the metadata for a label and rely on the transport service to apply appropriate protection. You know if the transport service applies protection to a message if the copy of the message in the Sent Items folder has a label but is unencrypted.

OWA can apply the OME Do Not Forward and Encrypt Only protection to outbound messages before submission to the Exchange transport service, but OWA cannot encrypt messages for sensitivity labels using either preassigned or user-defined permissions. Outlook Mobile always submits messages to Exchange Online for encryption.

Document Owners

When someone applies a sensitivity label with encryption to a message or document, they become the owner or issuer of rights for that content. The owner always has the right to access content, even if the policy sets an expiry date. Likewise, the owner can always access content offline.

Content Marking

If you decide that a sensitivity label should apply content marking to items, you can configure settings (Figure 19-8) to control the visual indicators inserted by applications after a user applies a label. Word, Excel, and PowerPoint support headers, footers, and watermarks and insert the markings as soon as a label is assigned to a file, while Outlook only supports headers and footers and inserts the text when it saves a message or meeting request.

Headers and footers can be up to 1024 characters, except for Excel, which limits these markings to 255 characters. Watermarks can be up to 255 characters. Footers applied by labels to HTML-format emails appear at the bottom of the most recent reply in the email thread. Footers for rich text format emails appear at the end of the email thread.

Content marking

Add custom headers, footers, and watermarks to content that has this label applied. [Learn more about content marking](#)

ⓘ All content marking will be applied to documents but only headers and footers will be applied to email messages.

Content marking

The screenshot shows a configuration interface for content marking. At the top, there's a note about applying custom headers, footers, and watermarks to content with the current label. Below this is a section titled "Content marking" with a toggle switch that is turned on. Underneath the switch are three checkboxes:

- Add a watermark (disabled)
- Add a header (disabled)
- Add a footer
 - Customize text
 - Employee Restricted

At the bottom of the screen are three buttons: "Back", "Next", and "Cancel".

Figure 19-8: Configuring content marking settings for a sensitivity label

Dynamic Watermarking

Content marking inserts static strings that users can change or remove. Although the values inserted can act as a visual deterrent to prevent people from inadvertently sharing confidential information, it's obvious that they have some limitations. Dynamic watermarking is a feature that inserts the user's email address as a watermark when people view or edit an Office document (other applications do not currently support dynamic watermarking). The option to enable dynamic watermarking is visible in Figure 19-5. It can only be used for sensitivity labels with administrator defined permissions. Labels with user defined permissions are unsupported.

Settings for Teams Meetings and Chat

Teams Premium allows users to protect Teams meetings with a sensitivity label. Users can select and assign a label when they create a meeting, or a [meeting template](#) used to create a meeting can enforce a specific label. Figure 19-9 shows the settings to control different aspects of Teams meetings.

All the controls imposed by a sensitivity label are applicable through other methods, either for individual events when meeting organizers set meeting options, or more generally through Teams meeting policies. See the Teams chapter for more information about the different controls.

When a sensitivity label includes Teams settings, Purview displays the label as available for "Teamwork."

Settings for Teams meetings and chats

These settings apply to all Teams meetings that have this label applied.

ⓘ If you select a setting below, the options you configure will be enforced when the label is applied to a meeting. Users won't be able to change the setting in Teams. If you don't select a setting, users will be able to select it themselves when creating a Teams meeting.

Control who can bypass the lobby ⓘ
People in my org, trusted orgs, and guests
 People dialing in can bypass the lobby

Control who can present

Control who can record
If selected, you won't be able to record meetings automatically, apply end-to-end encryption, or apply watermarks.
Organizers and presenters

Control whether meetings are recorded automatically
If selected, you won't be able to control who can record, apply end-to-end encryption, or apply watermarks.

Control end-to-end encryption for meeting video and audio ⓘ
If selected, you won't be able to record meetings automatically or control who can record.

Control watermarks ⓘ
If selected, you won't be able to control who can record or record meetings automatically.

Control meeting chat
In-meeting only

Prevent copying chat content to clipboard
Some meeting participants will be blocked from copying messages from the meeting chat. Also, additional steps are needed to prevent copying chat content from meetings created in Teams channels. [Learn more](#)

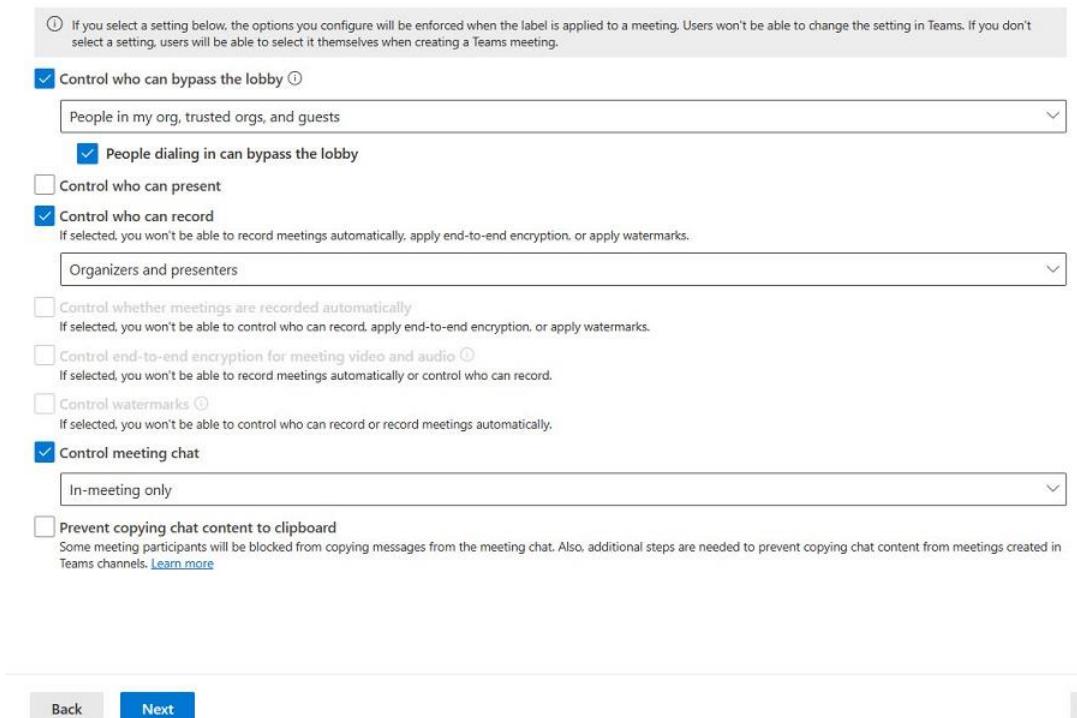


Figure 19-9: Sensitivity label options to control Teams meetings

Performance and Encryption

Microsoft warns that some degradation in performance is possible when accessing protected Word, Excel, and PowerPoint files. This is because users must authenticate with the protection service to establish their right to access the content, after which the app can decrypt the content. These operations are unnecessary for unprotected files. Usually, the slight delay in opening documents is not very noticeable. Large files always take some time to open, so the need to decrypt a large Word document or Excel spreadsheet will add a small amount to the time needed to open these files.

Client-Side Auto-Labeling with Sensitivity Labels

Client applications like the Office applications and OWA use the Microsoft Information Protection SDK to detect sensitive information types or classifiers and apply sensitivity labels automatically when a match is found in a message or document. For example, OWA checks an item's content and applies automatic labeling if matches are found when messages are sent. The check processes the content of the message body (but not header information or the message subject) to decide if a match for the specified sensitive data is present. The other Office applications perform automatic labeling when they save files.

The sensitive information types used for the automatic application of sensitivity labels are those used by other applications such as DLP policies and auto-label policies. Checking for matches uses the same concept of detecting a certain number of occurrences of the data type in content together with meeting a set confidence level that the data type is what it seems before deciding that a match exists (see the DLP chapter for more information).

In Figure 19-10 we see the properties of a sensitivity label with auto-labeling enabled. In this case, clients apply the label when they detect the existence of a single debit card number. Typically, you combine this feature with content marking to apply a header or footer to warn users that sensitive data is present and

perhaps note when the label encrypts content. The *message displayed to user* property is a policy tip displayed in a banner to communicate with users when their items receive labels automatically.

The screenshot shows the 'Auto-labeling for files and emails' configuration interface. At the top, there is a toggle switch followed by a note about encryption performance. Below this, the 'Detect content that matches these conditions' section is expanded, showing a 'Content contains' rule. This rule includes a 'Group name' field set to 'Default' and a 'Group operator' dropdown set to 'Any of these'. Under 'Sensitive info types', a 'Credit Card Number' entry is listed with 'Medium confidence' and an 'Instance count' of '1 to Any'. There are also 'Add' and 'Create group' buttons. A 'When content matches these conditions' section follows, with a dropdown set to 'Automatically apply the label'. Below it, a message states that automatic labeling works differently for items in Office 365 vs. files stored on Windows devices. The 'Display this message to users when the label is applied' section contains the message: 'We detected a credit card number so we protected your email with encryption'. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

Figure 19-10: Setting the auto-labeling properties for a sensitivity label

Several sensitivity labels published in a policy might invoke automatic labeling and match against an item's content. When this happens, Purview applies the label with the highest priority (as ordered in the sensitivity label policy published to the user). The automatic application of sensitivity labels is a premium feature.

Creating Protected Documents with Microsoft 365 Copilot

When a user creates new items based on documents protected by sensitivity labels (for instance, by including a protected document in a prompt), the new item inherits the sensitivity label from the source, including its protection. If the user specifies multiple documents in a prompt, the output file receives the sensitivity label with the highest priority from the items used in the prompt.

Following the creation of an item, users can change the sensitivity label inherited through the Copilot interaction to make sure that the item has the most appropriate label for its intended use.

Configuring Container Management Settings for Sensitivity Labels

Sensitivity labels configured with a scope of "Groups and sites" have additional settings to control the management of containers. We suggest that you separate labels used for container management from those used to protect items. This approach reduces the number of labels displayed to users and makes it easier for them to select the most appropriate label.

The visual marking aspect of container management via sensitivity labels replaces the previous markings set through text-only classifications defined in the Entra ID Groups policy (see the Groups chapter). Sensitivity

labels serve the same purpose as classifications in that users see a visual indicator (like "Secret" or "Confidential") to remind them of the importance or sensitivity of the container. Sensitivity labels have the extra benefit of being able to impose access controls on the containers. You can, for instance, assign a label to a team to stop the team owner from being able to invite guests from outside the tenant to join the team membership. The big advantage of settings applied via sensitivity labels is that the container owners (like team owners) cannot change the settings. Once applied by label, a setting can only be changed if administrators update the label settings.

To make container management even more useful, Microsoft has said that they plan to increase the range of management settings available through sensitivity labels in the future. For instance, a recent setting controls the discoverability of private teams to allow administrators to reveal or hide the existence of these teams when users look for teams to join. Another controls what types of teams can join the membership of shared channels owned by a labelled team.

Outlook desktop, OWA, Teams, and SharePoint Online support container management. If you create or edit groups using these apps, you can apply sensitivity labels to the underlying groups. When an owner applies a label to a container, the app applies the settings inherited from the label and synchronizes the label and its settings to the other workloads to ensure that all apps use the same settings.

Container Labels Don't Affect Content: It's important to realize that sensitivity labels applied to the container level do not affect the individual messages, conversations, and files stored in these containers. You can certainly assign sensitivity labels to individual files stored in document libraries, but these assignments are independent of anything applied to the container.

Five settings for container controls are available, presented on three screens. You can configure any or all these settings.

Define privacy and external user access settings

Control the level of access that internal and external users will have to labeled teams and Microsoft 365 Groups.

Privacy

These options apply to all Microsoft 365 Groups and teams that have this label applied. When applied, these settings will replace any existing privacy settings for the team or group. If the label is removed, users can change it again.

- Public. Anyone in your organization can access the group or team (including content) and add members.
- Private. Only team owners and members can access the group or team, and only owners can add members.
- None. Team and group members can set the privacy settings themselves.

External user access

Let Microsoft 365 Group owners add people outside your organization to the group as guests. [Learn about guest access](#)

[Back](#) [Next](#) [Cancel](#)

Figure 19-11: Sensitivity label container management settings for privacy and user access

Privacy and external user access settings (Figure 19-11):

- *Privacy* controls if the group is *Public* (anyone can join) or *Private* (members must be invited to join). The setting can also be set to *None*, which means that the group owner decides which level of access to apply to the group.
- *External user access* controls if the group membership can include guest users. If you block guest users for the group, the action updates the policy for that group to set the *AllowedToAddGuests*

setting to `$False`. Blocking external access does not remove existing guests from the group membership; it only blocks the addition of new guests.

Define external sharing and conditional access settings

Control who can share SharePoint content with people outside your organization and decide whether users can access labeled sites from unmanaged devices.

Control external sharing from labeled SharePoint sites
When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site.

Content can be shared with

Anyone ⓘ
Users can share files and folders using links that don't require sign-in.

New and existing guests ⓘ
Guests must sign in or provide a verification code.

Existing guests ⓘ
Only guests in your organization's directory.

Only people in your organization
No external sharing allowed.

Use Microsoft Entra Conditional Access to protect labeled SharePoint sites
You can either control the level of access users have from unmanaged devices or select an existing authentication context to enforce restrictions.

Determine whether users can access SharePoint sites from unmanaged devices (which are devices that aren't [Microsoft Entra hybrid joined](#) or enrolled in Intune).
(ⓘ For this setting to work, you must also configure the SharePoint feature that blocks or limits access to SharePoint files from unmanaged devices. [Learn more](#))

Allow full access from desktop apps, mobile apps, and the web

Allow limited, web-only access ⓘ

Block access ⓘ

Choose an existing authentication context. Each context has an Microsoft Entra Conditional Access policy applied to enforce restrictions. [Learn more about authentication context](#)
Require MFA - Access to information is only possible when accounts use MFA

Back

Next

Cancel

Figure 19-12: Configuring external sharing and device access settings for container management

External sharing and conditional access settings (Figure 19-12): These settings control access to content in SharePoint Online team sites. Microsoft requires that any account using sensitivity labels to manage settings for group-connected sites has a premium license. Two settings are available:

- **Control external sharing from labeled SharePoint sites:** The capability to share documents with external users from a site is controlled by a default setting for the tenant which can be overridden at the site level, which is what happens when a label is applied to a site. The available options are listed below (the relevant value used to set external sharing capability for a site by running the `Set-SPOSite` cmdlet is in parenthesis).
 - **Anyone** (`ExternalUserAndGuestSharing`): Sharing is allowed with all external users, and documents can be shared using anonymous access links (Anyone links).
 - **New and existing guests** (`ExternalUserSharingOnly`): Sharing is allowed with new external users, who must accept a sharing invitation and go through an authentication process to create a guest account.

- **Existing guests** (`ExistingExternalUserSharingOnly`): Sharing is only allowed with the guest users already in an organization's directory.
- **Only people in your organization** (`Disabled`): No sharing with external users is allowed.
- *Use Microsoft Entra Conditional Access to protect labeled SharePoint sites:* Limiting access to unmanaged devices depends on conditional access policies. Policy evaluation during the authentication process identifies the managed state of a device (by the organization or managed by the user). If the device is unmanaged, SharePoint Online can apply the restriction set in the label. See [this page for directions](#) on how to create the necessary conditional access policy.

Remember that the external sharing capability assigned to a site cannot be less restrictive than allowed by the tenant-level setting. Microsoft Purview does not check the tenant-level setting when adding sensitivity labels, so someone can create a label that allows a less restrictive external sharing capability than allowed by the tenant. For instance, if the tenant bars *Anyone* sharing links, a label should not select this level. If a label has an invalid sharing capability, SharePoint Online ignores it when it reads settings from the label.

Label Synchronization with SharePoint Online: SharePoint caches the container settings in sensitivity labels to improve performance. This means that changes to label settings that affect the operation of a site, such as an update to the external sharing capability will not become effective for at least 24 hours after the update. Settings imposed by new sensitivity labels apply 15 minutes or so after the publication of a new label to SharePoint.

The last screen controls Teams discoverability settings. If configured, private teams with the label can be marked as discoverable or non-discoverable. If the former, users can see the private teams with the label when they browse the *Join a team* gallery. Further settings control the types of teams that can be invited to join shared channels. For more information, see the Managing Teams chapter.

Conditional Access and Authentication Context

Highly confidential SharePoint sites often need special attention to ensure that connections are secure. An authentication context is a way of marking resources like SharePoint sites as needing special processing by conditional access policies. A sensitivity label can be associated with an authentication context in its external sharing settings. When such a link exists, Entra ID can invoke conditional access policies that include the authentication context whenever someone attempts to access SharePoint sites stamped with the label. For example, if a conditional access policy with an authentication context requires connections to use multi-factor authentication, attempts to connect to sites with labels linked to the authentication context will fail unless authenticated with MFA. Information about the selected authentication context is in the `ProtectionLevel` value in the `LabelActions` setting of the label. Using authentication context with SharePoint Online sites requires the Syntex - SharePoint advanced management license.

Coordinating Label Updates Across Apps

A change made to container settings in one app might have unforeseen consequences for another. For example, an Exchange administrator might apply a label that prohibits guest users to a group with OWA. SharePoint Online and Teams synchronize the update for the assigned label, and it becomes active for the site and team. While the newly assigned label won't stop existing guests from accessing the site or team, it will prevent site and team owners from adding new guests, which could come as a surprise to them. For this reason, it's wise to update group owners before applying a more restrictive label to their group.

Publishing Sensitivity Labels

Before sensitivity labels show up in applications and users can apply the labels to content or containers, a label policy must publish the labels. A label policy consists of:

- One or more labels to publish to the policy audience.

- A target audience. The default audience is everyone in the tenant. You can specify an audience by selecting Microsoft 365 Groups, security groups, distribution lists, or individual users. The requirement is that the objects must be mail-enabled, which excludes some security groups. You can't use dynamic distribution lists because the membership of these groups are unknown to Entra ID. Note that sensitivity label policies publish labels to people while retention label policies publish labels to storage locations like sites and mailboxes.
- Settings to define whether one of the labels in the policy is mandatory and applied to emails and Office documents and if users must give a justification if they remove a label or replace a label with a lower classification. A setting is also available to define a custom help page for users to consult to learn about the proper use of sensitivity labels within the organization. Label use settings don't apply to labels created solely for container management.

Clients that support sensitivity labels learn about new labels or changes to existing labels from the underlying workload. The time required for a client to acquire details about sensitivity labels vary, but you should anticipate that several hours are necessary. It all depends on when the client refreshes its cache of label information.

Select Labels and Target Audiences

When you define a new sensitivity label, Purview offers the choice to publish the label to users. You then have the option to add the new label to an existing sensitivity label policy or to create a new sensitivity label policy. Otherwise, you can create a sensitivity label policy at any time by selecting a sensitivity label from the list and clicking **Publish label**. The policy publication wizard starts with the selected label already added. You can add other labels to the policy with the **Edit** link. Otherwise, you can create a new sensitivity label policy and add the set of labels you want to publish (Figure 19-13).

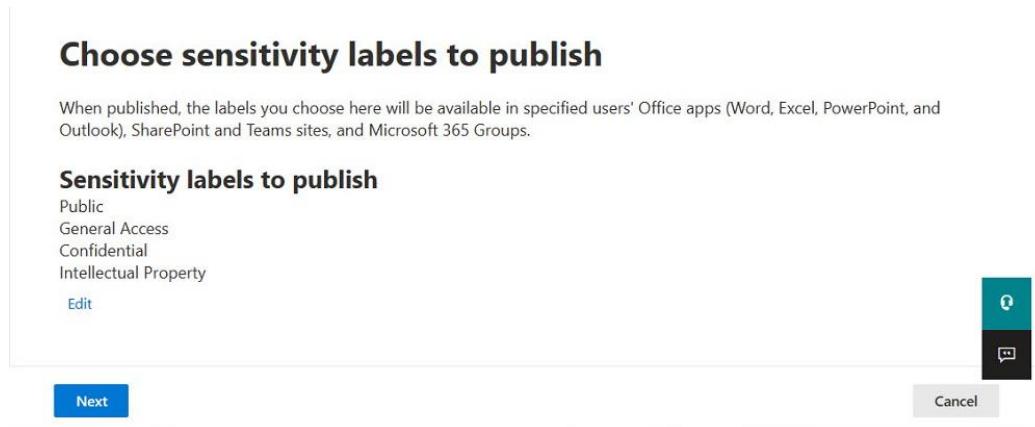


Figure 19-13: Beginning the publication process for a set of labels

The next step is to select the target audience who will be able to use the labels published in the policy. You can choose to target the labels at one or more administrative units (a feature requiring Office 365 E5 licenses), or you can select specific users and groups. One immediate advantage of using administrative units is that users see the labels when an administrator adds their account to one of the administrative units, including dynamic administrative units. Another is that administrative units support [scoped management](#).

In Figure 19-14, all users and groups receive the policy, which is the norm for labels in general use across the tenant. If you want to limit publication to specific users or groups, click **Choose users or groups**. You can select individual users, Microsoft 365 Groups, or distribution lists. Members of the groups keep access to the labels defined in the policy for as long as they are members. New members added to groups benefit from permissions granted in labels when they join.

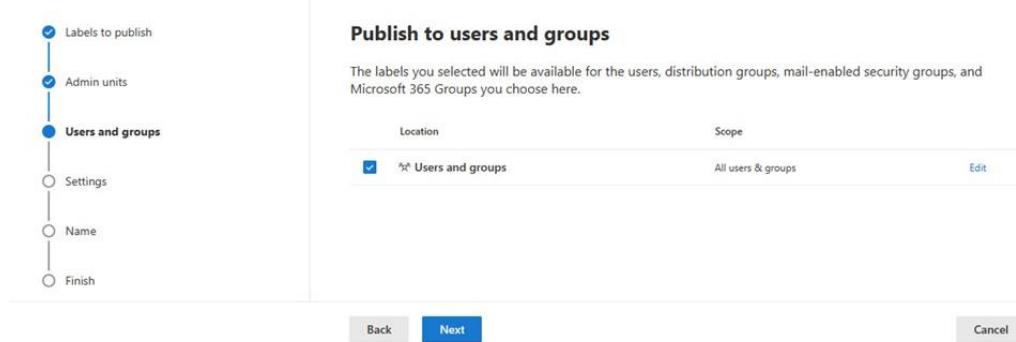


Figure 19-14: Specifying the target audience for the sensitivity policy label

When you define a target audience for a policy, make sure that the users in that audience have the necessary rights to access any encrypted content protected by the labels included in the policy. For policies used to publish container management labels, the target users should be the accounts allowed to create new groups. In some tenants, everyone can create new groups; other organizations restrict group creation by policy to the members of a specific group. See the section about the Groups creation policy in the Groups chapter for more information.

Excluding Mailboxes in a Sensitivity Label Policy

You might notice that the GUI to create sensitivity label policies allows administrators to select All or specific groups as the target (Figure 19-14). All means every user mailbox in the tenant: the Microsoft Purview Compliance portal doesn't support the exclusion of specific users when a policy uses the special *All* destination. Fortunately, this is possible with PowerShell. For example, this command excludes the mailboxes of Terry Hegarty and Kim Akers from receiving the labels published in the specified policy:

```
Set-LabelPolicy -Identity "General Sensitivity Policy" -AddExchangeLocationException
"Terr.y.Hegarty@Office365itpros.com", "Kim.Akers@office365itpros.com"

Get-LabelPolicy -Identity "General Sensitivity Policy" | Select-Object ExchangeLocationException
ExchangeLocationException
-----
{Kim Akers, Terry Hegarty}
```

Adding a mailbox to a label publishing policy in this manner does not overwrite the set of excluded mailboxes. To remove an excluded mailbox, run *Set-LabelPolicy* and pass the mailbox name in the *RemoveExchangeLocationException* parameter.

```
Set-LabelPolicy -Identity "General Sensitivity Policy" -RemoveExchangeLocationException Kim.Akers
```

Running the cmdlet to add more than a few mailboxes can become tiresome. In these circumstances, it's better to find the set of mailboxes using *Get-ExoMailbox* or another method and pipe the set of mailboxes to *Set-LabelPolicy*. For example, this code extracts the mailbox members of a distribution list into an array and uses the array to add policy exclusions:

```
[array]$Members = Get-DistributionGroupMember -Identity "Planner Gurus" | Where-Object
{$_.RecipientTypeDetails -eq "UserMailbox"} | Select -ExpandProperty PrimarySmtpAddress
Set-LabelPolicy -Identity "General Sensitivity Policy" -AddExchangeLocationException $Members
```

Publication Policy Settings

Settings in label publication policies allow the selection of a default label for assignment to new messages and documents. In Figure 19-15, we require users to apply a label to their emails and documents. Default labels only work with clients that support information protection during content creation, such as the Office apps. By

comparison, if someone sends an email when connected to Exchange Online via IMAP4 with the Thunderbird client, nothing will happen.

Depending on what types of sensitivity labels a label publishing policy includes, settings are available to control if users must apply labels to:

- Documents.
- Emails (can be the same as for Documents). An important point for emails is to decide if emails should inherit higher-priority labels from attachments. The default is off, meaning that attachments inherit the label applied to the email unless they have a higher-priority label. If set on, Purview checks attachments to determine the highest-priority label that's present for an attachment and applies that label to the email if it has a higher priority than the label assigned to the email. Unlabeled emails receive the highest-priority label assigned to an attachment.
- Meetings.
- Containers (groups, teams, and sites – if the policy includes these labels).
- Power BI content.

For each content type, you can define a default label to apply. Be aware that when you specify a label to be the default for a type of content, you create a dependency on that label. For instance, you cannot remove a content type from a label if it is the default for that type.

To make the different types of labels easier to manage, it's often best to have separate sensitivity label policies for the labels to handle the different types of content.

You can control whether users must provide a free-text justification when they change the assigned label to another label with a lower classification. The reason provided for a label change is viewable in the activity explorer.

The policy settings for default label assignments are not retrospective, so unlabeled items remain in this state until users or auto-label policies assign them labels. It's easier to deal with unlabeled groups because it's possible to search for unlabeled groups with PowerShell and then assign a suitable label to those groups.

To aid in driving user awareness about information protection, the *Provide users with a link to a custom help page* setting allows organizations to define a web page for users to view if they want added information about how to use sensitivity labels to mark content.

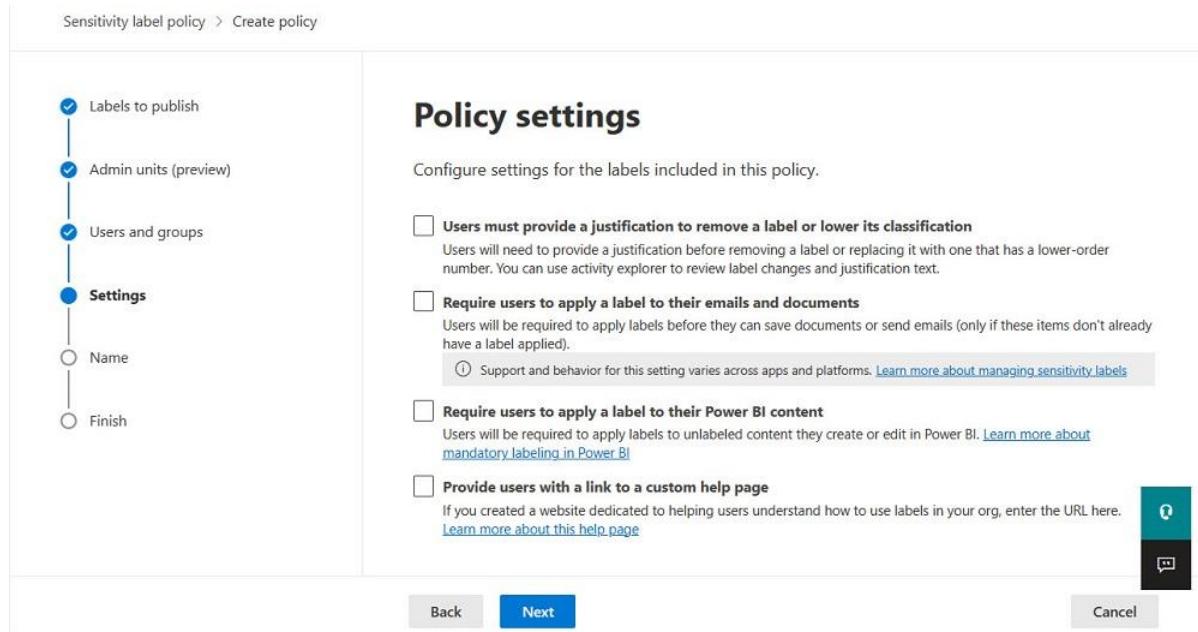


Figure 19-15: Defining settings for the sensitivity label policy

If you configure a default label for messages, Outlook creates new messages with the selected label in place. If the user then chooses to send using a different mailbox (group, user, or shared mailbox), Outlook prompts them to justify the removal of the label. This happens because the default label is associated with the original account, and when the user selects a different address to send from, Outlook removes the default label. It's logical because the account used to send messages might not have permission to use the original label.

The ultimate steps in the publication process are to create a name and description for the policy (you only need to enter a name), review the policy, and then publish it. You can't change the name of a label policy, but you can update its description at any time.

Audit Who Changes Sensitivity Label Policies: You might want to know who makes changes to sensitivity label policies. The easiest way to find out is to search the audit log for the *Set-LabelPolicy* event. The AuditData property in the audit event contains details of the changes made while the user who updated the policy is in the UserIds property.

Some Delay Before Policy Changes Become Effective

Don't expect people to be able to use new or updated sensitivity labels immediately after making changes. The publishing process takes time to enact policy changes by performing tasks like creating or updating labels. Also, multiple services must receive updates for the new policy settings. Applications pick up policy updates when they refresh their cache of tenant policies, usually within a couple of hours of an update. At this point, the applications combine the labels published through all the policies that cover the user and present the labels in a single list. Users cannot see details of the policies through which they access labels.

Multiple Sensitivity Label Policies

A tenant can have multiple sensitivity label publishing policies, each of which has different sensitivity labels and target audiences. For instance, you might create a general-purpose policy to publish a default set of sensitivity labels to everyone in the tenant and then have a set of specific policies to publish certain labels to specific groups. Another policy might publish a set of container management labels to users allowed to create groups, teams, and sites. Multiple sensitivity label publishing policies might cover the same user. If this is the case, clients combine the labels from all applicable policies to create a single set of labels to display to the user, and the policy settings which apply are determined by the order the policies are listed in the Microsoft Purview Compliance portal with the [lowest priority policy shown at the top](#) and the highest at the bottom.

In addition, if more than one policy requires mandatory labeling, Office applies the sensitivity label specified in the highest priority policy.

The Purview compliance portal doesn't include a facility to reveal which sensitivity label publishing policies make specific labels available to users. [This article](#) explains how to search the location information from policies for a user to find the set of policies that publish labels to the account.

Apply Sensitivity Labels Automatically

For licensing purposes, Microsoft differentiates between manual and automatic application of sensitivity labels to documents and email. The basic rules are:

- The Office 365 E3 license covers manual application of sensitivity labels to items. For instance, a user opens a Word document and selects a sensitivity label. If a sensitivity label policy includes a default label for different types of items, Microsoft considers that user applies the label manually when they create new items (they can choose to deselect the default and apply a different label), so this action is covered by Office 365 E3.
- Users must have specific licenses to cover the automatic application of sensitivity labels to content (see earlier comment). This covers the situation where administrators define default sensitivity labels

for document libraries. SharePoint Online applies the default label automatically when users upload new (unlabeled) items to the document library. Automatic processing also includes auto-label policies where clients or servers apply labels based on the content of messages or documents.

People might not consider default label assignment as automatic, but it is. A more advanced example is when you create an auto-label policy to assign sensitivity labels based on the content of a document or message. Auto-label policies make it easier for users to do the right thing to protect information but only for new content.

To address the problem of making sure that content receives the correct sensitivity labels, tenants can use server-side processing to auto-label email and documents, sometimes referred to as labeling content at rest (SharePoint Online and OneDrive for Business) or in transit (Exchange Online). Server-side processing is capable of processing files at scale and isn't dependent on clients, so it's appropriate when tenants have large quantities of information to protect. Organizations can define server-side automatic label policies in the Information protection section of the Microsoft Purview Compliance portal.

Points to Consider About Server-Side Sensitivity Label Processing

The following conditions apply to server-side sensitivity label processing:

- A tenant can deploy up to 100 auto-label policies to apply sensitivity labels. Each policy can cover all SharePoint Online sites and OneDrive for Business accounts in the tenant.
- The auto-label process can handle a maximum of 25,000 items per day per tenant.
- Server-side auto-labeling only works for Office documents in Open XML format (older formats like .doc Word documents don't support sensitivity labels). When an auto-label policy applies a sensitivity label to documents, it does not update their modification dates.
- Server-side auto-labeling can replace labels assigned by client-side auto-labeling, but only if the label applied by the client has a lower priority.
- Auto-label policies for SharePoint Online and Exchange Online use different rules to locate items for processing. You can define rules with the same effect for both locations. The rules for Exchange Online processing have additional conditions to match against message properties.
- Policies for Exchange Online can apply to all mailboxes or selected mailboxes.
- When an auto-label policy scans Exchange Online messages, it processes both attachments and message bodies, but if the policy finds a match, it applies the sensitivity label only to the message. In terms of rights management, the sender of the message is the issuer/owner.
- When a label applies encryption to emails, it encrypts both the message and some attachments. The encrypted attachments are Office documents and PDF files (if *EnablePdfEncryption* is True in the tenant's IRM configuration). Auto-labeling of PDFs stored in SharePoint Online and OneDrive for Business is possible if the SharePoint Online tenant configuration supports sensitivity labels for PDFs.
- If an auto-label policy matches messages protected using *Encrypt Only* or *Do Not Forward*, the sensitivity label defined in the policy replaces the protection.
- Encryption applied by sensitivity labels overrides any encryption applied by Exchange mail flow rules or data loss prevention policies. If the sensitivity label doesn't include encryption, then encryption by mail flow rules or data loss prevention policies apply.
- Incoming email passes through the Exchange transport service. It is at this point that auto-label policies evaluate messages and apply labels to matching messages. As the sender of inbound messages doesn't come from your organization, external messages encrypted by an auto-label policy don't have a valid owner. This won't matter in the normal course as recipients will have the necessary rights to read the messages.

Due to the possibility that an administrator mistake in policy configuration might auto-apply incorrect sensitivity labels to large numbers of files, the process of setting up an auto-label policy involves a simulation

period where Microsoft 365 reports results of auto-application without assigning labels. This phase allows those responsible for creating auto-label policies to evaluate the effectiveness of the policy settings by seeing what files match policy conditions. If necessary, they can adjust the conditions before releasing the policy to assign labels.

SharePoint Online uses a background process to evaluate auto-label policies. The process scans files to find instances of sensitive information types that match the rules set in policies. The scan for Exchange happens when messages pass through the transport pipeline. When a policy detects a match, the process applies the sensitivity label unless a user-applied label exists (explicit assignment always beats auto-assignment). Like labels applied by users, labels applied to documents by auto-label policies remain in place for the lifetime of documents, even if they move out of the target sites processed by policies.

Using Machine Learning to Apply or Recommend Sensitivity Labels

A variant of automatic label assignment uses machine learning to identify patterns in Office documents to decide to apply a sensitivity label automatically. Trainable Classifiers created by Microsoft or custom classifiers created within the tenant describe patterns to identify document types such as a resume (describing a document with job details) or code (computer code), and some to help identify problematic documents like those containing offensive, threatening, or profane content. Label policy settings then control the automatic application of sensitivity labels. See the section about trainable classifiers in the compliance chapter.

Removing Sensitivity Labels

It's not a good idea to delete a sensitivity label after users have applied the label to items. When an administrator removes a sensitivity label from label publishing policies, the label becomes unavailable to clients and invisible to users. Because the label metadata remains in place, any encryption applied by the label is intact. Some apps, like Office, can continue displaying the name of the label. Users cannot apply unpublished labels to content.

You can't delete a sensitivity label until after removing it from label publishing policies. If you attempt to delete a label without unpublishing it, Purview flags an error and shows which label policies include the label. To proceed and remove the label from the tenant, you must remove it first from the publishing policies.

After the deletion of a label, the underlying protection template enters an archived state. This ensures that protection remains for labeled content. Users won't be aware that files have labels because applications cannot resolve the label name against an active template. It's not possible to recreate deleted labels through the Microsoft Purview Compliance portal. Instead, you can recreate the label with PowerShell by running the *New-Label* cmdlet and (critically) passing the template identifier (GUID) of the removed label in the Identity parameter. This will reconnect the new label to the protection template. After a period to refresh client caches, the reconstituted label should reappear in applications.

Because of the issues involved in deleting sensitivity labels, it is always better to remove unwanted sensitivity labels from all label policies to unpublish them from clients instead of deleting the labels.

The removal of sensitivity labels used for container management is slightly easier. First, create a list of the containers with the sensitivity label you wish to remove. Use the *Get-Label* cmdlet to find the label GUID:

```
$LabelGuid = (Get-Label -Identity "Confidential Access").ImmutableId
```

Now find the containers that have this sensitivity label. This example uses the *Get-UnifiedGroup* cmdlet to find the Microsoft 365 groups with the label.

```
[array]$Containers = Get-UnifiedGroup -ResultSize Unlimited | Where-Object {$_ .SensitivityLabel -eq $LabelGuid.Guid}
Write-Host ("{} groups found with the sensitivity label {}" -f $Containers.count, $LabelGuid.Guid)
```

If the check finds some groups with the sensitivity label, you should replace it with the GUID of another label to maintain the settings applied to the containers. A loop like this does the job:

```
$NewLabelGuid = "d6cf185-f31c-4508-ae40-229ff18a9919"
ForEach ($Container in $Containers) {
    Write-Host ("Updating group {0} with new label {1}" -f $Container.DisplayName, $NewLabelGuid)
    Set-UnifiedGroup -Identity $Container.ExternalDirectoryObjectId -SensitivityLabel $NewLabelGuid }
```

Exchange Online will then synchronize the update with SharePoint Online and Teams to make sure that these workloads know that the containers have a different sensitivity label. This process may take a few days to complete. When it is complete, and you see that the containers show the new label in SharePoint Online and Teams, you can remove the sensitivity label that you replaced.

Remove Locations Rather Than Remove Policies

Along the same line, it's better to make a sensitivity label policy unavailable instead of deleting it as this allows for reinstatement of the policy if needed later. To do this, create a new blank group (or one with just an owner) and edit the policy so that the publication target is just that group. Purview withdraws the policy from the previous set of users, groups, and administrative units and publishes the policy to the empty group. This has the effect of nullifying the policy and putting it into a state where no one can use it. If required, you can easily reinstate the policy by editing it to publish the policy to a new set of target users and groups.

Using Sensitivity Labels with Auto-Signature Products

Many ISV products insert autosignature text into outbound messages. The autosignatures usually include personal details about the sender plus some organizational information and a company logo. If you apply a sensitivity label that protects content with encryption to an email, autosignature products might not be able to process messages because Outlook or OWA encrypts the content when sending the messages. Some products have client-side plug-ins that work by inserting text during message creation. These usually work because the client inserts the autosignature before encryption. [An Outlook API](#) makes it easier for ISVs to apply signatures to protected messages across all Outlook clients.

If you want to send encrypted emails with autosignatures, you should test the available products to find one that supports sensitivity labels. Alternatively, you can use a mail flow rule to insert an autosignature as messages pass through the transport pipeline. A mail flow rule can insert autosignature text even for encrypted email because Exchange Online uses its super-user privilege to decrypt the content, apply the autosignature, and then encrypt the message again.

Sensitivity Labels and Power BI

If enabled through the [tenant settings section of the Power BI admin portal](#), Power BI users with Pro (not free) licenses can apply sensitivity labels to reports, dashboards, datasets, embedded reports, and dataflows. Sensitivity labels are inherited by Excel spreadsheets generated through Power BI's PivotTable connection and when the Analyze in Excel feature is used. Label inheritance also occurs when new reports or dashboards are created from a dataset. By default, any licensed user can apply sensitivity labels to Power BI objects, but you can restrict access by allowing or excluding specific security groups.

Power BI uses sensitivity labels as visual markers of the relative sensitivity of the information in items and doesn't encrypt content even when a chosen label includes encryption settings. However, when Power BI exports objects to Excel, PowerPoint, or PDF, information protection encrypts the output file if required by the label. Users who export protected information from Power BI can edit the content, but they cannot change the label applied to the file. This is because the owner logged for the file is a service rather than a person, as we can see by running the *Get-FileStatus* cmdlet from the AIP module:

```
Get-FileStatus "basic data.pptx"
```

```
File      : Basic data.pptx
IsLabeled : True
LabelId   : 81955691-b8e8-4a81-b7b4-ab32b130bfff5
Label     : Secret
Method    : Privileged
Date      : 6/16/2020 11:17 AM
RMSGuid   : c7fc2174-097c-4123-9cad-15f1a32cb145
RMSTemplate : Secret
Owner     : 00000009-0000-0000-c000-000000000000@04dac1c9-6661-42f4-b974-c68551262cff.rms.eu.a
adrm.com
```

Sensitivity labels appear in the workspace list as a visual reminder to users of sensitive data. Labels are unsupported for template apps, and you can't apply the *Do Not Forward* label, labels with user-defined permissions, or labels based on HYOK.

Graph APIs for Sensitivity Labels

Two Graph APIs are available to work with Sensitivity labels for Office documents and PDF files stored in SharePoint Online. Sensitivity labels only support the latest version of the Office document formats:

- The [extractSensitivityLabels](#) API fetches details of labels assigned to an item. A document might have multiple sensitivity labels if it came from another tenant and the labels do not invoke encryption. Once a user assigns a label with encryption to a document, it becomes the only label for that document. See [this article](#) for a working example of how to use the API.
- The [assignSensitivityLabel](#) API assigns a sensitivity label to an item. This is a metered API. To pay for its use, an app that calls the API must be associated with an Azure subscription.

Some [additional methods are available to manage sensitivity labels](#) through the beta endpoint.

Protecting SharePoint Online and OneDrive for Business

Microsoft 365 includes two methods to protect content stored in SharePoint and OneDrive for Business sites.

- The optional [Information Rights management](#) (IRM) feature can protect items downloaded from a library or list. This is the older form of protection that originated in SharePoint on-premises to limit the set of actions users can take after they download files. It does not protect individual items held in the library or a list. However, IRM offers an advantage in that it doesn't require Office 365 E3 or above licenses.
- Sensitivity labels can protect individual documents, folders, and lists in a library. The label and associated protection stay with their assigned items even if the documents move from their original location. This is the preferred mechanism to protect documents stored in SharePoint Online and OneDrive for Business sites. Protection by sensitivity labels is also available for [some components used by Microsoft Syntex](#).

Apart from being an old-fashioned method to protect SharePoint content, the first approach is less preferable because protection depends on files being in a certain library and protection occurs when users download documents from the library. Assigning protection through labels applied to individual files is better because the protection persists no matter where the file travels, including outside the organization.

Optionally, file policies created by Microsoft Defender for Cloud Apps can inspect SharePoint Online documents and if sensitive data is in a document, apply a sensitivity label. [This functionality](#) is outside the scope of this book, but it's worth investigating if your organization uses Microsoft Defender for Cloud Apps.

Comparing Sensitivity Labels and IRM

Sensitivity labels are the preferred way to protect content stored in SharePoint Online and OneDrive for Business. They are more flexible and powerful than protecting SharePoint content with IRM. SharePoint Online and OneDrive for Business decrypt files protected with sensitivity labels to store and index their content. Decryption happens when users upload protected documents to a site for the first time or after editing. Being able to index protected content means that content searches and DLP policies can check both the metadata and content of protected files (SharePoint does not encrypt metadata such as document title and name for protected documents). In addition, Microsoft Search “trims” searches for protected content to ensure that only users who have access to that content see it in the results.

The advantages of sensitivity labels over traditional IRM include:

- Support for labels in a wide range of clients including desktop, browser, and mobile apps.
- Labels can apply visual markings to content in addition to protection. For instance, users see the label applied to a document when they share it with other people.
- Because rights management underpins labels, granular control is available to control who can do what with a file. Only users (including guest accounts) with access granted by the assigned sensitivity label can open a protected document (the View content right is the minimum needed).
- Users can upload protected documents if they have at least viewer permission for the documents. If the uploader doesn't possess sufficient rights, SharePoint will upload the file, but it cannot process the contents.
- Labels become part of the item metadata and protection travels with content as it moves between libraries or outside a tenant.
- Label assignments to Office documents and PDF files can be automatic (by label policy, default label set for a document library, DLP policies, or mail flow rules) or manual (by users).
- Labels can assign sensitivity markings and some group settings to Microsoft 365 Groups, Teams, and SharePoint containers. A sensitivity column is available in SharePoint Online browser document views to display labels assigned to documents. In addition, if you hover over a label in the sensitivity label column, SharePoint Online tells you if a user (manual) or policy (automatic) applied the label.
- Documents protected by sensitivity labels support advanced features like co-authoring and auto-save.
- SharePoint Online populates a sensitivity column to show the label applied to files (the column is not available in OneDrive for Business). If you hover over the label, you can see if label application was manual or automatic.
- Microsoft Search can index documents and PDFs protected by sensitivity labels. This means that protected content is available to content searches and eDiscovery, and accessible to any feature which depends on the content indexes, like DLP policies.
- SharePoint Online ensures downloaded Office files retain sensitivity labels. This capability also includes scenarios when content is created from protected files, like when PowerPoint generates a presentation from a Word document. If the input document is protected with a sensitivity label, the output file receives the same protection.

The benefit of traditional SharePoint “protection on download” is that encryption is applied automatically when files are downloaded from a library. Only people with access to the library can access the files. Users don't have to worry about applying a sensitivity label to protect confidential information.

Apps can use the Microsoft Information Protection SDK to incorporate the necessary functionality to apply and respect sensitivity labels. Office Online and Microsoft 365 apps for enterprise (Windows and Mac) support co-authoring for Excel, Word, and PowerPoint files if everyone involved has the appropriate access to protected files (the feature is in preview for Office mobile). If using the desktop apps, people must [use a version that supports co-authoring of protected files](#). Guest users can't apply sensitivity labels to documents.

The long-term strategy for any tenant should be to phase out the traditional SharePoint IRM-based protection and replace it with sensitivity labels as soon as business requirements and user training allow.

Enabling Sensitivity Labels for SharePoint Online and OneDrive for Business

When users or policies assign sensitivity labels with encryption to Office files stored in SharePoint Online or OneDrive for Business, some functionality cannot process the encrypted content in the same way as it can handle unprotected content. Until you enable support for sensitivity labels in SharePoint Online as described below, several issues exist. For more information, see [this support article](#). If you've invested in applications that update SharePoint Online with elements like custom type schemas, it's important to understand the effect that some [current limitations](#) might have on your deployment.

Exchange mail flow rules do not have the same issue because Exchange uses super-user permission (see later section) to examine protected email (and attachments) as messages pass through the transport pipeline.

Supporting Sensitivity Labels in SharePoint Online and OneDrive for Business

To enable support for sensitivity labels in SharePoint Online and OneDrive for Business, follow the directions on [this page](#). You can then enable the opt-in from the Microsoft Purview Compliance portal or by running the following PowerShell cmdlet from the SharePoint Online module:

```
Set-SPOTenant -EnableAIPIntegration $True
```

To revert, run the command again and set the switch to `$False`. This action does not remove any sensitivity labels assigned to documents. If your tenant uses multi-geo capabilities, you must run the command in each data center region (geo-location) used by the tenant.

Limitations

Some limitations currently exist in the level of access SharePoint Online has to specific types of protected documents. SharePoint Online cannot process protected documents with labels using:

- **Expiring access:** The label settings contain an expiration period after which access to the content is unavailable.
- **Double-key encryption or HYOK:** SharePoint Online doesn't have access to the key managed by the tenant.

Lack of support means that although you can store files protected with these labels in SharePoint Online or OneDrive for Business, SharePoint can't deal with the encryption and doesn't index the content (which affects eDiscovery). Features like preview and auto-save don't work, and labels with these attributes don't show up in Office Online apps. Put another way, the only supported labels are those which apply permissions set by the administrator, do not expire access, and use a single cloud-based encryption key. Some additional limitations exist which Microsoft is working through to resolve. Details of [currently-known limitations of sensitivity label support in SharePoint Online](#) are updated regularly.

When documents assigned supported sensitivity labels with encryption are uploaded into SharePoint Online or OneDrive for Windows, SharePoint Online decrypts their content before storing the document in Azure SQL. This step allows features like indexing and eDiscovery to work. The [metadata describing the sensitivity label](#) remains in place in the file and the data is protected in the store through the encryption at rest applied by Azure SQL. Any time afterward the file is requested, SharePoint checks if it needs to apply encryption and uses the metadata to ensure that the file is correctly protected. For example, encryption is reapplied when someone downloads a document with a label requiring encryption.

Default Sensitivity Label for Document Libraries

If the `DisableDocumentLibraryDefaultLabeling` setting in the tenant SharePoint configuration is False (the default), site administrators can define a default sensitivity label for a document library by selecting an appropriate label in the library settings. Any new Office document added to the library receives the assigned sensitivity label unless it already has a sensitivity label applied by a user or by an auto-label policy. In the case of policy assignment, the default label will replace the assigned label if the assigned label has a lower priority (determined by the priority number for labels set in the Microsoft Purview Compliance portal).

Stamping of sensitivity labels on new documents occurs using an asynchronous thread, so the sensitivity label does not appear (or a replacement occur) on the document for one or two minutes after its upload. Existing unlabeled documents in the library remain unlabeled until the next time someone edits the file; at which time the document receives the default label.

The default application of sensitivity labels to new documents is a premium feature that requires specific licenses (like Office 365 E5) for all members of the site hosting the document library.

To disable the default sensitivity label feature, run the `Set-SPTenant` cmdlet as follows:

```
Set-SPTenant -DisableDocumentLibraryDefaultLabeling $True
```

After running the command, the option to configure a default sensitivity label for a document library is unavailable and SharePoint Online will not assign a default label to new documents added to document libraries with a configured default sensitivity label. Sensitivity labels already assigned to documents are not removed.

Sensitivity Label Mismatches

A label mismatch occurs when someone creates, uploads, or updates a document in a site that has a sensitivity label with a higher priority than the label assigned to the site. Priority is set by the order of sensitivity labels defined in the organization. The order in which labels appear in the list should reflect their relative sensitivity or importance with the first label (order number 0) being the least sensitive and the last being the most sensitive. As an example of a mismatch, let's assume that a site has the *Confidential* label, at position 4 in the set, and a user uploads a document assigned the *Super Confidential* label, at position 5 in the set. The mismatch occurs because the document label has a higher priority than the site label. Note that SharePoint Online performs the comparison based on the position of parent labels (not sub-labels) within the set of labels in the organization.

When it detects a label mismatch, SharePoint Online sends an *Incompatible sensitivity label detected* email notification to the user who uploaded the document (Figure 19-16) to inform them that the label assigned to the document might be inappropriate for the site. No automatic action happens to rectify the issue and it's left to the user who uploaded the document (who should be in the best position to understand its true sensitivity) to decide what to do to resolve the mismatch.

The notifications help to educate users about the different levels of sensitivity labels, but it doesn't explain why this is important. In the example shown, the message recipient uploaded or updated a document with the *Confidential* label to a site labeled as *Internal*. Anyone who is a member of the site can see the document metadata even if they can't open the document. People can learn a lot about a document from its metadata and it's possible that some confidential information might leak because someone can see a document's title. For example, external people might be guest members of the site. The rights assigned in a highly sensitive label might not give some or all guests the ability to open the document to view its content, but the title might tell them what the document is about.

Another reason why mismatches matter is that a site marked with low sensitivity might allow access to people using unmanaged devices. When users upload documents of a higher sensitivity to the site, the risk exists that users might access those documents on unmanaged devices, which is not what you might want to happen.

To stop SharePoint Online sending emails to advise users about label mismatches, you can update the tenant configuration:

```
Set-SPOTenant -BlockSendLabelMismatchEmail $True
```

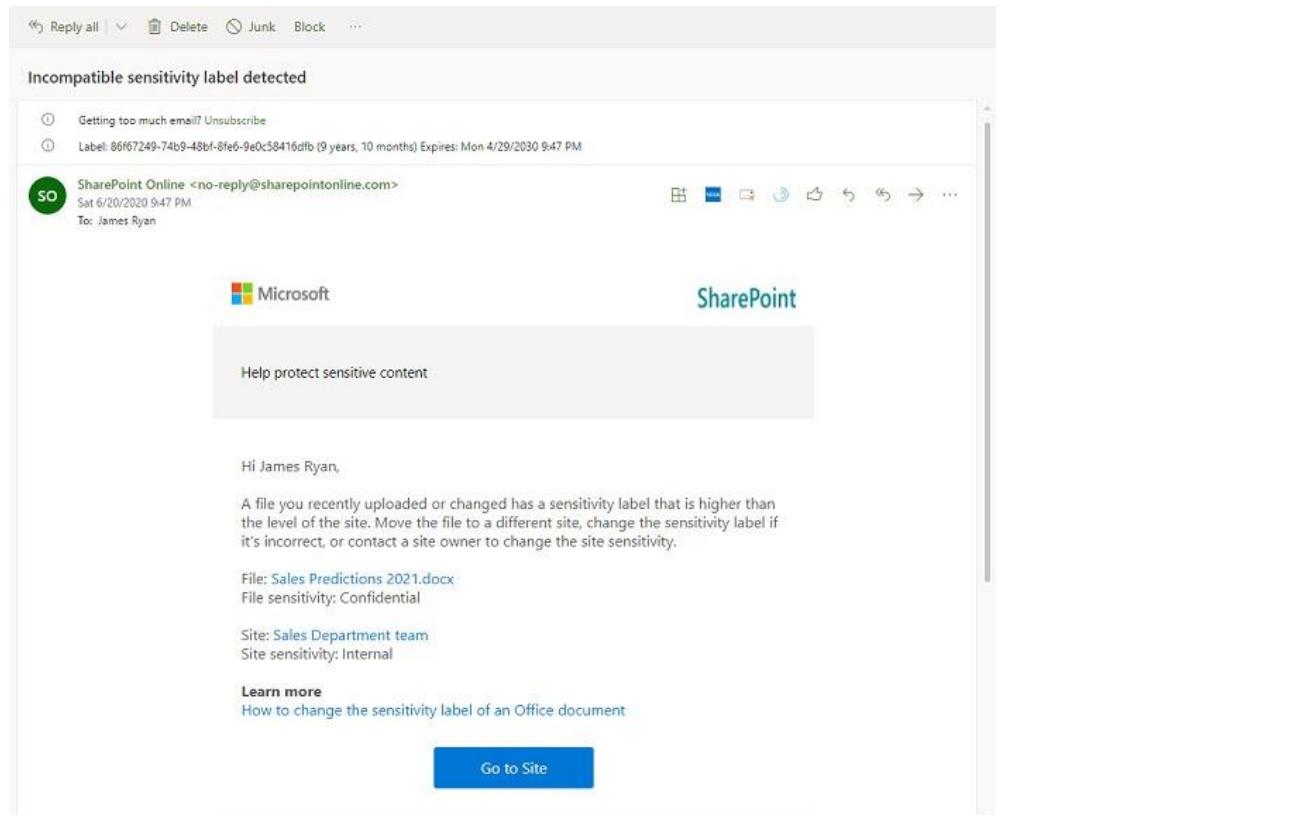


Figure 19-16: Email warning about a sensitivity mismatch for an uploaded document

The setting affects all sites. It isn't possible to block the notification emails about mismatched labels for selected sites. Blocking emails also stops SharePoint Online writing audit events to record document label mismatches. Microsoft plans to break the link between the two actions so that a tenant can block emails without stopping the creation of the audit records, but no date is available for this update.

Some organizations do not like users to receive the document mismatch notifications sent by SharePoint Online. If this is the case, it's easy to [use a mail flow rule to redirect the notification emails](#) to another recipient (perhaps the help desk) who can investigate and rectify the mismatch if necessary.

Label Order Matters for Mismatch Detection

As we know, each sensitivity label has a priority order in the set of labels. SharePoint Online uses the priority order to detect mismatches between site labels and document labels. If you separate the labels used for information protection from those used for container management, you might give the container management labels a higher priority than those used for information protection. In this scenario, you'll never see a mismatch condition occur because the label placed on the container will always have a higher priority than the labels assigned to documents. Conversely, if you place the container management labels at the less sensitive end of the label set, every document labeled will generate a mismatch condition.

If you want label mismatch checking to operate as planned, make sure that each container management label comes **after** all the information protection labels used for documents stored by the site. For instance, a

container management label called *Confidential Access* is used to label sensitive sites. An information protection label called *Confidential* is assigned to documents stored in sites labeled with *Confidential Access*. Another information protection label called *Super Confidential* exists which users should not apply to documents stored in sites assigned the *Confidential Access* label. Everything works properly if the priority order used for the labels is as shown below. In this scenario, a mismatch is detected if a document labeled *Super Confidential* is placed in a site labeled *Confidential Access*:

1. Information protection label: *Confidential*.
2. Container management label: *Confidential Access*.
3. Information protection label: *Super Confidential*.

SharePoint won't flag mismatches if the *Confidential Access* label has a higher priority than the *Confidential* and *Super Confidential* labels.

Searching for SharePoint Files with Sensitivity Labels

Office documents and PDFs store label information in their file attributes. To search for SharePoint files protected with sensitivity labels using Microsoft Search or Microsoft Purview eDiscovery (including a content search), you can:

- Use the *InformationProtectionLabelId* managed property to search using sensitivity label identifiers (GUIDs).
- Remap the *Sensitivity* crawled property to a searchable managed property to search using sensitivity label display names.

The SharePoint Online search schema includes a managed property called *InformationProtectionLabelId*, which holds the GUID (identifier) for the sensitivity label assigned to a document. You can use this property to search for documents with a specific sensitivity label in SharePoint search or content searches by using the form *InformationProtectionLabelId:GUID*. For example, *InformationProtectionLabelId:2fe7f66d-096a-469e-835f-595532b63560*. The search results are trimmed and only display documents whoever performs the search can access.

Microsoft Search captures sensitivity label data in crawled properties (extracted from a file when the SharePoint crawler processes a file). The properties include *Sensitivity*, which stores the local language version of the label applied to the stored document. You can remap the *Sensitivity* crawled property to one of the *RedefinableString* preconfigured managed properties to make label display name searchable. The SharePoint schema includes a set of 200 *RedefinableString* managed properties (from *RedefinableString00* to *RedefinableString199*) to allow tenants to customize search behavior.

To make label data searchable, use the Search section of the SharePoint Admin Center to [remap the *Sensitivity* crawled property](#) to one of the *RedefinableString* properties (for example, *RedefinableString01*). It is also a good idea to give the property an alias (for instance, *SensitivityLabel*) to make it clear what the data is. Because the crawler must process a file before the label data is searchable, you should reindex the sites that hold classified information to force the crawler to find and index the label data. After the label data is added to the index, you can search for it using terms such as "*SensitivityLabel:Confidential*".

Remapping the *Sensitivity* property allows users to search using label names like "Public" and "Confidential," but the downside is that it's possible to [assign multiple local language values for sensitivity label display names](#). If local language display names are defined for sensitivity labels, searches must include all the local language display names to be sure of finding the complete set of labeled files. By comparison, the identifier is unique and immutable, so using the label identifier is a better choice for search criteria.

Finding protected files is one thing. Being able to access them is another. Purview content searches or eDiscovery (standard) do not decrypt protected files, so you need to remove protection in another way such

as using the *Unlock-SPOSensitivityLabelEncryptedFile* cmdlet from the SharePoint Online management module or the *Set-FileLabel* cmdlet from the Purview Information Protection module. We'll discuss these cmdlets later.

Purview eDiscovery (premium) decrypts protected files unless the label has user-assigned permissions or an expiration date for user access. eDiscovery investigators can preview protected files or export them as part of a review set. If you're involved in an eDiscovery case that includes more than a few hundred protected documents, it's less expensive in terms of time and overall cost to invest in some Purview eDiscovery (premium) licenses to find and decrypt the target documents.

Offline Access

A valid use license must be available before a protected file can be opened. The use license lasts for 30 days and proves that the user has authenticated their access with Azure Information Protection to receive usage rights to the file. If a user synchronized documents and attempts to open files offline, an internet connection to Azure Information Protection is unavailable and they cannot obtain a use license. The requirement for a use license includes attachments sent with protected email.

The solution is to open protected files when online to secure the necessary use license, which becomes part of the file structure. If the user attempts to access the file when offline, the use license from the file proves that they can access and how they can interact with the file, providing that they attempt to open the file no more than 30 days after the file was last opened online. If the use license expired, the attempt to open the file fails and the only solution is to wait until an internet connection is available before attempting to open the file again.

Protecting Individual Office Documents

Users can assign sensitivity labels to Word, Excel, or PowerPoint files stored outside Microsoft 365 (for instance, a local drive). If the sensitivity label includes encryption, the app applies protection to the file the next time the user (or app) saves the file. Users must sign into a Microsoft 365 account to be able to access the set of sensitivity labels for a tenant.

If the information protection client is present on a PC, users can protect files using the **Apply Sensitivity Label with Microsoft Purview** option in File Explorer. Finally, if a user has access to PowerShell, they can run the *Set-FileLabel* cmdlet to protect individual files.

Applications can read file metadata to discover the protection status of files. Protection remains when labeled documents are uploaded to SharePoint Online or OneDrive for Business using the browser interface or if they are synchronized to a library with the OneDrive sync client. Protection for files downloaded in SharePoint Online or OneDrive for business also remains unaffected because downloading does not remove the sensitivity label.

Recognizing Labels Cross-Tenant

Sensitivity labels are specific to and owned by the tenant where they are generated and unknown outside that tenant. Sometimes (for example, during a corporate merger) you might want a tenant to recognize labels owned by other tenants. The owner of the document or message will continue to control the rights assigned by the label.

Protecting Email

Several methods are available to protect email:

- Users can apply the two default OME options (*Do Not Forward* and *Encrypt Only*) using Outlook desktop (click to run), Outlook for Mac, or OWA. Outlook mobile does not support these options.

Encrypt Only and *Do Not Forward* are available to tenants after configuring IRM. Users in tenants with Office 365 E3 and E5 can automatically read encrypted messages from other tenants; the IRM configuration must be in place to allow users to initiate new encrypted conversations.

- If configured for the tenant, users can apply sensitivity labels (with encryption) to protect messages. Recipients can only access the protected content if the rights assigned by the label allows them to interact with the content. Outlook Mobile supports sensitivity labels.
- Tenants can apply protection for messages sent to specific domains or sets of recipients by configuring mail flow rules.

Content searches can scan for and find information in protected messages. Unless you enable support for sensitivity labels as described earlier, SharePoint Online and OneDrive for Business only index the metadata of protected documents, which means that searches cannot check attachments for protected messages. To allow mail flow rules to process protected messages, Exchange Online invokes super-user capability to decrypt their content. The same occurs to index emails. In addition, Exchange Online Protection can scan the content of encrypted messages to detect malware.

All successful implementations of protection for common Office content such as email and documents involve communication with the user community to explain the need for the technology, how to protect information (including some examples of best practices based on common scenarios), and the consequences (as laid down in HR policies) that might ensue if someone ignores the protection applied to data. No need exists to hit users across the head with a 2-by-4 to enforce policies; instead, all that anyone needs is a common-sense approach from all concerned.

Enlightened and Unenlightened Email Clients

The Office 365 email clients support inline viewing of protected content. This means that clients decrypt and display encrypted information in the same way as they do for unencrypted messages. At the top of an encrypted message, clients display an information banner to tell the reader that the message is protected. These applications include the necessary software to use the rights management APIs to retrieve and consume rights policies and licenses. To enable offline access to protected messages, Exchange fetches pre-licenses for messages. Outlook for Windows and Mac (version 16.23.19021400 or later) use these licenses to decrypt the messages without needing further authentication with the server. Browser-based applications, like OWA or OneDrive for Business, run online and connect to the rights management service to obtain use licenses to handle protection for documents.

Table 19-4 lists enlightened email clients on different platforms. Unless they incorporate code from the Microsoft Information Protection SDK (the Samsung Email app for Android is an example of a client which leverages the SDK), other clients know nothing about rights management or its implementation within Microsoft 365. These clients can't obtain the necessary licenses to unwrap the protection around protected messages to display the content. In Microsoft terminology, these clients are called "unenlightened." Users of unenlightened clients must go to the OME portal to open encrypted messages.

Platform	Supported email clients
Windows	Microsoft 365 apps for enterprise (Outlook click to run) OWA Windows 10 Mail app Outlook 2013 SP1 or later
macOS	Microsoft 365 apps for enterprise (Outlook for Mac) OWA
iOS	Outlook for iOS OWA
Android	Outlook for Android

	Samsung Email app OWA
--	--------------------------

Table 19-4: Enlightened email clients

Microsoft consumer accounts can use Microsoft 365 apps for enterprise, Outlook mobile, or the OWA browser interface (outlook.com) to access protected email. Accounts belonging to other services can access protected email through the OME portal. See here for more information about [applications that support rights management](#).

Handling Unenlightened Clients

The Apple mail app for iOS is a good example of an unenlightened application that is popular with users. If an organization makes heavy use of rights management, forcing iOS users to go to the portal to read messages can be a sub-optimal experience. If you want these users to be able to read protected email on their devices, you can configure server-side decryption. The feature works for protected messages originating in the same Microsoft 365 tenant. It doesn't work for protected messages from other tenants. To enable server-side decryption, run this command:

```
Set-ActiveSyncOrganizationSettings -AllowRMSSupportForUnenlightenedApps $True
```

The downside of this approach is that decrypted copies of the message then exist on user devices. When people use an unenlightened mail app to view protected messages decrypted on the server, they see a header to tell them that the sender applied protection to the message. Unenlightened apps do not understand or apply the rights assigned to recipients, so a user of the iOS mail app can copy or print the message. Exchange Online knows that the original message has protection, and, if the user attempts to do something without permission that involves the server, like forwarding the message, the server blocks the action when it processes that message.

In most cases, if you want to protect email within a tenant, it is a better idea to encourage people to use Outlook clients rather than disabling encryption.

How Rights Management Protects Email

Users can protect email by assigning a sensitivity label (with encryption) or by using the default OME *Do Not Forward* and *Encrypt Only* features. Alternatively, if an organization has invested in S/MIME, it can use this method of protection by implementing a third-party solution or by [creating sensitivity labels to apply S/MIME digital signatures and encryption](#).

Protection for Non-User Recipients

The recipient list for a protected message can include a mixture of internal and external recipients, including those who do not use Exchange Online. Subject to the scoping defined for the sensitivity label used to protect a message, recipients will be able to open and access the content. Some restrictions exist when sending protected messages to recipients other than user mailboxes. For example:

- **Protected messages (and attachments) sent to a Microsoft 365 group** can be read by any member of the group, including guest accounts, because they authenticate their access through membership of the group. If a group member does not come within the scope of the label used to protect a message sent to the group, they can see that the conversation exists, who contributed to the conversation, and the title of the conversation, but they cannot see the content of the messages that make up the conversation because their credentials do not match the permissions assigned in the template. A banner informs the user that messages can't be displayed. If they click the banner, they see a link to the OME portal. This doesn't help either because the portal won't open protected messages when someone doesn't have the correct permissions.

- **Users with full access to a shared mailbox (delegates) can read protected messages delivered to the mailbox** if the client supports this access. This includes access to protected Office attachments. See the section about Outlook access to protected content later.
- Exchange Online can deliver **messages protected with Microsoft Purview Message Encryption** to members of a dynamic distribution list. However, the members of the list cannot read the protected content because their email addresses are not in the recipient list.
- Exchange Online cannot deliver **protected messages sent to the email address of a Teams channel** because the transport service cannot re-encrypt the message for delivery to the phantom mailbox used to route messages to Teams. The sender receives a 5.7.1. Delivery Service Notification (DSN). Exchange Online decrypts protected messages to allow mail flow rules to process their content as the messages pass through the transport pipeline.
- If you send **protected messages to a Viva Engage community**, the protected content arrives but community members cannot access the messages.

Protected messages keep their status for their entire lifetime. Any replies to messages inherit the same protection to ensure that only the intended recipients can access the entire conversation.

Microsoft Purview Message Encryption

Microsoft Purview Message Encryption (also known as Office 365 Message Encryption, or OME) is a feature available in Office 365 E3 and E5. OME makes two special rights management templates called *Encrypt Only* and *Do Not Forward* available to protect messages. *Encrypt Only* protects messages while allowing the recipient full control over the content. *Do Not Forward* blocks recipients from being able to forward a protected message. Clients encrypt messages protected by these options before they submit the messages to Exchange for onward processing. The only time Exchange applies encryption to email in transit is when a mail flow rule includes the application of a sensitivity label as an action.

Users can apply *Do Not Forward* or *Encrypt Only* to protect messages addressed to any user of any email system. Outlook and OWA clients connected to Exchange Online and Outlook.com accounts know how to process OME-protected messages, meaning that the clients can display message contents inline as normal. Recipients using other mail systems must go to the OME portal to read the messages.

Do Not Forward and *Encrypt Only* grant viewer permission to all recipients. By contrast, if you apply a sensitivity label to protect messages sent to other domains, the recipients cannot read the content unless the label settings include their email address or their domain in the list of users and groups allowed to access the content. Organizations cannot change these templates to change the permissions assigned to recipients.

Unlike a sensitivity label, which can restrict what a recipient can do after receiving a message, when you use *Encrypt Only* or *Do Not Forward* to protect a message, recipients have full rights over a message. Protection through encryption is like the set of rights defined in sensitivity labels. The sender grants the recipient the right to decrypt and view the content. Put another way, the sender implicitly trusts the recipient to do the right thing with the content when they receive it. This isn't the case with other sensitivity labels, where the assumption is that rights need to be removed from some recipients so that they don't do the wrong thing. The important thing is that both approaches assure the sender that only authorized recipients can access a message and its attachments.

The idea behind *Encrypt Only* is to encourage users to consider the protection of confidential messages as a normal thing to do. Unlike third-party solutions such as S/MIME or PGP, users do not have to configure and manage certificates or install plug-ins. To make the idea even more appealing, encryption works for messages sent to any email address. If they use an enlightened client, a recipient can read encrypted content inline, while users of other email systems can read encrypted messages through the OME portal. These users receive

a message with a link to allow them to log into the portal and read the message content. The link lasts for sixty days.

People who receive encrypted messages forwarded to them (by another person, rules, or when a forwarding address is set for a mailbox) cannot read the content because their addresses are not in the original recipient list. If a user forwards an encrypted message with OWA or Outlook, the recipient's address is added to the message header, and they can read the encrypted content.

S/MIME and Microsoft Information Protection

[S/MIME \(Secure/Multipurpose Internet Mail Extensions\)](#) is a protocol that uses X.509 digital certificates to digitally sign, encrypt, or sign and encrypt messages. Like any protection scheme, S/MIME helps people who receive emails to be sure that messages are not tampered with in transit. S/MIME also helps to authenticate the sender; it proves the message is not spoofed. Before sending messages, the sender chooses to sign and/or encrypt the message, which is then processed like any other outbound message. The recipient uses the PKI infrastructure to verify the certificate and confirm the signature of the message. When a message is encrypted by S/MIME, the certificate of the recipient is used. For the sender to encrypt a message, he must have access to the public key of the recipient's S/MIME certificate. This requires the sender to import the recipient's certificate information before encrypting the email. For messages sent within the organization, an administrator can automatically publish that information to the Global Address List.

Outlook desktop, Outlook Mobile, and OWA support S/MIME for signing and encrypting messages. You can use S/MIME signing for both internal and external communications. When the S/MIME setting is enabled, Outlook for iOS and Android automatically disable the **Organize by Thread** setting. This is because S/MIME encryption becomes more complex as a conversation thread grows. By removing the threaded conversation view, Outlook for iOS and Android reduces the opportunity for issues with certificates across recipients during signing and encryption. As this is an app-level setting, this change affects all accounts added to the app.

It is technically possible to combine encryption applied by S/MIME with Microsoft Information Protection (and you can configure a sensitivity label to use S/MIME). Applying multiple levels of protection only works if you use S/MIME to encrypt a message and then protect it afterward. Mixing protection types is only possible using Outlook desktop (for Windows) because this client is intelligent enough to resolve the inherent conflict between the two encryption schemes. Of course, just because something is technically possible does not mean that it is feasible in practice. Combining S/MIME and Microsoft protection might result in a message that the recipient cannot process. A more practical approach is to select one scheme and use it everywhere. An organization should only consider using S/MIME if it already has a heavy investment in the technology needed for key management and clients deployed which can consume S/MIME-encrypted messages or if the organization decides to use third-party technology for protection. Outside these circumstances, we recommend that tenants avoid the complications (and extra costs) to deploy, manage, and maintain third-party encryption mechanisms and use the information protection features built into Microsoft 365 to protect email and documents.

Real-world: When configuring S/MIME, you can use an internal or external (third-party) certificate authority. In both scenarios, the entire certificate chain must be uploaded to Microsoft 365. To do this, you can export the chain from a local machine into an SST file and upload it to Microsoft 365, as described in [this procedure](#). After uploading the certificate, allow at least 30 minutes for the changes to replicate across Exchange Online. If you do not upload the certificate chain, you will see a message that says "An error occurred while sending this S/MIME message. The certificate used to sign this message isn't trusted by your organization."

In addition, configuring sensitivity labels with S/MIME does not remove the requirement to have a fully-functional S/MIME deployment in place. A functioning S/MIME environment must exist before you can

create and publish sensitivity labels to apply S/MIME encryption or signatures. Finally, Microsoft 365 Copilot does not support and will not use S/MIME-protected email.

Encrypt or Protect

Given the choice to encrypt or protect messages, what should you do? Here's a simple rule of thumb:

- **Encrypt** messages to protect confidential or sensitive data sent to recipients outside your organization.
- **Protect** messages with confidential or sensitive data sent to internal recipients.

This rule of thumb is based on the simple fact that OME works for messages sent to any email address, so it is the catch-all solution when a need exists to protect content sent outside the company. Not every destination might be able to understand the limitations imposed by sensitivity labels, but if a label is configured to support recipients in an external domain, it is an excellent way to protect information for the lifetime of the content.

Protecting Email with Outlook

Outlook desktop clients automatically download the set of sensitivity labels available to users and refresh this information by connecting to the Information Protection service every four hours. Once the client downloads label information, Outlook has two options to protect email:

- **Apply a Sensitivity Label.** The **Sensitivity** button in the menu bar reveals the set of sensitivity labels scoped for email and published to your account. The same set of labels are available through a drop-down list beside the subject field (Figure 19-17). After selecting a label, the name of that label is visible here to act as a reminder of the protection status for the message. An Outlook profile can configure accounts from multiple domains, but sensitivity labels are specific to a tenant, so you only see the labels belonging to the tenant configured in the default profile.
- **Apply a standard template:** The **Encrypt** button in the **Options** tab applies the OME *Encrypt Only* or *Do Not Forward* templates. The default option is to apply the *Encrypt Only* template. Click the arrow under the button to apply *Do Not Forward* protection to the message.

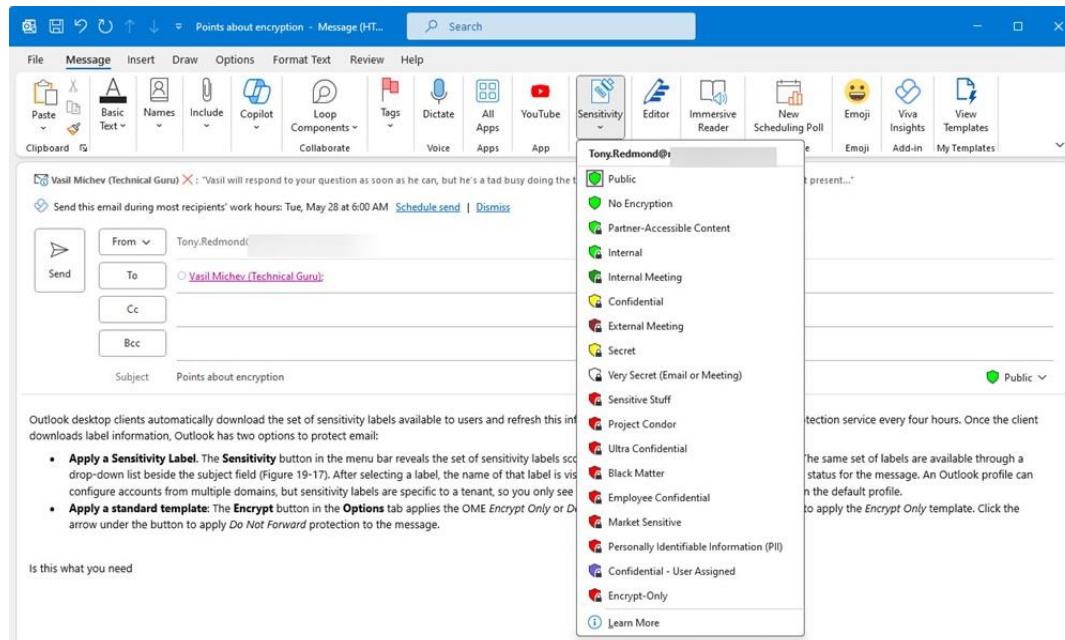


Figure 19-17: Selecting a sensitivity label for a message with Outlook for Windows

Any replies and forwards (if allowed) created in response to a protected message inherit the same level of protection. Because the author always has full control over the content, they can decide to forward the message to another person, reply to the original message, or apply a different label. The sensitivity label policy that makes labels available to Outlook determines how Outlook handles Office documents and PDFs attachments. Normally, attachments inherit the label assigned to the message unless an attachment has a higher-priority label. In that case, the attachment keeps its protection. However, a policy setting allows Outlook to increase the overall level of protection for a message to that of the highest-priority label assigned to an attachment. See the section about publishing sensitivity labels for more information.

Outlook Delegate Access

Delegates are users granted access rights to another user's mailbox or to a shared mailbox. The ability of a delegate with full access to a mailbox to read encrypted messages depends on the client used and the type of mailbox. Only Outlook clients support the ability of delegates to read encrypted messages (and attachments) subject to the following:

- Outlook for Windows clients do not support delegate access to encrypted messages sent to user mailboxes. Delegates can only read encrypted messages if the sender includes the delegate as a TO or CC recipient. In this scenario, the delegate's ability to read the message depends on the rights granted to them as a recipient.
- Outlook for Windows clients support delegate access to encrypted messages sent to shared mailboxes if the delegate has full access and auto-mapping is specified when the delegate receives permission to the mailbox. Auto-mapping is the default used by Exchange Online when delegates receive full access permission through the Microsoft 365 admin center or Exchange admin center. It forces Outlook for Windows to open the shared mailbox as part of the resources available to the delegate.
- The other Outlook clients (OWA, Outlook for Mac, Outlook Mobile, and the Windows Mail app) support delegated access to encrypted messages in both user and shared mailboxes if the delegate has full access to the mailbox.
- If a mail-enabled security group is a delegate for a shared mailbox, members of that group can view and respond to messages protected by the Do Not Forward and Encrypt-only templates.

Microsoft documents [some restrictions that apply when delegates attempt to open encrypted messages](#) in shared mailboxes. For outbound messages, it's important to understand that Purview scopes labels based on user accounts. For instance, let's assume that a sensitivity label publishing policy dictates that the default label for email is "*Private*." All messages created by users coming within the scope of the policy receive the *Private* label. However, messages sent by the same users when acting as a delegate for a shared mailbox do not receive the *Private* label because the shared mailbox is not within the scope of the label policy. To make sure that messages sent by delegates from shared mailboxes are appropriately protected, use a transport rule to apply labels after the delegates send the messages.

If you want to prevent users with full access to a user or shared mailbox from being able to view encrypted messages using clients other than Outlook for Windows, you can block their access by running the *Set-MailboxIRMAccess* cmdlet. For example, this command blocks the ability of Kim Akers to read any encrypted messages delivered to the Customer Services mailbox:

```
Set-MailboxIRMAccess -Identity Customer.Services@Office365itpros.com -User Kim.Akers@Office365itpros.com -AccessLevel Block
```

To make sure that a block is in place, use the *Get-MailboxIRMAccess* cmdlet:

```
Get-MailboxIRMAccess -Identity Customer.Services@Office365itpros.com -User Kim.Akers@Office365itpros.com
```

Identity	User	AccessLevel
Customer Services	Kim.Akers@office365itpros.com	Block

A block on delegate access remains in place until an administrator removes it and only affects the ability of a delegate to read encrypted messages using clients that support the block. For instance, the block will stop a delegate reading encrypted messages in a shared mailbox using OWA or Outlook for iOS, but they can switch to Outlook for Windows to see the message content. In addition, blocking access does not hide message subjects, which can contain sensitive information, nor does it prevent a delegate from deleting or moving encrypted messages. The block exists for reading, and only works for clients that support the block.

To remove the block and restore the ability to read encrypted messages to a delegate, run the `Remove-MailboxIRMAccess` cmdlet:

```
Remove-MailboxIRMAccess -Identity Customer.Services@Office365itpros.com -User
Kim.Akers@Office365itpros.com
```

Remove Encrypt Only: Some organizations consider that users should only use sensitivity labels to protect messages and want to remove the standard OME *Encrypt Only* template. The instructions to do this are [available online](#).

Protecting Email Attachments

Unprotected Office documents (and PDF files if enabled: see the notes about the *EnablePdfEncryption* setting in the tenant IRM configuration earlier) attached to protected messages inherit the same protection as assigned to the message. For example, if you attach a Word document to a message protected with a sensitivity label that only allows edit access for the author, the recipients will be able to view its content but will not be able to edit it. If a higher level of protection is applied to a file before it is attached to a message, that protection is preserved for the attachment.



Figure 19-18: A protected Word attachment viewed with Word for iOS

Figure 19-18 shows a Word document open on an iPhone. This is an attachment to a protected message opened by Outlook for iOS. The user can discover what rights they have over the content by clicking **Permissions**.

Recipients can open and edit attachments in file formats that do not support sensitivity labels, like text files or bitmap images, unless you protect the files with the information protection client before attaching them to the message. If a user applies a sensitivity label without encryption to a document and attaches the file to a message, Outlook assigns the same label as applied to the message to the document to ensure consistency of protection.

Automatic Decryption of Encrypt Only Attachments

Dealing with protected attachments is not an issue for Exchange Online clients because they can obtain the necessary use licenses to decrypt the attachments when opening messages. If a message using Encrypt Only goes to recipients of other email systems like Gmail, recipients can read the messages after authentication through the OME portal, but they cannot access the contents of a downloaded attachment because the downloaded copy of the attachment remains protected. If you want external recipients to be able to download decrypted copies of attachments, you must update the IRM configuration to instruct Exchange Online to decrypt attachments and remove protection whenever they are accessed or downloaded by an authenticated recipient. The effect is to give recipients full control over the downloaded files. To change the configuration, run this command to update the tenant IRM configuration:

```
Set-IRMConfiguration -DecryptAttachmentForEncryptOnly $True
```

This setting only applies to messages protected with the Encrypt Only feature.

Viewing Rights

When you open a protected item, you see the name of the template and some information about its intended use. Outlook users can click a message header to gain more insight into what they can and cannot do with a protected item (Figure 19-19). It is obvious from the list of rights supported for email that you cannot block every conceivable action that a recipient can take with a message.

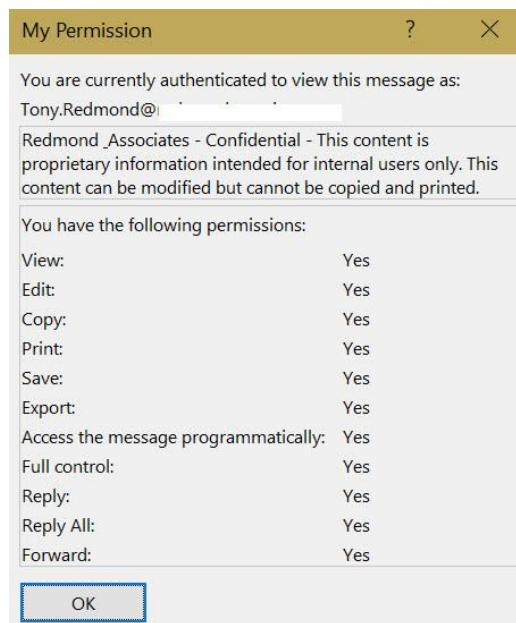


Figure 19-19: Outlook reveals the rights available for a message

For instance, although you can remove the Copy right to stop someone from copying text from a message or attachment, including blocking screen captures on Windows devices, you cannot stop someone from taking a

screenshot with a smartphone and circulating that image to others. The point here is that protection cannot prevent every kind of unacceptable user interaction with content. Users must accept some responsibility for their actions. Applying a sensitivity label to an item makes users aware that the author protected the information for a reason and that they should therefore deal with that information appropriately. What they do is entirely up to the user.

Protecting Email with OWA

Because OWA operates in online mode, it always uses the current set of sensitivity labels published for a user. In saying this, we should realize that some client-side caching occurs for performance and that a small delay is likely before a new label or a change to an existing label published by the Microsoft Purview Compliance portal becomes available in OWA.

The Sensitivity button is available as an option in the OWA new message window. After a label is set on a message, the label name appears in the banner above the message recipients. In Figure 19-20, the sensitivity label selected for the message invokes encryption because of the padlock icon beside the label name. A sensitivity label that acts as a visual indicator (applies no encryption) has a plain label icon without a padlock. OWA also displays these icons for labeled items in the read message window. Like Outlook, the protection applied to a message also applies to any of its attachments.

Users can also apply sensitivity labels to replies to messages that do not have labels. In this case, the **Sensitivity** option to apply a label is in the [...] menu of the reply message window. When you assign a sensitivity label to a reply, it does not apply to the previous messages in the thread, but Exchange automatically assigns the same label to future messages in the thread.

OWA can also use the OME *Encrypt Only* and *Do Not Forward* features to protect messages. Click the Options menu and you'll find **Encrypt** in the list of menu choices. Using these templates for protection does not assign a sensitivity label to the protected messages.

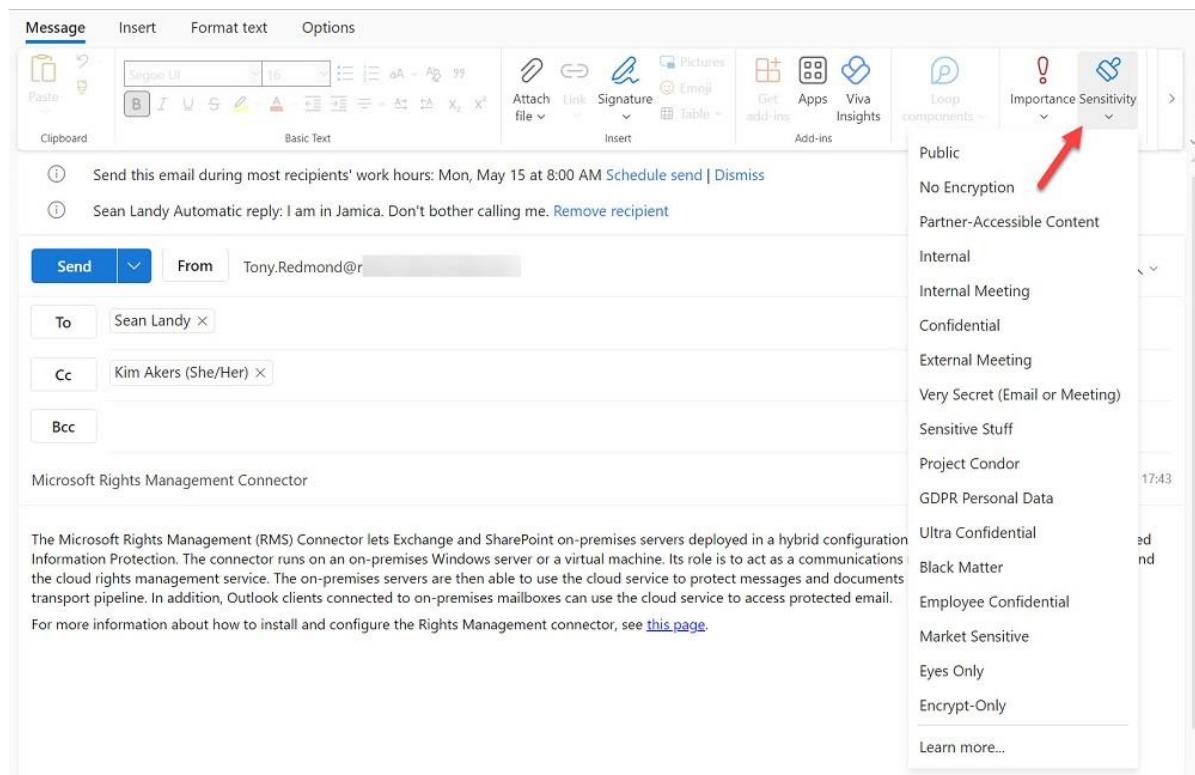


Figure 19-20: Applying a sensitivity label to a message with OWA

Microsoft Rights Management Connector

The Microsoft Rights Management (RMS) Connector lets Exchange and SharePoint on-premises servers deployed in a hybrid configuration access the capabilities of cloud-based Information Protection. The connector runs on an on-premises Windows server or a virtual machine. Its role is to act as a communications relay between on-premises servers and the cloud rights management service. The on-premises servers are then able to use the cloud service to protect messages and documents and process protected email in the transport pipeline. In addition, Outlook clients connected to on-premises mailboxes can use the cloud service to access protected email.

For more information about how to install and configure the Rights Management connector, see [this page](#).

Managing Microsoft Purview Message Encryption

Microsoft Purview Message Encryption (OME) is an online service built on top of rights management to allow users to protect emails sent to recipients in any email system. OME includes:

- The default Encrypt Only and Do Not Forward templates.
- The ability to encrypt messages sent to specific destinations through mail flow rules. For example, you might decide to encrypt all messages sent to a partner domain. Any sensitivity label with encryption can protect content using a mail flow rule.
- The message encryption report (available to Office 365 E3 and E5 tenants), is available in the [Reports section of the Microsoft Purview Compliance portal](#). This report details how messages receive protection (by users or by policy) and whether encryption occurs through a default template or sensitivity label. The data is useful in terms of understanding how many people protect email the organization. Because Exchange Online generates the report data daily, the information is not real-time and can be up to a day behind.

OME-protected messages do not support protecting messages sent to dynamic distribution lists. Exchange Online bifurcates messages to deliver copies to the members of the dynamic distribution list when they pass through the transport pipeline. Although the list members receive copies of the message, they are not direct recipients and do not have the right to open the message. A sensitivity label protects messages sent to dynamic distribution lists if the permissions assigned in the label grant access to everyone who receives a copy.

It's worth emphasizing that OME is all about protecting email without needing the recipient to install any special software. Sensitivity labels can also protect email with encryption, but the big difference is that sensitivity labels also define the actions a recipient can take after they open that content. Organizations can also include sensitivity labels as an action for mail flow rules to execute on outbound messages.

Customizing the OME Configuration

When an external recipient (not belonging to another Office 365 tenant or Outlook.com) receives a protected message, they receive a notification message to tell them what they must do to access the content. The notification directs the recipient to sign into the OME portal using an account from one of the federated identity providers. If they cannot sign in or prefer not to, the recipient can get a one-time code to read the content. After signing in, the user sees a modified version of the OWA read message window, which enforces the permissions they have over the content.

You can customize the OME configuration (otherwise known as a branding template) to add custom text used in the notifications and the OME portal. To start, use the `Get-OMEConfiguration` cmdlet from the Exchange Online module to view the details of the standard OME configuration. In this case, the configuration has several customized settings, which we can update further with the `Set-OMEConfiguration` cmdlet.

```
Get-OMEConfiguration -Identity "OME Configuration"
```

```
TemplateName      : OME Configuration
Image           : {137, 80, 78, 71...}
ImageUrl        :
EmailText       : Thank you for communicating with our company. To protect our
confidentiality, this message has been encrypted.
PortalText      : Our Great Encrypted EMail Portal
IntroductionText :
DisclaimerText   : Office 365 for ITPros takes no responsibility for the operation of this
portal
ReadButtonText  : Protected Email
OTPEnabled      : True
SocialIdSignIn  : True
ExternalMailExpiryInterval : 00:00:00
PrivacyStatementUrl :
Identity        : OME Configuration
```

Important settings include:

- **BackgroundColor:** You can set the background color for OME messages and the portal by passing the hex code color. Usually, people who know about corporate branding will know [the right code](#) to use.
- **DisclaimerText:** A string of up to 1024 characters placed at the bottom of the encrypted message intended as a disclaimer but can convey a different message. If you don't provide a value, OME uses: *"This email message and its attachments are for the sole use of the intended recipient or recipients and may contain confidential information. If you have received this email in error, please notify the sender and delete this message."*
- **EMailText:** A string of up to 1024 characters to tell the recipient that they have received an encrypted message. If you don't provide a value, the default OME text is *"You've received an encrypted message from"* plus the SMTP address of the sender. If you change the default message, OME does not include the sender's SMTP address (but it still appears in the message header).
- **Image:** An image file (.png, jpg, .bmp, or .tiff) of less than 40 KB to show that messages originate from the sender's company. Ideally, you might use a 170x170 pixel version of the company logo. By default, OME does not display a logo.
- **OTPEnabled:** If true (the default), recipients can opt to get a one-time code to access the portal. Set this to False if you want to force users to authenticate using an account from one of the supported providers.
- **PortalText:** A string of up to 128 characters that the OME portal displays when users connect to access a decrypted message.
- **PrivacyStatementURL:** A link to a web page for the company's privacy policy. This link is invoked when a user clicks the Privacy Statement link in an OME notification.
- **ReadButtonText:** A string to display on the Read button in the notification. To make sure that it fits on the button, this text should be no more than 16 characters.
- **SocialIdSignIn:** Defines if a recipient can authenticate to read a message using an identifier from a recognized social network such as Google or Yahoo! If False, the recipient can authenticate using another method such as a one-time password.

For example, this PowerShell command updates several properties in the OME configuration:

```
Set-OMEConfiguration -Identity "OME Configuration" -BackgroundColor "#5183cd" -DisclaimerText "We
take zero responsibility for anything that happens here." -EmailText "Yippe! You've got some
encrypted super-secret email" -PrivacyStatementUrl "https://office365itpros.com/privacy.html"
```

Here's how to add a graphic file for the logo displayed in notification messages and the OME portal:

```
Set-OMEConfiguration -Identity "OME Configuration" -Image (Get-Content "C:\Temp\CompanyLogo.jpg"
-Encoding Byte)
```

When you update the OME configuration, Microsoft warns that custom content used in configurations is the tenant's responsibility. In other words, make sure that any graphics and text used are not protected by trademarks or other restrictions.

Figure 19-21 shows the effect of the updated OME configuration. The logo appears at the top of the message, the email text appears under the link, and the customized disclaimer text is in place. The restricted permission attachment (rpmsg) is the encrypted content shown when the user accesses the message through the OME portal. Internal recipients do not see notifications unless they use a non-Outlook client that can't obtain the necessary use licenses to decrypt and display the protected content automatically. For example, if you connect to your mailbox using an IMAP4 client, you'll see notifications for protected messages sent by other people in the tenant.

Fwd: Looking after our customers during COVID-19

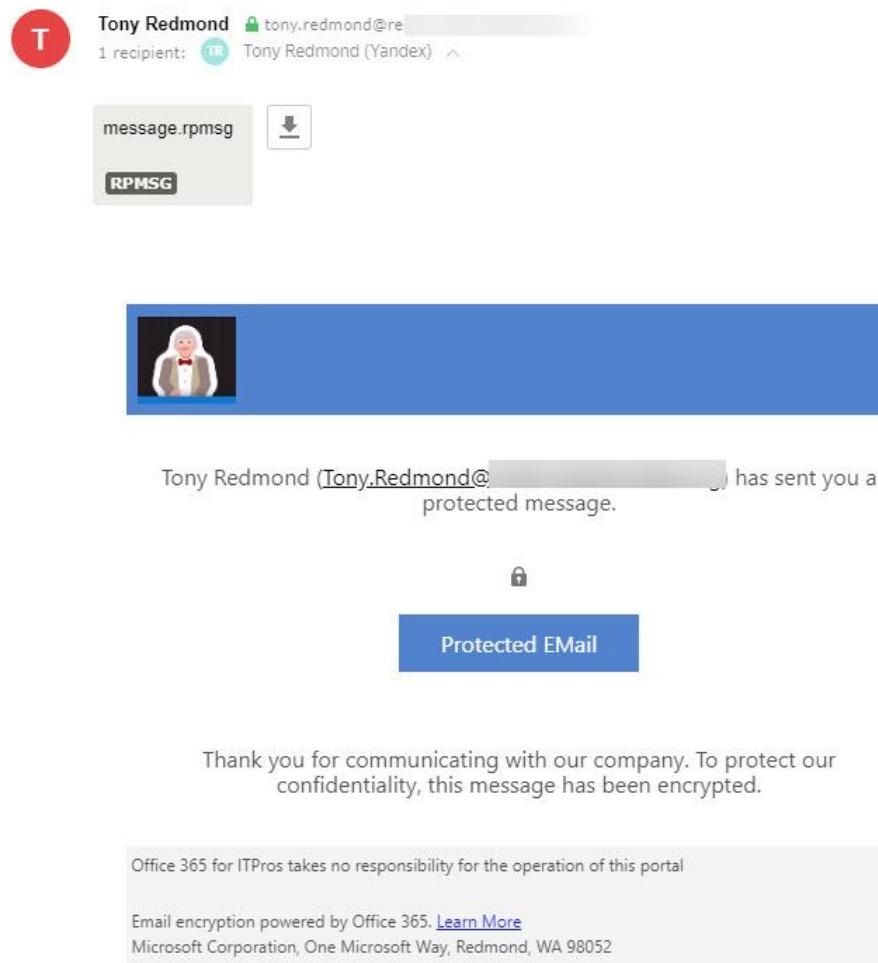


Figure 19-21: The OME notification received to let someone know that they should read some protected email

Creating a Custom Branding Template for OME

Custom branding templates are available to tenants with Office 365 E5 licenses and are created with PowerShell. This example shows how to create a new branding template and then populate the properties of the new template.

```
New-OMEConfiguration -Identity "Office 365 IT Pros Branding"  
  
Set-OMEConfiguration -Identity "Office 365 IT Pros Branding" -DisclaimerText "Office 365 for IT Pros takes no responsibility for this portal." -PortalText "Office 365 for IT Pros Secure Messaging" -EmailText "Good things happen when you protect email" -ExternalMailExpiryInDays 10
```

```
-IntroductionText "has sent you a secret message" -Image (Get-Content "C:\Temp\SmallBookCover.jpg"
-Encoding byte)
```

See [this page](#) for more information about how to customize a branding template. Remember that it can take between 15 and 30 minutes for a change made to a mail flow rule to become effective, so factor this into the time needed to test how custom branding templates work. Recipients of custom-branded messages cannot read protected content inline, even if they use a client that supports inline decryption like Outlook. The logic here is simple: if you apply custom branding to messages, you want recipients to see the custom branding and that can't happen if they read the emails inline.

To test that branding works, create a mail flow rule to apply a custom branding template to messages in a specific domain and send a protected message to an account in that domain. When it arrives in the recipient mailbox, check that the custom branding is visible when the recipient opens the message.

Administrator Revocation of Encrypted Messages

Recipients of protected messages fall into two categories: internal and external recipients. Revocation, which means removing the right of a recipient to view encrypted content, is only possible for external recipients that receive messages including a link to access the decrypted content. This is because the OME portal controls access to the protected content. Messages to users in other Microsoft 365 tenants or Outlook.com are irrevocable because these users don't need to access the OME portal to read protected messages.

Administrators can revoke a message through PowerShell by finding the identifier of the message to revoke and then running the *Set-OMEMessageRevocation* cmdlet. The easiest method to find a message identifier is to use the [Message Trace feature in the Exchange admin center](#) (or by running a message trace with the *Get-MessageTrace* cmdlet).

Execute a search to find the message, select it in the set of results, and look at its properties. The message identifier is a long string ending in something like "prod.outlook.com." When you have the identifier, run the *Get-OMEMessageRevocation* cmdlet to check that the message is revocable. At this point, Exchange Online knows if the message recipient received a link to the OME portal or could read the message inline. If you see that the message is revocable, run the *Set-OMEMessageRevocation* cmdlet to revoke permission. For example:

```
$MessageId = "AM6PR0402MB3462A8DF67AF7AF9C9F0B20A8BE50@AM6PR0402MB3462.eurprd04.prod.outlook.com"
```

```
Get-OMEMessageStatus -MessageId $MessageId | Select Subject, IsRevocable
```

Subject	IsRevocable
----- Important Information	True

```
Set-OMEMessageRevocation -Revoke $True -MessageId $MessageId
```

The encrypted email with subject "*Plans for next year*" and Message ID "AM6PR0402MB3462A8DF67AF7AF9C9F0B20A8BE50@AM6PR0402MB3462.eurprd04.prod.outlook.com" was successfully revoked.

To check the status of the message, you can run the *Get-OMEMessageStatus* cmdlet. The results returned by the cmdlet confirm the revocation of the message:

```
Get-OMEMessageStatus -MessageId $MessageId
```

RunspaceId	: 4039a474-e2ab-498f-a92c-460154537c8f
Identity	: 04e78939-85a9-4bf8-8d65-9f533648bb37
IsValid	: True
ObjectState	: New
Container	: SystemMailbox{D0E409A0-AF9B-4720-92FE-AAC869B0D201}@office365itpros.onmicrosoft.com
Subject	: Tony Encrypt
ReceivedTime	: 7 Oct 2021 14:03:55
Revoked	: True

When the recipient goes to the OME portal and tries to read the protected message, they see "the message has been revoked by the sender" and that they should contact the original sender if they want access to the content. If an administrator revokes a message, there's no way for the original sender to cancel the revocation. If the administrator makes a mistake and revokes a message incorrectly, the original sender will have to resend the message.

Advanced Microsoft Purview Message Encryption

The standard OME supports a single branding template, applied by Exchange Online to all protected messages delivered to recipients outside the tenant. Advanced OME adds support for:

- Multiple branding templates and the application of branding templates in mail flow rules. For instance, you could use a mail flow rule to protect all messages sent to a partner domain and customize the template that recipients in that domain see. To do this, select the **Apply Custom Branding to OME messages** action in a mail flow rule along with the custom template to use and the criteria to apply the branding (for example, specific domains). Custom branding templates are updated in the same manner as the general template used by the standard version of OME (see above).
- Expiry of protected email. The custom templates support the ability to expire messages sent to external recipients after a set period of anything from one to 730 days.
- [Revoke access for external recipients to protected email](#). This feature is available in OWA when senders have an Advanced OME license, and the recipient accesses the encrypted content through a link to the OME portal. Alternatively, an administrator can revoke access to a message on behalf of a user using PowerShell (see below).

Advanced OME is an Office 365 E5 feature also licensed using the Microsoft 365 E5 Compliance SKU.

Custom branding is an optional action for mail flow rules. If you apply custom branding in its own rule, make sure that the rule to apply branding runs (has a lower priority) after any rule which applies encryption. In addition, make sure that any rule which applies encryption or custom branding does not terminate rule processing and let other rules with lower priority run afterward.

Using Microsoft Purview Message Encryption with Mail Flow Rules

The basic scenario is when a mail flow rule protects email sent to a specific destination, which could be a group of users or one or more domains. Messages sent by clients connected to Exchange Online mailboxes must pass through the transport pipeline. As messages flow through the transport pipeline, Exchange Online uses the criteria defined in mail flow rules to examine messages. If an email matches a rule, Exchange Online applies the action or actions defined in the rule. The rule set can span hundreds of rules to account for different circumstances, and Exchange Online examines each message against each rule until it reaches the end of the rule set, or the action set in a rule causes rule processing to halt.

Adding protection to messages by applying a template is one of the actions available for mail flow rules. This capability is often used to ensure that protection is applied to messages even if they originate from clients that do not support rights management, such as the default mail apps for iOS and Android. Using mail flow rules to apply encryption also avoids the need for users to select the right template to apply when they compose a message. If many different templates exist, users might not know what template they can use to protect messages sent to a certain domain or user. For this reason, organizations often use mail flow rules to apply protection to ensure that confidential information cannot pass in an unencrypted form to recipients outside the tenant. A mail flow rule can apply protection using criteria such as:

- Any message sent to specific domains.
- Any message sent to specific users.

- Any message that contains a specific phrase in the message text or an attachment.
- Any message that has a specific word in its subject.

When a mail flow rule protects outbound messages, the senders of those messages might not be aware that this processing occurs because the copy of the item in their Sent Items folder is unprotected. This is because mail flow rules apply sensitivity labels in the transport pipeline to protect the message copies delivered to recipients. The copy of the message in the sender's mailbox has not been through the transport pipeline and is therefore unprotected. If users want to see a protected copy, they must include their email address as a recipient.

Configuring a Mail Flow Rule to Apply Protection

Management of mail flow (transport) rules is performed in the **Mail flow** section of the EAC (for more information on this topic, see the discussion about mail flow rules in the Mail Flow chapter). In Figure 19-22, we see details of a mail flow rule to do the following:

- Monitor messages sent by members of the Executive Committee distribution list; and
- Apply the "Internal" template to these messages using a modify the message security action.

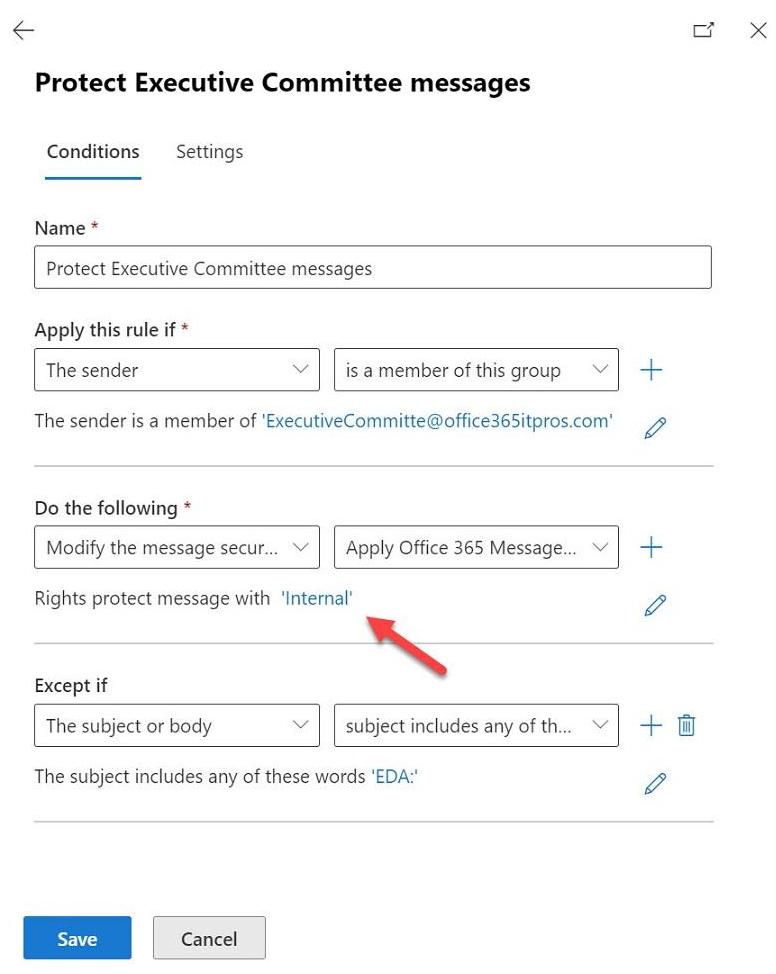


Figure 19-22: Applying protection with a mail flow rule

Microsoft publishes details of a mail flow rule to encrypt outbound messages with certain sensitive information types (like credit card numbers). The prototype rule they suggest is a good start, but you should [carefully review and adjust the rule](#) to ensure that it meets the need of your tenant.

Exemptions

Often rules include an exception condition to allow users to override the rule in certain circumstances. For example, if the subject of the message has a specific text pattern, the rule will not apply the sensitivity label. When a rule allows a message to pass without intervention due to an override, because the transport captures the fact that it processed the rule in the message header, Exchange Online will not try to apply the rule again to replies and forwards that flow from the original message.

Another common exception is not to apply protection when the recipient is a member of a specific group. The logic here is that the members of the group might need to change or update the content circulated in emails.

Although distribution lists are an excellent way to specify the users that come under the scope of a mail flow rule, remember that Exchange Online caches group membership to avoid the performance penalty of going back to Entra ID to expand membership each time a group is in a message header. For this reason, do not expect a change made to a group used in a mail flow rule to be effective at once. It can take between 30 minutes and an hour before the transport service learns about the new group membership.

Interlocking protection: You can apply a mixture of DLP checking and sensitivity labels to make sure that sensitive data does not leave the organization unprotected. If the transport service detects sensitive data protected by a DLP policy in a message, a mail flow rule can apply a label. This level of interlocking protection helps organizations ensure that people do not misuse sensitive data.

Handling Protection when Mail Flow Rules Process Protected Messages

Users might protect messages using the default Encrypt Only or Do Not Forward templates that are subsequently processed by a mail flow rule which also attempts to protect the message. When this happens, the level of protection is adjusted if the protection applied by the rule is more restrictive (higher sensitivity) than chosen by the user, which might affect the rights assigned to recipients.

This is logical because the author has already explicitly applied protection to the message with what they believe is the right level of protection. Overriding protection selected by a user with a rule runs the risk of interference with the recipient's ability to process the message in the way intended by the author.

Applying Protection in Mail Flow Rules with PowerShell

Two methods are available to apply templates to outbound emails. The traditional approach that we've just explored is to use a mail flow rule; a newer approach is to specify protection as an action in a DLP policy that fires when the DLP service detects sensitive data in a message. You can find information about how to invoke protection in DLP policies in the Data Loss Prevention chapter. Because of the complexities involved in many rules and policies, it is often easier to build them through the relevant GUI (EAC for mail flow rules, Microsoft Purview Compliance portal for DLP policies), but PowerShell can also be used for the task.

The *New-TransportRule* cmdlet creates a new mail flow rule. In this example, we create a rule that applies the "Sensitive Board Reports" label to messages sent from one distribution list to another distribution list.

```
New-TransportRule -Name "Protect Board Meeting Information" -FromMemberOf "Board Reports"
-SentToMemberOf "Board Members" -ApplyRightsProtectionTemplate "Sensitive Board Reports"
-ExceptIfSubjectContainsWords @("Override") -StopRuleProcessing:$False -Mode Enforce
-Comments "Protect Board Information when circulated" -RuleErrorAction Ignore
-SenderAddressLocation Header
```

Another example is where you want to protect messages that contain sensitive information types such as credit card numbers. A wide range of default sensitive information types are available for use in DLP policies, and you can define custom sensitive information types if necessary. A mail flow rule can use any sensitive information type to identify messages for protection by including it in the *MessageContainsDataClassifications*

parameter. Here's a simple PowerShell example that looks for six different sensitive information types. If any are found in a message, Exchange Online applies the Encrypt template.

```
New-TransportRule -Name "Encrypt external email with PII content" -SentToScope NotInOrganization -ApplyRightsProtectionTemplate "Encrypt" -MessageContainsDataClassifications @(@{Name="ABA Routing Number"; minCount="1"},@{Name="Credit Card Number"; minCount="1"},@{Name="U.S. / U.K. Passport Number"; minCount="1"},@{Name="U.S. Bank Account Number"; minCount="1"},@{Name="U.S. Individual Taxpayer Identification Number (ITIN)"; minCount="1"},@{Name="U.S. Social Security Number (SSN)"; minCount="1"}) -Mode Enforce
```

Alternatively, you can create a DLP policy that applies a template when messages are shared outside the organization. Two steps are needed to do this with PowerShell. The first creates a DLP policy; the second creates the rule to encrypt email with the same set of sensitive information types specified for the mail flow rule and attaches the rule to the policy.

```
New-DlpCompliancePolicy -Name "Encrypt external sensitive mail" -ExchangeLocation "A11"

New-DlpComplianceRule -Name "Encrypt external email with PII content" -Policy "Encrypt external sensitive mail" -AccessScope NotInOrganization -EncryptRMSTemplate "Encrypt" -NotifyUser "LastModifier" -NotifyPolicyTipCustomText "This email contains sensitive PII information and will be encrypted when sent." -NotifyEmailCustomText "This email contains sensitive PII information and will be encrypted when sent." -ContentContainsSensitiveInformation @(@{Name="ABA Routing Number"; minCount="1"},@{Name="Credit Card Number"; minCount="1"},@{Name="U.S. / U.K. Passport Number"; minCount="1"},@{Name="U.S. Bank Account Number"; minCount="1"},@{Name="U.S. Individual Taxpayer Identification Number (ITIN)"; minCount="1"},@{Name="U.S. Social Security Number (SSN)"; minCount="1"})
```

Several methods are available to apply encryption via policy to outbound email. It's important to choose either mail flow rules or DLP policies to protect sensitive data as it is easy to confuse matters if protection is applied for the same content using multiple methods.

Applying Sensitivity Labels Markings with Mail Flow Rules

If you apply a sensitivity label with encryption to a message using a mail flow rule, it protects the message. However, the rule does not apply any of the visual markings defined in the label to the item. Exchange recognizes the presence of a sensitivity label for a message through the presence of an x-header called *msip_labels*. The value of the header points to the GUID for the sensitivity label. Exchange uses GUIDs instead of text values to allow clients to show label names in local languages. If the *msip_labels* x-header is not present in a message header, clients that understand labels cannot display a label. Therefore, if we want to apply a label to a message, we must do so by adding the label with a client or applying the label with a mail flow rule as the message passes through the transport pipeline. The technique works for outbound messages. It doesn't work for inbound messages.

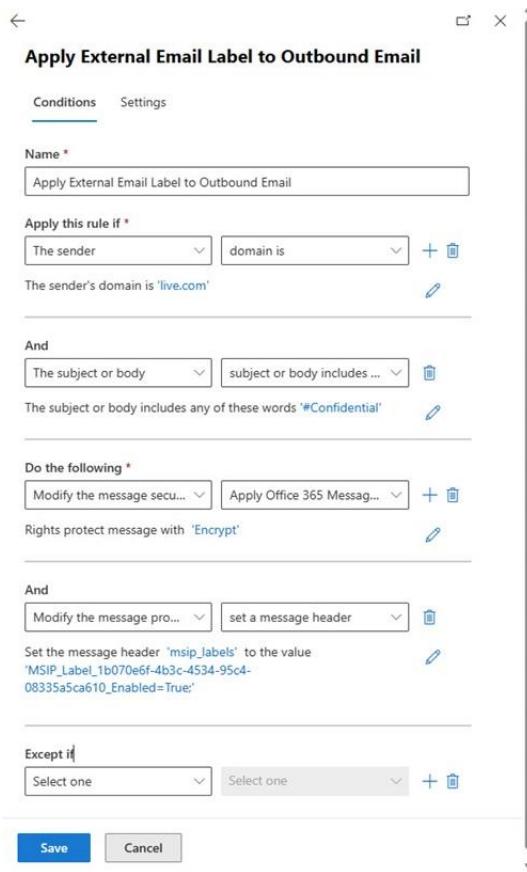


Figure 19-23: Setting a mail flow rule to add the *msip_labels* x-header to a message

Figure 19-23 is an example of applying a label in a mail flow rule. The rule is very simple and does the following:

- If the message subject or body contains the word *#Confidential*, execute the rule. This is an easy way of allowing people who use clients that don't support rights management (like older Mac devices or mobile devices that don't support an application capable of applying labels to items) to have Exchange protect messages. The rule applies to messages sent inside and outside the organization.
- Apply the Encrypt template to protect the message.
- Add *MSIP_Label_1b070e6f-4b3c-4534-95c4-08335a5ca610_Enabled=True*; as the value of the *msip_labels* x-header in the message. The closing semi-colon is important as it terminates the x-header.

A big question for anyone wanting to use a sensitivity label in a mail flow rule is how to find its GUID. The Microsoft Purview Compliance portal doesn't display this information for a sensitivity label, but you can retrieve label GUIDs by running the *Get-Label* cmdlet (see the section covering using PowerShell to manage sensitivity labels). You can combine labels with templates. In other words, even if a label includes protection, you can decide that a mail flow rule should apply an x-header for one label and protect the message with a different template (that isn't associated with a label). If you want to use a sub-label, make sure you use its GUID and not that of the parent label.

Remember that the senders of messages processed by this rule will not see a label or protection on the copy of the message in their Sent Items folder because protection only applies to messages that go through the transport pipeline. If you want to check that the rule works as expected, include your address as a recipient and examine the copy of the message delivered in your Inbox with a client that supports sensitivity labels. You should find the *msip_labels* x-header in the message headers and that the message is both labeled and encrypted. It's also true that the label information will mean nothing to a different email system (or different

tenant) because those systems won't be able to translate the GUID into a label. Protection will still apply even if the label isn't respected, and that is probably the most important thing.

Detecting and Blocking Protected Messages in Mail Flow Rules

We know that protected messages have x-headers holding information about the label applied to protect the content. We can exploit this fact to create a mail flow rule to block messages leaving the organization if their headers include a certain label. In this case, the criteria are:

- Apply to outbound messages.
- Check the *msip_labels* x-header and if the GUID for the label exists, block the message with the action "Reject the message with the explanation." The text for the explanation is up to you but might be something like "You can't send sensitive messages outside the organization."

For example, let's assume that you have a label with a GUID of *ed4411cc-bec4-444a-b279-c404aad79d6*. The text that the mail flow rule should look for in the x-header is:

MSIP_Label_ed4411cc-bec4-444a-b279-c404aad79d6_Enabled=true;

If found, we know that the label protects this message (or one of its attachments), so the rule can go ahead and block the message.

Exchange Online can read the label metadata for messages and Office and PDF attachments. Another complication is that OWA and Outlook mobile clients apply protection to messages using special hidden rules executed as items pass through the Exchange Online transport pipeline. It is more efficient to encrypt messages after the processing of other mail flow rules finish, so the transport service applies encryption to outbound messages after all tenant-specified rules finish. The net effect is that protection (and the x-header) is only present in messages sent by OWA and Outlook mobile after Exchange has processed all the other rules, so the rule described above can only block protected messages sent by Outlook desktop.

Hybrid Protection

In a hybrid deployment, the on-premises Active Directory RMS servers support on-premises mailboxes, and Office 365 supports cloud mailboxes. Automatic synchronization of configuration data, including templates, does not occur. You must:

- Export the trusted publishing domain (TPD) data from your on-premises [RMS servers](#).
- Allow [external access](#) to your on-premises servers.
- [Import the TPD data](#) into Azure RMS.
- Enable any on-premises templates that are in use and make them available to cloud users.

It is desirable to ensure that the same templates are available to both cloud and on-premises users and that they run in the same manner. Because no automatic synchronization exists, any time an administrator updates the configuration for either the on-premises or cloud platforms, you must replicate the change to the other platform.

Protecting Windows Files

An extension for File Explorer (installed with the Information Protection client) allows users to select and apply protection to files in much the same way as they perform other operations like printing. You can protect multiple files and folders in a single operation. To protect a file, you select the file in File Explorer and select **Apply Sensitivity Label with Microsoft Purview** from *Show more options* on the right-click menu. The options exist to merely classify a file or to apply full protection where you specify a list of users who can interact with the file together with the permissions you want to give them.

Labels with preassigned rights cannot be altered. Labels with user-defined rights can be updated to meet the needs of individual circumstances. For convenience, roles like Viewer – View Only and Co-Owner dictate the actions that recipients can take when they receive protected files. You can select recipients from the corporate GAL or input the email addresses for individual recipients, distribution lists, or complete domains. As you can see in Figure 19-24, you can also add an expiration date after which recipients no longer have access to the content.

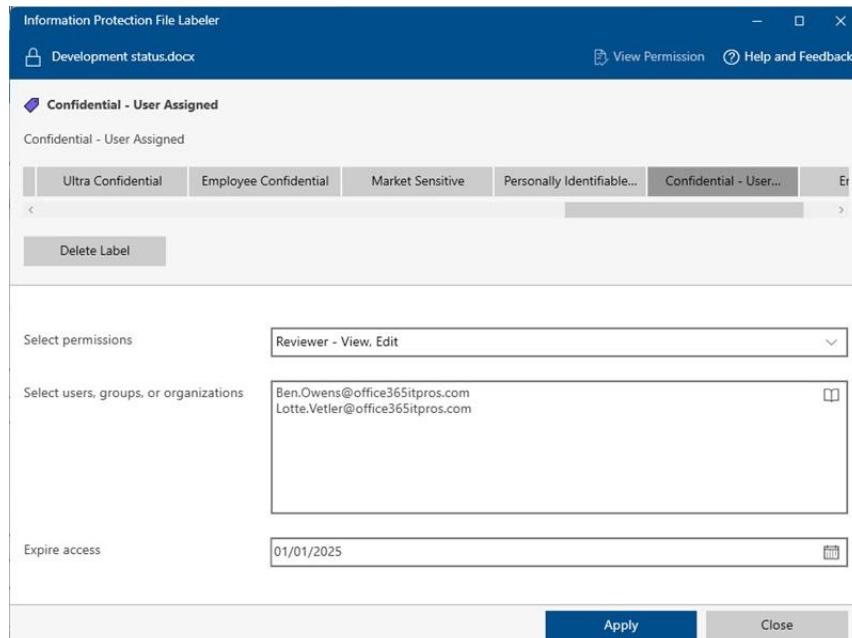


Figure 19-24: Applying a sensitivity label to a Windows file using the Information Protection client

After you protect a file, the client updates its properties to reflect the new protection. In some cases, like Office documents, this is a matter of adjusting the built-in attributes that control access to the file. In others, like JPEG files, the client converts the file into another format (in this case, protected JPEG). After protecting the file, you can share it with anyone you like using whatever mechanism is best. For instance, you can attach the file to a message and send it to someone. The protection placed on files works no matter how users share files, including uploading files to cloud sharing services like DropBox.

If the recipient is on the list of the users specified to access the content, they will be able to open it and interact with the content based on the rights granted by the author. Anyone else will be unable to access the content and told that they need to contact the owner to receive a version of the file that includes them in the permissions list. If the file is in a format supported by an application that supports rights management, the recipient can open and interact with the file in that application. If the file is in a format that is unsupported by enlightened applications or such an application is unavailable, you can download a [lightweight viewer](#) that understands how to interpret the protection placed on the file and open it for viewing.

Disabling the Apply Sensitivity Label with Microsoft Purview option: Some have asked if it is possible to disable the **Apply Sensitivity Label with Microsoft Purview** option so that it doesn't show up in File Explorer. It is possible by creating a new DWORD value called *LegacyDisable* at *HKEY_CLASSES_ROOT\AllFilesystemObjects\shell\Microsoft.Azip.RightClick*. Set the value to 0 (zero) to disable the option. Before doing this, remember that the File Explorer option might be the only way for people to apply sensitivity labels to PDFs and other non-Office file types.

Protected PDFs

[Microsoft and Adobe](#) collaborate to deliver a “native” integration of rights management protection for Adobe PDF documents. Native means that protection applied to PDF files uses the V1.7 of the ISO specification for

PDF encryption. Applications that support the standard can open and process the protected content. Protection is unsupported for signed PDFs because this would break the method used to attest to the validity of the signatures.

Unlike earlier third-party implementations of rights-management protected PDFs, which use a PPDF file extension to show the encrypted nature of the files, native-protected files keep their PDF file extension.

Three options exist to apply Microsoft Information Protection to PDF files:

- The [Information Protection client](#), using the **Apply Sensitivity Label with Microsoft Purview** option in File Explorer to choose a label or to assign custom permissions.
- PowerShell, using the *Set-FileLabel* cmdlet.
- The paid-for version of [Adobe Acrobat](#) supports application, removal, and updating of sensitivity labels to PDFs

Organizations can store protected PDFs in SharePoint Online or OneDrive for Business document libraries, but unless you use the Edge browser, you must download the files and use a supported viewer to view their content as the normal viewer used by SharePoint Online cannot decrypt the files. You can't apply, change, or remove sensitivity labels from PDFs stored in SharePoint Online or OneDrive for Business. Instead, you must download the file and process it with one of the options outlined above, and then upload it again. Because SharePoint Online can't process protected PDFs, sensitivity labels applied to PDFs do not appear in document views.

To access the content of protected PDFs, use a supported reader which understands both the ISO standard and how to display the assigned rights, such as Adobe Acrobat Reader (Microsoft's list of PDF readers that support Information Protection [is available online](#)). To use Acrobat, you need a recent version of Adobe Acrobat Reader or Reader DC and the [Microsoft Information Protection plug-in](#) (the Adobe installer bundles the plug-in). Only Adobe Reader and not the Adobe Acrobat (paid-for) products support access to protected content. To have the Adobe products display information about the label assigned to protected PDFs, it's necessary to have a DWORD *bShowDMB* with a value of 1 at:

HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\MicrosoftAIP

The Edge browser can open PDFs protected with sensitivity labels belonging to any tenant if the user has the appropriate rights.

Generating Protected PDFs from Office Documents

Microsoft 365 enterprise apps (from build 2208 in the general channel and build 2209 in the monthly enterprise channel) create protected PDFs for the following actions:

- File – Save as PDF (unsupported for the PDF/A format).
- File – Export as PDF.
- Share – Send a Copy – PDF.

The Print to PDF option removes sensitivity label protection before it can generate a PDF. Because of this, the apps make the option unavailable if mandatory labeling is in force. In addition, password protection is unsupported for protected PDFs. To disable sensitivity label support for output PDFs, use the Cloud policy service to apply disable the *Use the Sensitivity feature in Office to apply sensitivity labels to PDFs* setting.

The browser versions of the Office apps can also apply sensitivity labels to output PDFs. If the label applies encryption, it must be removed before Office can export the document to PDF.

Protected Office files exported to PDFs by Visual Basic for Applications (VBA) functions also inherit the sensitivity label and protection from the source file.

Managing Sensitivity Labels with PowerShell

To work with sensitivity labels through PowerShell, run the *Connect-IPPSession* cmdlet. When connected, you can create and manage labels used for information protection and container management.

Listing Rights in a Label

The *Get-Label* cmdlet returns the set of sensitivity labels defined in a tenant or the properties of an individual label. If encryption is enabled for a sensitivity label, its link to the underlying rights management template is in an object in the *LabelActions* property with the Type value set to "encrypt." The *LabelActions* property also holds the GUID for the label in the *TemplateId* field. In this example, we use the *Get-Label* cmdlet to fetch the properties of the Black Matter sensitivity label and then extract the rights definitions from its settings.

```
Connect-IPPSession
$Label = Get-Label -Identity "Black Matter"
$Rights = $Null
ForEach ($Action in $Label.LabelActions) {
    $Action = $Action | ConvertFrom-Json
    If ($Action.Type -eq "encrypt") {
        $Rights = $Action.Settings | Where-Object {$_.Value -like "*Identity*"} | Select-Object
-ExpandProperty Value | Convertfrom-Json
    }
}
If ($Rights) { $Rights | Format-List }

Identity : BoardMembers@Office365itpros.com
Rights   : VIEW,VIEWRIGHTSDATA,OBJMODEL,DOCEDIT,EDIT,PRINT,EXTRACT,REPLY,REPLYALL,FORWARD

Identity : Black.Matter.Team@office365itpros.com
Rights   : VIEW,VIEWRIGHTSDATA,OBJMODEL,DOCEDIT,EDIT,REPLY,REPLYALL,FORWARD

Identity : Sanjay.K.Patel@office365itpros.com
Rights   : VIEW,VIEWRIGHTSDATA,OBJMODEL
```

The rights assigned in this label cover two groups and an individual user. The first set of sets equates to the co-author role. The second equates to the reviewer role and the last to the viewer role.

Linking Labels to Parent Labels

As discussed earlier, the compliance portal doesn't support the linking or unlinking of sublabels to parent labels. These operations can be done using the *Set-Label* cmdlet. To begin, find the *ImmutableId* (GUID) for the parent and child labels. This command lists the name and *ImmutableId* for the set of labels:

```
Get-Label | Format-Table Name, ImmutableId
```

After identifying the target parent and child labels, you can run the *Set-Label* cmdlet to connect the two labels using their GUIDs.

```
Set-Label -Identity "969ca0c8-9699-4950-a943-32c1e044b546" -ParentId "d179fcf9-43d4-41b6-9ddb-3e1aaaf3224c8"
```

Updating a regular sensitivity label to become a sublabel changes the priority order of the label. This can lead to [priority mismatches](#) when users apply the sublabel to files stored in SharePoint Online if container management labels are used to manage sites. It's a small point to be aware of.

To disconnect a sublabel from a parent label, run *Set-Label* and set the parent label identifier to \$null. These commands disconnect a sublabel and resets its priority:

```
Set-Label -Identity "969ca0c8-9699-4950-a943-32c1e044b546" -ParentId $null
Set-Label -Identity "969ca0c8-9699-4950-a943-32c1e044b546" -Priority 30
```

Removing Sensitivity Labels from SharePoint Online and OneDrive for Business Files

Global and SharePoint admins can run the *Unlock-SPOSensitivityLabelEncryptedFile* cmdlet to remove sensitivity labels with encryption from documents stored in SharePoint Online document libraries and OneDrive for Business accounts. The cmdlet is in the SharePoint Online module. It can only remove sensitivity labels belonging to the same tenant; it has no effect when run against documents protected by labels originating outside the tenant.

In effect, the unlock cmdlet delivers the same functionality available to rights management super-users when they use the *Set-FileLabel* cmdlet to remove labels from files. Because SharePoint Online stores files protected by sensitivity labels in an unencrypted form (SharePoint applies encryption when users download documents), the cmdlet works by stripping the MIP metadata from documents.

The input parameters to the cmdlet are the full URL for the file and a justification for the removal of the label. These examples remove a label with encryption from files in a SharePoint Online document library and a OneDrive for Business account:

```
Unlock-SPOSensitivityLabelEncryptedFile -Justification "Needed to remove label"
-FileUrl https://office365itpros.sharepoint.com/sites/billing/Shared Documents/Invoice Tracking
2020.xlsx

Unlock-SPOSensitivityLabelEncryptedFile https://office365itpros-
my.sharepoint.com/personal/kim_akers_office365itpros_com/Documents/Planning.docx -Justification
"Needed to remove label from OneDrive files"
```

Some limitations exist. The only sensitivity labels removed by the cmdlet are those which:

- Include encryption using permissions assigned by an administrator (in other words, an administrator defines the rights for the label when creating or editing the label).
- Do not have user-defined permissions.
- Do not use Double-key encryption (DKE – see earlier section).

The unlock cmdlet doesn't do anything when it processes a file without a label or one with a label that doesn't include encryption.

Removing Encryption from All Files in a Folder

The need often exists to remove protection from multiple files. Because it's focused on administrative activities, the SharePoint Online PowerShell module does not contain cmdlets to list files in a folder. Suitable cmdlets are available in the SharePoint PnP module. By combining the two we can:

- Connect to a target site and find all the documents in a target folder.
- Use the *Get-FileSensitivityLabelInfo* cmdlet to check each document for the presence of a sensitivity label with encryption.
- If a sensitivity label with encryption protects a document, remove it using the *Unlock-SPOSensitivityLabelEncryptedFile* cmdlet.

```
$SiteURL = "https://office365itpros.sharepoint.com/sites/BlogsAndProjects"
$FolderURL= "/Shared Documents/Blog Posts"
$UnLocks++
# Connect to PnP using modern authentication
Connect-PnPOnline -Url $SiteURL -Interactive
# Get all documents in the target folder
$FolderItems = Get-PnPFolderItem -FolderSiteRelativeUrl $FolderURL -ItemType File
Write-Host "Checking" $FolderItems.Count "documents to remove sensitivity labels with encryption"
ForEach ($Item in $FolderItems) {
    $ItemPath = $SiteURL+$FolderURL+"/"+$Item.Name
```

```
$ProtectionStatus = Get-FileSensitivityLabelInfo -FileUrl $ItemPath
If ($ProtectionStatus.ProtectionEnabled -eq $True) {
    Write-Host ("Removing {0} from {1}" -f $ProtectionStatus.DisplayName, $Item.Name)
    $UnLocks++
    Unlock-SPOSensitivityLabelEncryptedFile -FileUrl $ItemPath -JustificationText "Administrator removed label"
}
Write-Host "All Done." $Unlocks "documents unlocked"
```

When the cmdlet removes a sensitivity label from a file, SharePoint updates the name of the last user to modify a document to *System Account*. If you want to discover the account which ran the cmdlet to remove a sensitivity label, you should check the audit log to examine the *FileSensitivityLabelRemoved* events captured upon the removal of labels. The justification given by the user is captured in the audit event.

An example script [downloadable from GitHub](#) shows how to use a combination of PowerShell and Graph API calls to achieve better performance when the need exists to download large quantities of documents.

Updating Rights in Sensitivity Labels

The *Set-Label* cmdlet updates label properties. For example, here's how to update the display name, priority, and supported content type for a label:

```
Set-Label -Identity Ultra -DisplayName "Ultra Confidential" -Priority 12 -ContentType Email
```

Another example is to use the *Set-Label* cmdlet to update rights assignments for a label. For instance, this command assigns a single set of rights to a domain and a separate set of rights to all authenticated users:

```
Set-Label -Identity "Ultra Confidential" -EncryptionRightsDefinitions
"quest.com:VIEW,VIEWRIGHTSDATA,DOCEDIT,PRINT; AuthenticatedUsers:
VIEW,VIEWRIGHTSDATA,OBJMODEL,DOCEDIT,EDIT,REPLY,REPLYALL,FORWARD"
```

The important thing to remember here is that if you run *Set-Label* to update the rights defined for a label, you overwrite the existing rights. It's therefore important that you retrieve the existing rights and include them in the set written back to the label. If you don't, anyone with rights to interact with content protected by the label will lose their access. You don't have to add rights for creators of documents and messages as they always have author rights.

The *New-Label* cmdlet is available to create new labels while the *Remove-Label* cmdlet deletes a label. As explained earlier, it's best not to remove a sensitivity label unless you are sure that the users have not applied the label to protect information. Usually, the better course is to remove the label from all label publishing policies to make it inaccessible to users. The label will continue to work but users cannot the label to new content.

Given the complexity of labels, especially those used with encryption, it is usually best to manage day-to-day updates through the Microsoft Purview Compliance portal and use PowerShell for common operations scripted to remove any chance of an error. For example, let's assume that a label protects content shared with partner organizations. You could:

- Maintain the list of partners in an Excel spreadsheet or other file.
- When a new partner is added, import the list of partner organizations from the file.
- Use the list to create rights definitions and add them to the label.

For more information on how to approach creating such a script, see [this article](#).

Once coded and tested, a process like this is invariably faster, more accurate, and less prone to error than performing a manual update through the GUI (it's also less boring). Microsoft Purview captures all use of label cmdlets, like *New-Label*, *Set-Label*, and *Get-Label*, executed through PowerShell or the Microsoft Purview

Compliance portal, in events in the audit log. It is possible to extract and analyze the label usage events with PowerShell to understand who is updating labels in the tenant.

Managing Label Actions for Sensitivity Labels

Purview stores standard label settings in the *LabelActions* property of the label, where we find settings to control actions like encryption, content marking, and the site and group settings in JSON format. The settings stored in *LabelActions* are in the following sections:

- *protectgroup*: Privacy and external user access.
- *protectsite*: Access to SharePoint content from unmanaged devices. Group members can only access documents through online apps using managed devices.
- *protectteams*: Settings for Teams Premium meetings set through meeting templates.
- *encrypt*: Settings to apply rights management encryption.
- *applycontentmarking*: Settings for visual markings (headers and footers) applied to documents and messages.
- *applywatermarking*: Settings to apply watermarking to documents.

To see the settings for a single label, run the *Get-Label* cmdlet and use the *IncludeDetailedLabelActions* parameter:

```
Get-Label -Identity Confidential -IncludeDetailedLabelActions | Select-Object LabelActions | Format-List
```

Given the number and variety of label settings, it can be difficult to interpret the values. To make things easier, create a report of label action settings by:

- Run *Get-Label* to fetch all labels (you don't need to use *IncludeDetailedLabelActions* when fetching all labels).
- Extract the label action settings and convert them from JSON.
- Interpret the settings and write out what you find. Some attention is needed to extract the rights assigned to users, groups, and domains.

Apart from anything else, generating information about label properties allows an organization to store the data as a form of backup. If someone changes a label, it's easy to check what the label properties were beforehand. [This article](#) explains how to create a report detailing sensitivity label settings.

By checking the content type of labels, we can discover the labels that serve different purposes. For instance, here's how to create an array of labels used for container management:

```
[array]$Labels = Get-Label | Where-Object {$_.ContentType -Like "*UnifiedGroup*"}  
$Output = $Labels.DisplayName -Join ", "  
Write-Output ("These labels support container management: {0}:" -f $Output)
```

The same technique can be used to find the set of sensitivity labels used to protect Teams meetings by checking the *ContentType* property for "Teamwork."

Advanced Settings

Standard label settings are the set visible when editing labels in the Compliance portal and are stored in a label's *LabelActions* property. Microsoft uses advanced settings to introduce a new capability for labels or as a way for tenants to manipulate settings that aren't exposed through the Compliance portal. For example, an advanced setting is available to block access to Microsoft content services. Office documents assigned a sensitivity label with this setting don't send information about the content for analysis by Microsoft content services. This stops some features like DLP policy tips and text prediction working, but it's intended as a precise mechanism to stop Microsoft 365 Copilot from processing very confidential documents. The *Set-Label* cmdlet adds the setting to a label:

```
Set-Label -Identity "Market Sensitive" -AdvancedSettings @{BlockContentAnalysisServices="True"}
```

Here's an example of viewing the advanced settings defined for a label:

```
Get-Label -Identity 'Market Sensitive' | Select-Object -ExpandProperty Settings

[tooltip, Information that if it leaked out could compromise our business]
[displayname, Market Sensitive]
[contenttype, File, Email]
[color, #008b8b]
[blockcontentanalysisservices, True]
```

Sometimes, Microsoft moves a setting (like a site's external sharing capability) from the advanced set and adds it as a standard setting available through the Compliance portal. When this happens, the setting moves into the set stored in the *LabelActions* property. The previous advanced setting remains in the label's properties, but the value of the setting in *LabelActions* takes precedence.

Managing Sensitivity Labels for Containers with PowerShell

You can assign sensitivity labels to containers with PowerShell. Remember to use the GUID of a label instead of its display name. To assign a sensitivity label to a Microsoft 365 group, use the *Set-UnifiedGroup* cmdlet:

```
Set-UnifiedGroup -Identity "Banking Team" -SensitivityLabelId "9ec4cb17-1374-4016-a356-25a7de5e411d"
```

Assigning a sensitivity label updates the settings of the group as defined by the label. For instance, if you assign a label that blocks guest access, the group inherits that setting. *Set-UnifiedGroup* won't allow you to assign a sensitivity label to a group unless the group comes within the scope of a label publishing policy containing the label.

The *Set-SPOSite* cmdlet updates the sensitivity label for a SharePoint Online site:

```
Set-SPOSite -Identity "https://office365itpros.sharepoint.com/sites/dunesproject"
-SensitivityLabel "9ec4cb17-1374-4016-a356-25a7de5e411d"
```

In this example, we search for a set of sites and apply the same sensitivity label to each site in the returned set. If you want to apply the sensitivity label to OneDrive for Business sites at the same time, *Get-SPOSite* will find those sites if you use the *-IncludePersonalSite \$True* parameter in the command.

```
$LabelGuid = "27451a5b-5823-4853-bcd4-2204d03ab477"
$Sites = Get-SPOSite -Limit All -Filter "URL -like 'Accounting'"
$Sites | ForEach-Object {Set-SPOSite $_.URL -SensitivityLabel $LabelGuid}
```

Instead of using the *Set-SPOSite* cmdlet to assign a sensitivity label to individual sites and processing multiple sites that way, the *Set-SPOTenant* cmdlet can assign a sensitivity label to every SharePoint Online site in a tenant. This method is faster when the tenant has more than a thousand sites:

```
$Sites | ForEach-Object {Set-SPOTenant $_.url -SensitivityLabel $LabelId }
```

Set-SPOSite does not allow assignment of a sensitivity label unless the target site comes within the scope of a label publishing policy containing the label. The error is silent, and you won't realize that the assignment failed unless you check the site properties afterward.

To remove labels from one site or a set of sites, use the *Set-SPOSite* cmdlet with the *RemoveLabel* parameter. For example, to remove the labels from the sites in the set used above, we'd run the command:

```
$Sites | ForEach-Object {Set-SPOSite $_.URL -RemoveLabel}
```

The *New-UnifiedGroup* and *New-SPOSite* cmdlets support adding a sensitivity label during the creation of a new group or SharePoint site. The *New-Team* and *Set-Team* cmdlets in the Teams PowerShell module do not currently support sensitivity labels, but you can assign a sensitivity label to a team using the *Set-UnifiedGroup*

cmdlet. When administrators assign labels to containers from one of the supported workloads, background synchronization processes make sure that the other workloads pick up the change. Groups used for Viva Engage communities do not currently support sensitivity labels.

The Microsoft Graph Groups API also supports [assignment of sensitivity labels to Groups](#). Apart from the Microsoft Information Protection SDK, no public API is yet available to assign a sensitivity label to individual documents.

Fetching Sensitivity Label Information for SharePoint Sites

To respond faster, when used to fetch a set of site objects, the *Get-SPOSite* cmdlet returns a limited set of properties. Sensitivity labels are not one of these properties, so if you want to find out which sites have labels, you must call *Get-SPOSite* to check each site. For example:

```
$Sites = Get-SPOSite -Limit All -Template Group#0
Foreach ($Site in $Sites) {
    $SiteDetails = Get-SPOSite -Identity $Site.URL
    If ($SiteDetails.SensitivityLabel.length -ne 0) {
        Write-Host "Site" $SiteDetails.Title "has sensitivity label" $SiteDetails.SensitivityLabel }}
```

Updating Site Sharing Permissions

Another advanced setting for sensitivity labels controls the sharing permissions for sites. In the SharePoint browser interface, this option is available through *Site Permissions – Site Sharing*. Three settings are available:

- **MemberShareAll**: Site owners and members can share files, folders, and the site. People with edit permissions can share files and folders. This is usually the default setting assigned to new sites.
- **MemberShareFileAndFolder**: Site owners and members, and people with edit permissions, can share files and folders, but only the site owners can share the site.
- **MemberShareNone**: Only site owners can share files, folders, and the site.

To assign a new site sharing permission, run the *Set-Label* cmdlet and update the *MembersCanShare* advanced setting. For example:

```
Set-Label -Identity 'General Access' -AdvancedSettings @{MembersCanShare='MemberShareFileAndFolder'}
```

The ability to set sharing permissions for sites through sensitivity labels is currently in preview.

Advanced Policy Settings

Management of most sensitivity label policy settings occurs through the Microsoft Purview Compliance portal. The information protection client introduced [advanced policy settings](#) (or “custom configurations”). Over time, Microsoft updated sensitivity label policies to support some of the advanced settings through the GUI or PowerShell. For example, the label policy created earlier defines the default label to be “Public.” We can create a policy setting to force Outlook to use a different label in the GUI or with PowerShell as follows:

```
Set-LabelPolicy -Identity "General Sensitivity Policy" -AdvancedSettings
@{OutlookDefaultLabel="2fe7f66d-096a-469e-835f-595532b63560"}
```

To check the normal and advanced settings for a policy, use the *Get-LabelPolicy* cmdlet as shown below. We can see that Outlook uses a different default label to the default label defined for documents, and that container support is enabled to allow super-users to use the *Set-FileLabel* cmdlet to remove labels from compressed files.

```
(Get-LabelPolicy -Identity "General Sensitivity Policy").Settings
[requiredowngradejustification, true]
[mandatory, true]
[outlookdefaultlabel, 2fe7f66d-096a-469e-835f-595532b63560]
```

```
[defaultlabelid, 27451a5b-5823-4853-bcd4-2204d03ab477]
[siteandgroupmandatory, false]
[enablecontainersupport, True]
[disablemandatoryinoutlook, True]
```

Outlook for Windows, Outlook for Mac, Outlook mobile, and OWA read and respect policy settings for:

- **DisableMandatoryInOutlook:** If the sensitivity label policy dictates mandatory labeling, this setting allows Outlook to avoid the need to assign labels to new messages. Set to False if Outlook should apply mandatory labeling, or True to disable mandatory labeling. Even if you disable mandatory labeling for Outlook, it continues to be mandatory for documents created in Word, PowerPoint, and Excel.
- **OutlookDefaultLabel:** If the sensitivity policy dictates mandatory labeling, this setting allows Outlook clients to use a different default label to the one applied to documents (as defined in the *DefaultLabelId* policy setting). The setting contains the GUID (label identifier) for the default label used by Outlook. Note that if a default label is defined for Outlook and mandatory labeling is required (even if disabled for Outlook), Outlook applies its label to all new messages.

Neither PowerShell nor the compliance endpoint validates the name of the advanced setting you update. If you misspell a parameter, PowerShell writes it into the label policy. If you pass an incorrect value, it will end up in the policy too. Always double-check the values you plan to use before updating a policy.

Controlling Default Sharing Links for Sites and Documents

When someone shares a document or folder, SharePoint Online or OneDrive for Business creates a sharing link. The link set the scope (who can use the link) and permissions (what they can do). The sharing link inherits default settings for the scope and permissions from site settings or the tenant defaults. The default sharing settings can deliver a powerful hint to help people understand the level of confidentiality of information held in a site or individual document by guiding them to a certain mode of sharing. Although users can change a sharing link after SharePoint creates it, they often accept the default settings.

SharePoint administrators can configure the default sharing link settings for sites in the SharePoint admin center or by running the *Set-SPOSite* cmdlet with the *DefaultSharingScope* and *DefaultShareLinkPermission* parameters (which overrides the tenant defaults). This action can also be performed by configuring the advanced settings of a sensitivity label. Even better, the default sharing link settings held in a sensitivity label can apply to:

- **SharePoint Online sites:** Use the sensitivity label for container management and apply it to a site. The site inherits the settings from the label and overwrites any existing site settings. The setting inherited from a sensitivity label takes precedence over the tenant default.
- **Documents:** Apply the sensitivity label to a document. When someone shares the document, the default sharing link settings from the label take precedence over the site setting except when the site settings are more restrictive than the label settings. In that case, SharePoint Online uses the site settings.

Being able to apply default sharing link settings at a document level helps to protect documents stored in a site that should not be shared as widely as permitted by the site settings. For example, you might have a site holding project documents which can be shared with anyone in the organization except for project pricing files which must be restricted to specific people. In this scenario, administrators apply a sensitivity label to the site with a default sharing link settings to allow edit access for anyone in the organization while the pricing documents use a different label whose settings generate sharing links limited to specific people. Being able to control the default sharing link settings through sensitivity labels also helps when users store confidential documents in OneDrive for Business, again because users are likely to accept the default or at least think

more about how they share information if they must adjust the sharing link settings before they share a document.

You update the default sharing link settings for sensitivity labels using the PowerShell *Set-Label* cmdlet. First, connect a PowerShell session to the compliance endpoint. You can then use the *Set-Label* cmdlet to update sensitivity label settings. These settings are available:

- **DefaultSharingScope** defines the scope of the sharing link. The supported values are SpecificPeople, Organization, or Anyone.
- **DefaultShareLinkPermission** controls what a sharing link recipient can do with a file. The two available options are Edit and View.
- **DefaultLinkToExistingAccess** is True or False (default False). If set, this overwrites any other sharing link control and sets the link scope to people who already have access.

You can update default sharing link settings separately or together. For example, these commands set the default sharing scope and permission in two steps:

```
Set-Label -Identity 'Guest Access' -AdvancedSettings @{DefaultSharingScope = "SpecificPeople"}  
Set-Label -Identity 'Guest Access' -AdvancedSettings @{DefaultShareLinkPermission = "Edit"}
```

Or set the two values in one command:

```
Set-Label -Identity 'Non-Business Use' -AdvancedSettings @{DefaultShareLinkPermission = "Edit";  
DefaultSharingScope = "Anyone"}
```

To check the sharing link settings for a sensitivity label, run the *Get-Label* cmdlet. Values only appear for advanced settings after an update:

```
Get-Label "Non-Business Use" | Select-Object -ExpandProperty Settings  
  
[contenttype, Site, UnifiedGroup]  
[tooltip, Site, team, or group holding information that is confidential to the organization but can  
be shared with guest users. Private access.]  
[displayname, Guest Access]  
[defaultsharelinkpermission, Edit]  
[defaultsharingscope, Anyone]
```

To enable *DefaultLinkToExistingAccess*, run:

```
Set-Label -Identity 'Confidential Access' -AdvancedSettings @{DefaultLinkToExistingAccess = "True"}
```

Like any other changes made to sensitivity labels, it can take up to 24 hours before SharePoint Online respects updates to the default sharing link settings.

Locale Settings for Label Names and Tooltips

By default, applications display the name and tooltip defined for a sensitivity label. If you work inside a monolingual organization, this shouldn't cause a problem as the default language is likely the one used by everyone. Inside a multilingual organization, it's a good idea to assign locale-specific values for label names and tooltips. PowerShell is the only supported method to update language values for a sensitivity label. For example, here's how to create a set of locale-dependent display names for the Confidential Access label used for container management. The code does the following:

- Define the label to update.
- Define an array holding the set of supported languages.
- Define an array holding the translated display name for the label in the supported languages.
- Define an array holding the translated tooltips for the label in the supported languages.
- Build JSON structures for the display names and tooltips.
- Run *Set-Label* to update the label settings.

This approach is much easier than the alternative of inputting all the values in one long command.

```
$Label = "Confidential Access"
$Languages = @("en-en", "fr-fr", "it-it", "de-de")
$DisplayNames=@("Confidential Access", "Accès confidentiel", "Accesso riservato", "Vertraulicher Zugang")
$Tooltips = @("Used for corporate confidential information", "Utilisé pour les informations confidentielles de l'entreprise", "Utilizzato per informazioni riservate aziendali", "Wird für vertrauliche Unternehmensinformationen verwendet")
$DisplayNameLocaleSettings = [PSCustomObject]@{LocaleKey='DisplayName';
Settings=@(
@{key=$Languages[0];Value=$DisplayNames[0];}
@{key=$Languages[1];Value=$DisplayNames[1];}
@{key=$Languages[2];Value=$DisplayNames[2];}
@{key=$Languages[3];Value=$DisplayNames[3];})}
$TooltipLocaleSettings = [PSCustomObject]@{LocaleKey='Tooltip';
Settings=@(
@{key=$Languages[0];Value=$Tooltips[0];}
@{key=$Languages[1];Value=$Tooltips[1];}
@{key=$Languages[2];Value=$Tooltips[2];}
@{key=$Languages[3];Value=$Tooltips[3];})}
Set-Label -Identity $Label -LocaleSettings (ConvertTo-Json $DisplayNameLocaleSettings -Depth 3 -Compress),(ConvertTo-Json $TooltipLocaleSettings -Depth 3 -Compress)
```

The key thing is to make sure that the set of language values for the display name matches the set of language values for the tooltips. In the example, both sets have values for default, en-us (U.S. English), French, Italian, and German. If you define a tooltip without a matching display name, the cmdlet will fail to update the label. The length of the tooltips makes them harder to input, so it's wise to compose the command outside PowerShell and paste the code into the console.

A more developed script demonstrating how to use the Microsoft Translator service to generate local language values for sensitivity label display names and tooltips is [described in this article](#).

Setting Label Colors

The Office subscription and online applications support the display of different colors to help users identify labels. Administrators can assign colors to labels through the Microsoft Purview Compliance portal and or PowerShell by running the *Set-Label* cmdlet. For example:

```
Set-Label -Identity "Confidential" -AdvancedSettings @{color="#008b8b"}
```

The *Set-Label* cmdlet accepts the color for a label in a hex triplet code giving the red, green, and blue combination to build the color. The example above assigns the hex code for dark cyan to the label. See [this page to interpret hex color codes](#).

As an example of how to apply colors to sensitivity labels, [this article](#) explains the use of a traffic light system where green labels are safe to share outside the organization, orange labels need some care, and red labels mean content that must remain internal. The script featured in the article is [available from GitHub](#).

Updating Visual Markings

The Purview compliance portal supports the updating of settings for the visual markers (header, footer, and watermark) applied to Office documents. The GUI allows administrators to choose from a limited set of colors for text (black, yellow, blue, green, and red). This example shows how to select a different color along with some other visual marker settings:

```
Set-Label -Identity $LabelId -LabelActions '{
    "Type": "applycontentmarking",
    "SubType": "footer",
    "Settings": [
        {"Key": "fontsize", "Value": "12"},
        {"Key": "placement", "Value": "Footer"},
```

```
{"Key":"alignment","Value":"Center"},  
 {"Key":"text","Value": "*** Confidential Information ***"},  
 {"Key":"fontcolor","Value":"#8b0000"}  
 ]}'
```

Azure Rights Management PowerShell

If you want to manage the protection service with PowerShell, you must download and install the [AIPService PowerShell Module](#) from the PowerShell gallery (or update the module to make sure that you have the latest release). After installing the module, you can connect to the service on an ad-hoc basis or include commands to connect to the service in your PowerShell profile. When you connect to the service, you can run the *Get-AipService* cmdlet to discover if protection is active (enabled) for the tenant. If the service is not enabled, you won't be able to protect information.

```
Import-Module AipService  
Connect-AipService  
  
A connection to the Azure Information Protection service was opened.  
Get-AipService  
Enabled
```

Administrator Role for the AIP Service

Your account must have administrative rights for the rights management service before you can run the *Connect-AipService* cmdlet to connect PowerShell to the service. Accounts have administrative rights if they are:

- A global administrator for the tenant.
- A global administrator for the Azure tenant.
- Granted administrator access with the *Add-AipServiceRoleBasedAdministrator* cmdlet. For example, this command grants administrator access to the Kim Akers account. You'll see an error if the account already holds the role.

```
Add-AipServiceRoleBasedAdministrator -EmailAddress Kim.Akers@Office365itpros.com
```

To check the current list accounts assigned the AIP Service administrator role, run the *Get-AipServiceRoleBasedAdministrator* cmdlet:

```
Get-AipServiceRoleBasedAdministrator | Format-Table DisplayName, Role, EmailAddress  
  
DisplayName Role EmailAddress  
-----  
Kim Akers GlobalAdministrator SMTP:Kim.Akers@office365itpros.com  
Marc Vilas GlobalAdministrator SMTP:Marc.Vigneau@office365itpros.com  
James Ryan GlobalAdministrator smtp:JRyan@Office365itpros.com
```

The latest version of the AIPService module can [use certificate-based authentication](#) to support scenarios like fetching log information for ingestion into SIEM systems.

Super-Users

Super-users are accounts that can decrypt any protected content. On-premises deployments often use super-user permissions to decrypt content to allow examination as messages pass through the Exchange transport service or when they review items following retrieval by eDiscovery searches. Assigning highly privileged access like super-user status is something that needs control, restricted to as few people as possible, and audited to track the use of super-user privileges.

The cloud is a very different environment. It is under Microsoft's control and tenant administrators do not have access to servers and other basic infrastructure elements that they could use to compromise information. Because Office 365 is a locked-down infrastructure, Microsoft runs a different regime where components decrypt protected content automatically. Mail flow rules can access protected content, discovery searches uncover protected content with ease, and journaling generates unencrypted reports. You do not need to nominate any account as a super-user to make any standard functionality in Exchange Online or SharePoint Online work.

A situation might exist where you need to assign super-user status to an account to allow it to access encrypted content. For example, you might recover a set of protected Word documents left by an ex-employee that investigators need to review. Another example is where an eDiscovery search recovers a set of protected documents. Microsoft 365 Search can find protected content, but files remain encrypted when exported in the search results. In both instances, a super-user can decrypt the protected documents. Super-users are even able to decrypt documents if a tenant archives the sensitivity labels used for protection or after a document expires. The only time a super-user is unable to decrypt a document is after the deletion of a template. If the template does not exist, decryption is impossible.

You must enable the super-user feature before you can nominate accounts to be super-users. To enable or disable the super-user feature, first, load the protection cmdlets into a PowerShell session and connect to the rights management service. The set of commands to enable or disable the super-user feature are:

```
Connect-AipService
Enable-AipServiceSuperUserFeature
The super user feature is enabled for the Azure Information Protection service.

Disable-AipServiceSuperUserFeature
The super user feature is disabled for the Azure Information Protection service.
```

After enabling the super-user feature, you can add accounts to the super-user list. The email address that you pass must be valid for a user account belonging to the tenant, including those synchronized from on-premises Active Directory. You can add multiple users at one time, separating each email address with a comma. You'll receive an error if you try to add a user who is already on the super user list.

```
Add-AipServiceSuperUser -EmailAddress Oisin.Johnston@Office365ITPros.com
Oisin.Johnston@Office365ITPros.com was added to the list of super users for the Azure Information Protection service.
```

The other commands used to manage super-users are straightforward. *Get-AipServiceSuperUser* returns a list of the current accounts holding the super-user privilege. Normally this list should be empty and the presence of any account on the list should have justification for the status. To remove an account from the super-user list, run the *Remove-AipServiceSuperUser* command as shown below:

```
Remove-AipServiceSuperUser -EmailAddress Oisin.Johnston@Office365ITPros.com
```

Information Protection logs all additions and removals of super users. You can retrieve this information from the AIP Admin log (but not in the unified audit log). This example shows how to download the admin log for the last seven days.

```
Get-AipServiceAdminLog -Path "C:\Temp\AipAdminLog.log" -FromTime (Get-Date).AddDays(-7)
```

Super-User Group

You can also add a super-user group by running the *Set-AipServiceSuperUserGroup* cmdlet. The address specified must point to a Microsoft 365 group or a mail-enabled security group.

```
Set-AipServiceSuperUserGroup -GroupEmailAddress MIPSuperUsers@Office365itpros.com
```

If you define a super-user group, the members of the group are all considered super-users. If the group is created with the ability to hold Entra ID roles (something that can only be done when a group is created in the Entra admin center), it can be used with Entra ID Privileged Identity Management to assign super-user permission for limited periods to individual group members. In other words, instead of having unrestricted super-user access to any protected content in the tenant, the members of the super-user group can only access content when they receive access for a defined period.

App-Based Super User Permission

The Microsoft Information Protection SDK supports the *Content.SuperUser* permission to allow Graph-based apps access to any protected content in a tenant. Like any other Graph permission, the app must be assigned the permission and consent granted by an administrator before the super user access can be used. See [this page](#) for more information.

Using PowerShell to Protect Files

A set of PowerShell cmdlets is available to protect and apply labels to one or more files through scripting. These cmdlets are only available after installing the information protection client on a Windows workstation. The cmdlets call code in the client to add or remove protection to or from files. Authentication to use the cmdlets is through the account used to sign into the client.

Retrieving Protection Information

The Purview Information Management module drops the old "AIP" prefix for cmdlet names. However, the module includes aliases to allow the old cmdlet names (like *Get-AIPFileStatus*) to work.

The *Get-FileStatus* cmdlet returns protection properties for files, including the label and templates applied to files.

First, let's check for files in a folder that have a label. Note that the cmdlet cannot return the status for a file if it is open in an application.

```
Get-FileStatus -Path "C:\Office 365 for IT Pros - Eighth Edition Files" | Where-Object  
{$_.MainLabelId -ne $Null} | Format-Table FileName, MainLabelName, LabelDate
```

Another example shows how to find files in a folder protected by a specific template.

```
Get-FileStatus -Path "C:\Office 365 for IT Pros - Eighth Edition Files" | Where-Object  
{$_.MainTemplateName -eq "Viewer - View Only"} | Format-Table FileName, MainTemplateName
```

Applying Protection to Files

To apply a label to files, we need to know the GUID used for the label. The easiest way to get this is to capture the label identifier from a file that we know is already assigned that label.

```
$LabelId = (Get-FileStatus "C:\Temp\Important Staff.xlsx").MainLabelId.Guid
```

You can also find the GUID in the *Label ID* property of a label when viewed through the Microsoft Purview Compliance portal or by running the *Get-Label* cmdlet (after connecting to the compliance endpoint):

```
$LabelId = (Get-Label -Identity "Secret").GUID
```

We can now use the label identifier to apply the same label to one or more files. In this case, we look for all Word documents in a folder and its subfolders that do not yet have a label and apply the selected label to those files.

```
$TargetLocation = "c:\Temp\"  
$TargetFiles = "*.docx"  
$Files = (Get-ChildItem ($TargetLocation + $TargetFiles) -File -Recurse)  
ForEach ($F in $Files) {  
    $FileName = $TargetLocation + $F.Name
```

```
$FileStatus = (Get-FileStatus -Path $FileName)
If ($FileStatus.IsLabeled -eq $False) {
    Set-FileLabel -Path $FileName -Label $LabelId
}
```

Applying a label to a file updates the file and it can take several seconds to process a file. Be careful when you apply labels to a folder holding many files.

Reporting Labeled Files

We can use the same technique to generate a report about the labeled and protected files in a folder, including folders holding synchronized files from a SharePoint Online or OneDrive for Business library. This code looks for any Office documents in a folder and then checks each file for the presence of a label. If a label is found, we extract details of the label and any associated rights management template. Note that the *Get-RMSTemplate* cmdlet is available after connecting to Exchange Online.

```
$Report = [System.Collections.Generic.List[Object]]::new() # Create output file for report
$Files = (Get-ChildItem "c:\temp\" -Include *.docx, *.xlsx, *.pptx -Recurse)
ForEach ($F in $Files) {
    $FileName = "c:\temp\"+ $F.Name
    $TemplateName = $Null
    $Status = (Get-FileStatus -Path $FileName)
    If ($Status.IsLabeled -ne $False) {
        If ($Status.RmsTemplateId -ne $Null) {
            $TemplateId = [GUID]($Status.RMSTemplateId)
            $TemplateName = (Get-RMSTemplate -Identity $TemplateId.Guid -ErrorAction
SilentlyContinue).Name
            If ($TemplateName -eq $Null) {$TemplateName = $Status.MainLabelName }
        }
        $ReportLine = [PSCustomObject]@{
            File      = $F.Name
            IsLabeled = $Status.IsLabeled
            LabelId   = $Status.MainLabelId
            Label     = $Status.MainLabelName
            Date      = Get-Date($Status.LabelDate) -format g
            RMSGuid   = $Status.RMSTemplateId
            RMSTemplate = $TemplateName
            Owner     = $Status.RMSOwner }
        $Report.Add($ReportLine)}
    }
$Report | Export-Csv -NoTypeInformation c:\Temp\LabeledFiles.csv
```

The output for an individual file that has a sensitivity label with protection is:

```
File      : ABPs and Teams.docx
IsLabeled : True
LabelId   : 81955691-b8e8-4a81-b7b4-ab32b130bfff5
Label     : Secret
Date      : 13 Nov 2018 12:29:42
RMSGuid   : c7fc2174-097c-4123-9cad-15f1a32cb145
RMSTemplate : Secret
Owner     : Tony.Redmond@office365itpros.com
```

After processing the files, the script writes the information collected into a CSV file that can be opened and analyzed with Excel or Power BI.

Removing Labels

To remove a sensitivity label from a document, run the *Set-FileLabel* cmdlet and specify the *RemoveLabel* parameter. You must also give a reason for the removal of the label. This command only works when:

- The logged-in account is an AIP super user.
- The target file is not open in any other application.

- The information protection client is installed on the PC. If you don't install the client, the Purview Information Management module will not load with the AIP Service module, and you can't run the *Set-FileLabel* cmdlet.

For example:

```
Set-FileLabel "C:\Temp\Important Stuff.docx" -RemoveLabel -JustificationMessage "Label no longer necessary"
```

Before a super-user can run the *Set-FileLabel* cmdlet to remove protection from compressed containers like PST, MSG, ZIP, or RAR files, you must update the advanced settings of the label policy which applies to the super-user account to enable container support. This command is an example of enabling container support for a label policy:

```
Set-LabelPolicy -Identity "General Sensitivity Policy" -AdvancedSettings @{EnableContainerSupport="True"}
```

The *Set-FileLabel* cmdlet only works against items protected with Microsoft Information Protection encryption. It doesn't work against items messages protected with S/MIME, even if a sensitivity label applies S/MIME to an item.

Processing Protected Documents Found in Content Searches

As an example of how to use the PowerShell cmdlets, let's assume that your organization must respond to a GDPR Data Subject Request (DSR). The Microsoft Purview Compliance portal can create and process DSRs. In this context, a DSR is a special form of eDiscovery case that depends on one or more content searches to find information relating to a named individual (the data subject). To satisfy a DSR, we need to find all content relating to a data subject. Protected messages in Exchange Online mailboxes are decrypted when exported by a content search; protected documents stored in SharePoint Online and OneDrive for Business libraries are not.

Before the organization can deliver copies of documents found by searches to the data subject, someone must review the content to make sure that the documents are related to that person. This means that protected documents found by searches must be decrypted to allow the check to proceed. In addition, there's no point in giving someone a set of protected documents that they cannot read.

A content search can export protected documents. When you export the results, you nominate a target folder to receive copies of the found files. Under the target folder, a folder (named after the date and time of the search) holds the search results, including the export summary, manifest, and a folder called SharePoint. Inside the SharePoint folder are folders for each site where the search found items and folders navigating to the point in the site where the search found the content. The path to such a folder might be something like this:

```
C:\Temp\Search for documents_Export\06.05.2018-1106AM\SharePoint\GDPR Planning Mark II\gdprplanningmarkii\Shared Documents\General
```

The best approach is to gather all the protected documents found by a search in a single folder and process them there. The method used is to examine each file in the target folder and remove the protection if it exists. In this example, after running the *Connect-AIPService* cmdlet to connect to the rights management service with an account granted super user permission, we can form a collection of the files in the target folder and then loop through the set to find any that are protected. We then use the *Set-FileLabel* cmdlet to remove the protection.

```
$TargetFolder = "C:\Temp\Search for documents_Export\06.05.2018-1106AM\SharePoint\GDPR Planning Mark II\gdprplanningmarkii\Shared Documents\General"
$Documents = Get-ChildItem -File $TargetFolder
ForEach ($D in $Documents) {
    $ProtectStatus = Get-FileStatus -Path $D.FullName
```

```
If ($ProtectStatus.RMSTemplateId -ne $Null) {  
    Write-Host $D.Name "is protected with" $ProtectStatus.RMSTemplateName  
    $Message = $ProtectStatus.RMSTemplateName + " removed for GDPR DSR"  
    Set-FileLabel -Path $D.FullName -RemoveLabel -JustificationMessage $Message }  
}
```

The output is something like:

```
APC123.docx is protected with Intellectual Property  
SPO Protected Content Test.docx is protected with Patent Submission  
  
FileName  
-----  
C:\Temp\Search for documents_Export\06.05.2018-1106AM\SharePoint\GDPR Planning Mark  
II\gdprplanningmarkii\Shared Documents\General...  
C:\Temp\Search for documents_Export\06.05.2018-1106AM\SharePoint\GDPR Planning Mark  
II\gdprplanningmarkii\Shared Documents\General...
```

When all the protected files are unprotected, investigators can review the document content to decide whether to release files as part of the response to the DSR. The same problem of how to deal with protected documents exists for any content search. Remember to remove the account from the list of super users after completing the decryptions.

Using Microsoft Defender for Cloud Apps to Protect Office 365 Content

[Microsoft Defender for Cloud Apps](#) (MDCA) is a cloud access security broker (CASB) that can ingest and act upon [Office 365 audit information](#). The current set of supported apps includes:

- SharePoint Online.
- OneDrive for Business.
- Exchange Online.
- Teams.
- Dynamics 365.

MDCA is designed to give administrators insight into security-related events for a tenant. Given the number of events that even a small tenant can generate, automation through policies that act when specific criteria are matched is the best way to manage common conditions. For example, what action should happen when someone shares a file outside the tenant or creates a new document in a confidential site. If [Azure Information Protection is integrated with MDCA](#), MDCA retrieves the list of available labels in the tenant hourly, and adding a protection label to Office documents and PDF files is a supported action. Using this capability means that you can automatically apply protection to files matching policy criteria as users interact with them. On the basis that it should not override a decision made by a user, MDCA only applies a label if protection doesn't already exist on a file.

MDCA does not apply protection as users add files to Office 365. Instead, as MDCA ingests events from the audit log, it looks for events (like document creation or modification) matching the criteria set in its policies and applies labels as necessary. The elapsed time between something happening a workload and a response occurring in MDCA depends on the ingestion of events from the audit log and the processing of those events in MDCA queues. Depending on the load on the service, the exact time will vary. For example, it might take between ten and twenty minutes before MDCA applies a label to a new file created in a SharePoint document library. If needed to protect an important file overlooked by a policy, an administrator can apply a label to a file from the MDCA dashboard.

The actions taken by MDCA to label files are visible in the Investigate section of its dashboard. You can apply filters to create queries to identify activity for specific applications, users, data ranges, and so on.

MDCA isn't free, but if you are concerned about protecting confidential Office documents stored in SharePoint Online or OneDrive for Business, it's hard to ignore the advantages of using policy-driven application of protection to sensitive content. You could take the manual approach and rely on individual users to do the right thing to protect their documents, but policy-driven automation invariably delivers a more reliable outcome.

Microsoft Information Protection Auditing

Taking the necessary steps to make protection available to users is one step. Knowing that people use technology to protect important content is another. Microsoft Information Protection captures a wide range of audit data covering [most protection activities](#), such as someone applying a sensitivity label to a document or reading a protected document (but not protected messages). In addition, using the [AIP Scanner](#) generates some discovery actions when it scans sources to find files. Administrators can access the audit data through:

- The Activity Explorer in the Microsoft 365 admin center.
- The Audit feature in the Microsoft 365 admin center.
- The PowerShell `Search-UnifiedAuditLog` cmdlet.

The audit log ingests events for sensitivity labels with the other events generated by workloads. See the Auditing and Reporting chapter for information about how to retrieve and analyze data from the audit log. A [script downloadable from GitHub](#) illustrates how to interpret the content of the events logged for sensitivity label actions.

Audit Records Captured for Office Applications

When users assign, remove, or change sensitivity labels to documents using the Office (Word, PowerPoint, and Excel) apps, Microsoft Information Protection captures events for these actions. The events are:

- **SensitivityLabelApplied:** A site owner or administrator applies a sensitivity label to a SharePoint site.
- **FileSensitivityLabelApplied:** A user applies a sensitivity label to an Office document.
- **FileSensitivityLabelChanged:** A user changed a sensitivity label (upgrade or downgrade) for an Office document.
- **FileSensitivityLabelRemoved:** A user removed a label sensitivity from an Office document (in an app or with PowerShell).
- **DocumentSensitivityMismatchDetected:** A mismatch occurs because the sensitivity label applied to a document is higher than the level of sensitivity of the label applied to the site. The SHAREPOINT\system account generates the event when it detects the mismatch for a new or edited document. The audit record generated for a document mismatch does not contain any detail about the user who caused the mismatch to occur. [You can use PowerShell](#) to fetch this information from the audit record captured when the user modified or uploaded the document.

The desktop versions of Word, Excel, and PowerPoint generate a different set of events:

- **SensitivityLabelApplied:** A user applies a sensitivity label to an Office document. This event differs from that logged for a site because its record type is *SensitivityLabelAction* rather than *SharePoint*.
- **SensitivityLabeledFileOpened:** A user opens a protected Office document on a workstation.
- **SensitivityLabeledFileRenamed:** A user generates a new version of a protected Office document by renaming the file.
- **SensitivityLabelRemoved:** A user removes a sensitivity label from an Office document. Office 365 also captures this event when a user edits a labeled file stored on a local device (not a copy synchronized by OneDrive).

Outlook desktop clients generate a *MIPLabel* event when a user applies a sensitivity label to a message. You will also see *SensitivityLabelApplied* events generated when Outlook sends protected messages. Exchange

Online generates the *MIPLabel* event when the transport service processes the protected message; the same happens when a mobile client sends a protected message. The *MIPLabel* event contains more complete data about the message, including recipient names and subject. When analyzing the usage of sensitivity labels in email, you can ignore the *SensitivityLabelApplied* events and focus on the *MIPLabel* events instead. See [this article](#) for an example of how to analyze the audit records captured for sensitivity label events.

In addition, the audit log does not capture events when third-party applications apply sensitivity labels to non-Office documents.

Track that document! Protected documents usually hold some form of confidential information, and it is good to know who has access to that information and to be able to revoke access if needed. To meet this need, users can track the progress of protected documents by signing into the [document tracking site](#). The ability to track documents is a premium feature (tracking of email messages is unsupported). For more information, see [this page](#). This feature will become more interesting when it is integrated into the Microsoft Purview Compliance portal. Microsoft hasn't said when this will happen.

Cloud Exit for Encrypted Content

A "cloud exit" is when an organization decides to move some or all its content from a cloud service to some other platform. The other platform could be on-premises or another cloud service. An organization might need to perform a cloud exit after deciding to move all processing back to on-premises servers, to a competing service like Google Workspace, or even temporarily to regain access to content during a major outage. Tenant-to-tenant migrations also need to process protected content before moving data from the source to the target tenant to make sure that users can continue to access the content after they receive new user principal names in that tenant. The bottom line is that when organizations use rights management to protect content move to a new platform, they must do some up-front preparatory work to be able to move protected content to the target platform and maintain access. This often involves the decryption of large numbers of items.

The cloud exit process differs depending on if you use a Microsoft managed key (MMK) or have a company-owned encryption key (HYOK), and is described in [this post by the Information Protection team](#). The majority of Office 365 tenants that use MIP do so with an MMK. To move back on-premises, these organizations must export the keys (TPD) and then import them into an Active Directory rights management server before they can transfer and decrypt the protected content. This is not an operation that happens overnight, so it's necessary to do some up-front planning and preparation. It's also wise to export your tenant keys so that you always have access to this data should a problem arise.

In scenarios where organizations need to decrypt protected content before moving to a new platform, they can use the following approaches to decrypt information stored in Exchange Online, SharePoint Online, and OneDrive for Business:

- The *Set-FileLabel* PowerShell cmdlet from the Purview Information Management module together with a super-user account to remove labels from files.
- The *Unlock-SPOSensitivityLabelEncryptedFile* and a SharePoint administrator account to remove labels from files stored in SharePoint Online or OneDrive for Business. See [this article](#) for an example.
- A content search to find and export protected Exchange Online messages (including protected attachments). Microsoft Purview eDiscovery (standard) decrypts the messages (including some attachments) during the export process and generate a separate PST for each mailbox.
- Microsoft Purview eDiscovery (premium) can find and export protected Office documents stored in SharePoint Online and OneDrive for Business. See the earlier discussion.

None of these methods are fast, especially when tens of thousands of items are involved. They can only deal with content protected by Microsoft encryption technology (sensitivity labels and OME) and not with any other third-party encryption mechanism.

Temporary cloud exits might be necessary to access protected content in the case of an outage. For instance, if you use a third-party backup service to copy Exchange Online mailboxes, then restoring mailboxes to a usable state requires the decryption of any protected messages. Without access to a rights management server and the tenant keys, it might be possible to restore the mailbox but none of the protected content is accessible.

Chapter 20: Managing Auditing and Reporting

Tony Redmond

Microsoft 365 gathers audit information from workloads about user and system actions to track the interaction with workloads to add, update, and remove data. This chapter reviews how the audit system gathers audit events from multiple workloads into one repository for administrators to query in multiple ways. Apart from the native tools, other Microsoft products like Office 365 Cloud App Security and Microsoft Sentinel consume audit data, and many organizations export the audit data to SIEM repositories for analysis and reporting by ISV products. We also consider the question of how best to generate reports about user activity and consider the value delivered by the reports included in Microsoft 365 and third-party reporting solutions.

Microsoft 365 Audit Framework

The ability to reliably audit user and administrative operations is an important part of any compliance strategy. Although it is easy to enable auditing for a single workload, creating a common infrastructure to process and store auditing data from many different workloads is more challenging. This is especially true as lines blur between workloads when applications such as Groups, Teams, and Planner integrate components and data from multiple workloads.

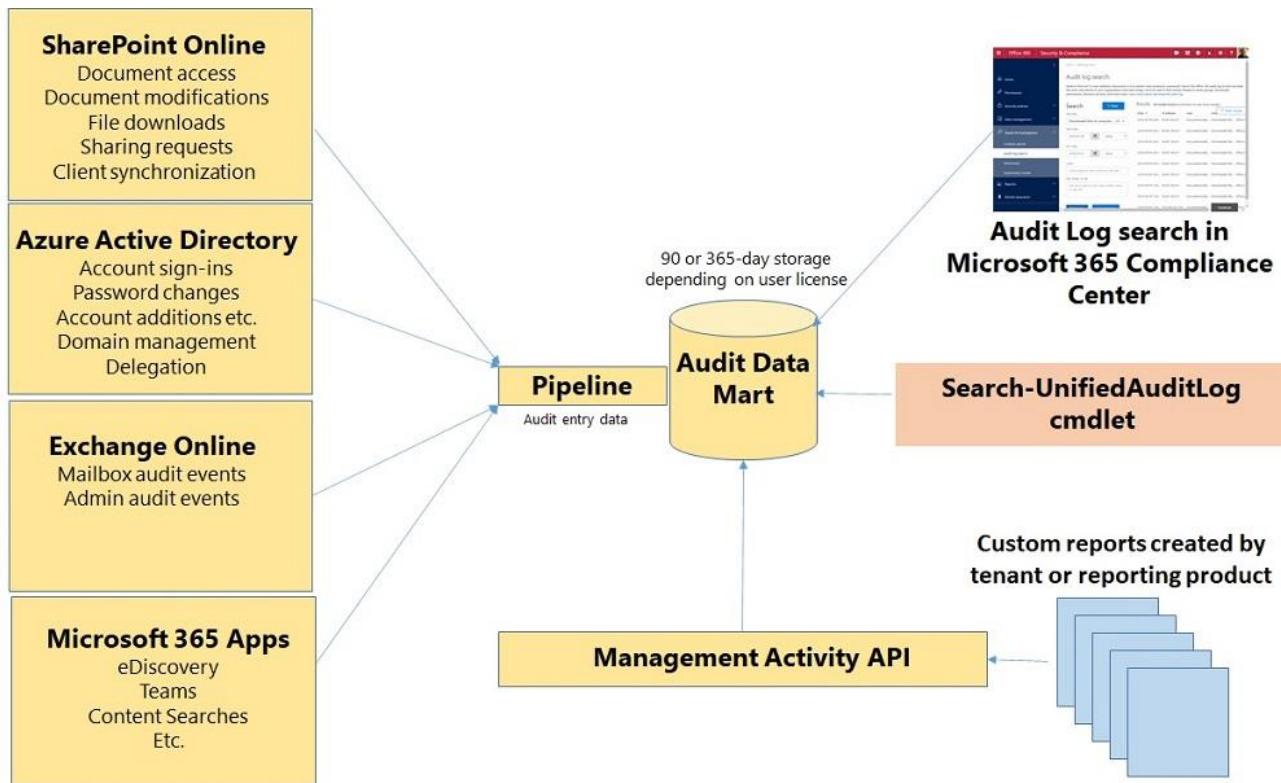


Figure 20-1: Auditing Framework

The background and history of the on-premises Exchange and SharePoint server applications is that each had a different method to enable and control auditing, specific ideas about what audit data to capture, and how

to store audit data. Applications also implemented different methods to control access to the audit data. The result is a mess of inconsistencies and no way to ensure audit information remains secure and immutable. Microsoft 365 solves the problem by using a common auditing framework covering all workloads in the suite. The architecture of the auditing framework in Figure 20-1 includes:

- **Data feeds flow from multiple workloads.** Each workload has varying abilities to capture audit data. It is therefore important to normalize the data retrieved from multiple workloads so that the audit events exist in a consistent format. As the audit log (a set of special mailboxes managed by Exchange Online storage) ingests audit events, the ingestion process applies a [common schema](#) to events recorded in different workloads to make sure that all the events include a consistent set of essential information such as a timestamp, the user identity, the client IP address, client type, the action taken, and the object accessed. Events flow into the audit log from many workloads, including Exchange Online, SharePoint Online (including OneDrive for Business), and Entra ID as well as applications like Stream, Teams, and Planner. The audit log also captures administrative functions such as eDiscovery operations. The schema accommodates the need for applications to capture information specific to their activities through product-specific schemas built on top of the common schema. For example, SharePoint Online supports product-specific schemas to describe file operations and sharing events. See [properties of audit log entries](#) for more information. Microsoft 365 tenants generate billions of audit events daily. In November 2023, Microsoft said that users create 2.3 billion documents in SharePoint Online daily. The actions to create and edit those documents generate billions of audit events.
- **The Audit log ingests and stores events from the data feeds.** The retention period for events stored in the audit log depends on the Microsoft Purview Audit license assigned to user accounts. This license is included in products like Office 365 E3 and Microsoft 365 E3.
 - **Microsoft Purview Audit (Standard):** From October 2023, the retention period for audit events is 180 days (beforehand, it was 90 days).
 - **Microsoft Purview Audit (Premium) or the Microsoft 365 E5 Advanced Compliance add-on:** 365 days for Exchange, SharePoint, and Entra ID audit data.
- Office 365 Cloud App Security downloads audit data into a separate store and retains the events for 180 days. If you need to keep audit data for a longer period, you can extract and store audit data in third-party repositories. The data mart is immutable because administrators cannot remove or change audit records. The data mart must ingest audit entries before records are accessible for reporting purposes. This usually happens within an hour or so but can take longer, depending on the source workload, other activities running within the service, and system events such as software updates. For this reason, the view of audit data is more precise when working with data a day or so after events occur than it is in the short term.
- **Access methods** are available to consume the audit data:
 - The Audit log search (described below) in the Audit section of the Microsoft Purview Compliance portal. The log search supports ad-hoc queries through a GUI with the ability to export discovered records to a CSV file for later examination.
 - The Exchange Online *Search-UnifiedAuditLog* cmdlet can search the audit data from PowerShell.
 - The [AuditLog Query API](#) creates and runs search queries to retrieve audit log records asynchronously using the same approach as the Audit log search in the Purview compliance portal. [This script](#) demonstrates how to use the API with the Microsoft Graph PowerShell SDK.
 - Microsoft Defender for Cloud Apps consumes audit events. See the later section. Other Office 365 features, such as activity alerts, also depend on audit events.
 - The [Office 365 Management Activity API](#) is available to developers to build third-party tools for audit reporting or analysis (or to extract data for injection into a different audit store – [a](#))

([GitHub example is available](#)). The Management Activity API is a REST-based web service. The API aggregates actions and events drawn from the source workloads into tenant-specific content blobs, classified by their type and the content they hold (such as Exchange Online, SharePoint Online, or Entra ID). Tenants can use the Management Activity API to build customized audit analysis tools to handle situations where PowerShell is unviable, as in the case of large-scale tenants where the number of audit records generated daily is too high for PowerShell to process. In these scenarios, the AuditLog Query API is a better answer.

In a multi-geo scenario, some audit data might not be available as expected. For example, if a user has permission to send an email by impersonating another user and the accounts are hosted by different data center regions, Exchange Online captures the *SendAs* audit event in the sender's region but not in the region hosting the mailbox.

Microsoft 365 workloads generating audit events: The intention is that audit events should be available and reportable from all workloads. The full set of auditable events is [documented online](#) and includes:

- Exchange Online administrative events.
- Exchange Online mailbox events such as when mailbox delegates send messages (only for user and shared mailboxes, and not for public folder, resource, or group mailboxes). These events only appear for mailboxes enabled for auditing (the default in Exchange Online).
- Microsoft 365 Groups (created and updated by many different applications). These events appear under the Entra ID workload.
- SharePoint Online and OneDrive for Business file and folder events.
- SharePoint Online and OneDrive for Business site administration events.
- Entra ID events (like the creation of user accounts and groups, account logins and failed login attempts).
- eDiscovery (events like creating or running a content search), including the use of cmdlets to perform searches and other eDiscovery activities.
- Power BI (see instructions on [how to enable auditing for Power BI](#)).
- Microsoft Information Protection, such as the application of Sensitivity labels to documents.
- Teams, including the creation and removal of teams, channels, connectors, and tabs plus membership management.
- Power Automate (Flow), including the creation and deletion of flows and assignment of permissions.
- Stream, including the creation, removal, and editing of videos, channel activities, uploading and sharing of videos, and even when someone likes a video.
- Threat Intelligence (on the detection of phishing email or malware).
- Office 365 Cloud App Security alerts.

Extra information about Entra ID audit events is available from the Entra admin center. Not all Entra ID events flow through to the unified audit log. For instance, if you need to investigate failed or suspicious logins, more data is available through the [Entra admin center](#). Audit events for Planner, To Do, and Project are available in tenants with the Purview Audit Premium licenses.

Some consider that the gathering of audit data from multiple workloads constitutes a Security Incident Event Management (SIEM) or Cloud Access Security Broker (CASB) capability. Closer analysis reveals that the Microsoft 365 auditing system lacks the analysis and investigation features typically found in SIEM or CASB products like Microsoft Sentinel, or available in Microsoft Defender for Cloud Apps. The big advantage Microsoft 365 auditing has over third-party products is the way that the various workloads integrate the generation of audit events into their operations. Many tenants leverage this capability by ingesting audit events into a SIEM for long-term storage and analysis.

The gathering of information from multiple sources following a common format makes the audit log a critical resource for anyone who wants to find out what happens inside a tenant. Along with Entra ID sign-in records

and the Entra ID audit log, the audit log is a prime asset for forensic investigations, as [noted in this blog](#) by Microsoft DART (cybersecurity response team).

Enabling Auditing for a Tenant

The audit log collects events generated by user and system activity from workloads on an ongoing basis.

Before you can search for events in the audit log, you must make sure that event ingestion is working.

[Microsoft enables auditing for new tenants with appropriate licenses](#) (Office 365 E3 or better), but it's possible that it is not working in older tenants or if an administrator disabled auditing in the past.

The easiest way to enable auditing is by running the *Set-AdminAuditLogConfig* cmdlet from the Exchange Online PowerShell module:

```
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $True
```

The first time you run this command in a tenant, the substrate creates the audit log store to allow the ingestion of audit events to commence. You only need to run the command thereafter if someone pauses the audit log and you wish to reenable it. You cannot pause the audit log through the Compliance portal, but you can do it with PowerShell:

```
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $False
```

Pausing the audit log allows workloads to capture events, but the events don't show up in the audit log until an administrator releases the pause. When that happens, the flow of events resumes populating the audit log. It might take some time before events flow from all workloads and the ingestion of events into the log stabilizes. During this time, some events might not reach the audit log.

Multi-geo audit searches: Exchange Online stores mailbox audit records in user mailboxes. For this reason, if you perform mailbox log searches with PowerShell for multi-geo organizations, make sure that you "anchor" the search in a region by [connecting to a mailbox in the target region](#). To create results from multiple regions, you can combine the events found in each region into a single array.

Searching Audit Events

When a tenant is enabled for auditing, events from the different workloads start flowing into the audit log. Workloads use different methods to capture audit events, so it should come as no surprise that events flow into the audit log at different intervals after the workloads capture audit records. Because of the dependency on available service resources, Microsoft doesn't guarantee exactly how long after an event occurred the audit record appears in the audit log. The exact periods ebb and flow with demand and volume, it's normal to experience a delay of between 30 and 90 minutes for core workloads (Exchange Online, SharePoint Online, Entra ID, and Teams). Audit events from other workloads can take longer. The audit log is definitely not a real-time solution and should not be treated as such.

Selecting **Audit** in the Microsoft Purview Compliance portal displays a form to collect the parameters to initiate an audit log search. Figure 20-2 shows the audit search interface. Audit searches run in the background. Up to ten filtered searches can run concurrently (per administrator account), each of which generates a separate set of results. Administrators can see the current set of results while a search is in progress or wait until the search is completed before they export the results for further analysis.

The screenshot shows the 'Audit' search configuration page. At the top, there are tabs for 'New Search' (which is selected) and 'Audit retention policies'. Below the tabs, there are three status indicators: 'Searches completed' (2), 'Active searches' (0), and 'Active unfiltered searches' (0). The main search configuration area includes fields for 'Date and time range (UTC)*' (Start: Mar 01, End: May 23), 'Activities - friendly names' (Choose which activities to search for), 'Users' (Add the users whose audit logs you want to s...), 'Activities - operation names' (MeetingDetail.MeetingParticipantDetail), 'File, folder, or site' (Enter all or a part of the name of a file, websit...), 'Keyword Search' (Enter the keyword to search for), 'Record types' (Select the record types to search for), 'Workloads' (Enter the workloads to search for), 'Admin Units' (Choose which Admin Units to search for), and 'Search name' (Teams Meeting Details). Below these fields are two buttons: 'Search' (highlighted in blue) and 'Clear all'. At the bottom, there is a table showing search results with columns: 'Copy this search', 'Delete', 'Refresh', 'Search name', 'Job status', 'Prog...', 'Searc...', 'Total results', 'Creation tim...', and 'Search performed by'. Two entries are listed: 'Audit Search via cmdlet' (Completed, 100%, 7m, 54s, 1905 items, created May 21, 2024, by tony.redmond@i...), and another entry for 'Audit Search via cmdlet' (Completed, 100%, 7m, 48s, 1902 items, created May 21, 2024, by tony.redmond@i...). A total of 4 items are shown.

Figure 20-2: Configuring an audit search in the Compliance portal

Points to consider about audit searches include:

- Available audit events can be selected from the drop-down **Activities** list. You can combine events from many audit sources in a single search, subject to the 5000-item limit on the number of entries returned by a search. You might find that some operations are not available in the picker but are available in a PowerShell search. This is because it can take time to update the picker after Microsoft adds new events to the ingestion process.
- The date range to use. The default is to search for the last seven days (not including today), but you can go back as 365 days if you have Purview Audit premium licenses. The retrieval limit for audit events for users with Purview Audit standard licenses is 180 days.
- The user or users that performed the action you are looking for. You can leave the **Users** field blank to retrieve data for all users. You can see a list of users, including guest accounts, by entering a couple of characters in the field.
- If searching for SharePoint or OneDrive for Business audit events, you can add supplementary information for the search such as the name of a file, folder, or URL. If you want to search for a word in a document title, give the full word rather than a partial substring. For example, if you want to search for events related to a document called "Reporting and Auditing," a search will find it if you specify "Auditing," but will not for "Audit."
- Search jobs initiated via the GUI do not require the web browser window to remain open to complete. Searches continue to run in the background even after the browser window is closed. Background jobs (search and export) have lower priority than user processing and can take between ten and fifteen minutes to complete.

- Purview stores the results of completed search jobs for 30 days to give administrators the ability to reference historical audit searches. These search jobs are presented in the UI, listing the search name, search job status, progress %, Number of results, Creation Time, and Searched by.
- Filters can be applied against search results to focus on specific events.

After inputting the search criteria, click Search to start.

The usual way to perform an audit search is to start by looking for a specific activity that occurred in a certain time range and then gradually refine the search to focus on a more precise set of events. You can refine the search by specifying the user whose activity you are interested in or a specific file, folder, or site to which an item belongs. You can combine a wide range of activities drawn from different workloads into a single search. Each event that you include in a search will probably increase the number of entries returned from the audit log and might make it more difficult to find the precise information that you want.

The GUI Doesn't Show All: Not every audit record available in the audit log appears in the search results returned in the Compliance portal. This is because the normal operation of Microsoft 365 generates many internal events that might confuse or distract a log search. If you want to see the raw information in the audit log, use the *Search-UnifiedAuditLog* cmdlet.

In Figure 20-3, the results pane shows some *FileModified* events, indicating that the search is for audit records captured when users update files in SharePoint Online document libraries. The number of the records shown for the total result count (1,051 in this instance) is an estimate. The actual total is only revealed if you force the portal to retrieve every record found by the search by advancing page by page until no more records are available. To speed access to the audit data, the portal fetches and displays the first page of 150 events (the most recent entries) and only displays a small number of audit event properties. If the search found more entries, the user prompts by the portal to fetch additional pages by scrolling to the bottom of the list. Although it's possible to examine the details of large data sets of audit records on-screen, you might lose interest in the search by the time you scan through thousands of lines of audit data.

Date (UTC)	IP Address	User	Record type	Activity	Item	Admin Units	Details
7 Mar 2024 23:53	2001:bb6:5f26:8f00...	tony.redmond@	SharePointFileOper...	Modified file	Finding Devices Us...	Global HQ dynamic...	Modified in "Share...
7 Mar 2024 23:46	2001:bb6:5f26:8f00...	tony.redmond@	SharePointFileOper...	FileModifiedExtend...	https://redmondas...	Global HQ dynamic...	
7 Mar 2024 23:46	2001:bb6:5f26:8f00...	tony.redmond@	SharePointFileOper...	Modified file	Finding Devices Us...	Global HQ dynamic...	Modified in "Share...
7 Mar 2024 22:43	51.171.212.123	tony.redmond@	SharePointFileOper...	Modified file	Office 365 for IT Pr...	Global HQ dynamic...	Modified in "Share...
7 Mar 2024 17:22	51.171.212.123	tony.redmond@	SharePointFileOper...	FileModifiedExtend...	https://...	Global HQ dynamic...	
7 Mar 2024 17:22	51.171.212.123	tony.redmond@	SharePointFileOper...	FileModifiedExtend...	https://...	Global HQ dynamic...	
7 Mar 2024 17:21	51.171.212.123	tony.redmond@	SharePointFileOper...	FileModifiedExtend...	https://...	Global HQ dynamic...	
7 Mar 2024 17:21	51.171.212.123	tony.redmond@	SharePointFileOper...	Modified file	23 Managing Tena...	Global HQ dynamic...	Modified in "Share...
7 Mar 2024 17:19	51.171.212.123	tony.redmond@	SharePointFileOper...	FileModifiedExtend...	https://...	Global HQ dynamic...	

Figure 20-3: Viewing the results from an audit log search

Auditing and Secure Score: If auditing is enabled for your tenant, your Microsoft Secure Score goes up by 15 points. Enabling auditing is not sufficient to make a tenant more secure. It's more important to review what's gathered in the audit log regularly to understand what happens in the tenant and be able to detect when something out-of-the-ordinary occurs.

Examining an Audit Record

To see more details of an audit record found in a search, select it from the search results. Purview displays some key information about the event to allow the reader to decide if this relates to an activity that requires further investigation. The information includes:

- **Date:** The timestamp recorded by the originating workload when an event occurred.
- **IP address:** The IP address of the originating client. This can be in IPV4 or IPV6 notation. Some workloads, like the Office Online apps, display the IP address of a trusted application calling into the service instead of the actual address of the device. Admin activities and those performed by system accounts for Entra ID updates don't record IP addresses.
- **User:** The user principal name of the account responsible for the event.
- **Activity:** The registered activity for the event. For example, if someone updates a file in a SharePoint Online document library, the registered activity is "modified file."
- **Item:** A description of the activity.

To expose the extended audit information for an event, click on the event. The information revealed helps you to understand exactly what happened when something performed an action against an object. We will discuss how to retrieve the same information with PowerShell shortly.

User and System Events

It is also important to recognize that both user- and system-initiated operations generate audit events. For example, if offline copies of files from SharePoint Online or OneDrive for Business sites exist on the PC for some reason, a background synchronization process checks the sites periodically to ensure that the local cache holds up-to-date copies of the online files. The synchronization process shows up as a series of "Viewed File", "Accessed File", and "Downloaded File" events and might lead the observer to conclude that the user has accessed many files over a brief period.

Another example of an event that occurs as a by-product of user activity is the Accessed File event logged for the JPEG file for a user's profile photo. It is a fact that someone accessed the file, but it is unlikely that the fact will be important in any sense except in circumstances when you absolutely must prove that someone looked at someone else's profile photo. Examples of system-initiated activity include events recorded for the user "*app@sharepoint*", which relate to background processing of SharePoint and OneDrive sites while those generated by "*NT AUTHORITY\SYSTEM (Microsoft.Exchange.ServiceHost)*" belong to Exchange Online background jobs used to update the organization configuration. For instance, each time a user updates a file in a SharePoint library, you should see a matching *app@sharepoint* event as the crawler re-indexes the updated content. *app@sharepoint* also appears in "Added user or group to SharePoint group" events when users join the membership of a group and that change replicates to the SharePoint group for the team site.

For these reasons, you should take care to restrict the extraction of events to a manageable quantity by using a filter such as a limited time or events for selected users. In addition, you should ask yourself why an event might show up rather than jumping to any conclusions. Microsoft recognizes that the amount of audit data generated by a search can be excessive occasionally and that a filter to separate user-started from system-initiated events might be a sensible future enhancement.

IP addresses in audit records: If you look up the IP addresses reported in audit logs, you might find some that seem to be in unexpected places. The IP address might be for a home router connected to an ISP or it

might be an IP address managed by Microsoft and assigned to one of their data centers. For this reason, products that use IP-based geolocation sometimes report that a connection comes from places that you know the user has never been. For instance, occasionally an audit record pops up to say that I accessed SharePoint Online from Helsinki. Much as I like the Finnish capital, I have not been there for at least 15 years. However, one of Microsoft's EMEA data centers is outside Helsinki and that is where the IP address originated. [Here's an article](#) describing how to use a web-based geolocation service to return information about IPv4 addresses.

Exporting Audit Data

To capture audit data for further analysis, you can export the audit events to a CSV file. To export retrieved items, wait for the search to finish, and then use the **Export** option. After a while, the CSV file is ready to download. The file has a name like `1561b76d-eb92-4089-bc4c-98ebbebba580.CSV`.

The CSV file holds raw audit data. The export process does not expand and format the information about audit events. Instead, the details held in the *AuditData* column are in [JavaScript Object Notation](#) (JSON) format, so further processing is necessary to format the data for easier reading.

The maximum number of audit events that can be exported at one time is 50,000. If you end up downloading 50,000 events to a CSV file, the potential exists that more matching audit events are available that are not in the downloaded set, so it is a good idea to do another search to find events that might be missing (perhaps by using a different date range) and then merge the two sets of results.

Searching Audit Data with PowerShell

The audit log ingests thousands of different events generated by a range of workloads. The `Search-UnifiedAuditLog` cmdlet searches and returns data from the audit log. As we'll see, the cmdlet has some quirks to understand to execute successful searches, especially when it comes to interpreting the content of the *AuditData* property because different workloads insert different types of information into this property.

By default, `Search-UnifiedAuditLog` returns 100 audit records for any search request unless you specify the number of records to retrieve in the *ResultSize* parameter (up to 5,000). A single search can process a maximum of 50,000 audit records using page retrieval (see below). With the increasing number of workloads generating data for the audit log, a casual search can return hundreds if not thousands of records. It is important to be as specific as possible with search parameters to restrict the number of records returned.

Because the `Search-UnifiedAuditLog` cmdlet is an Exchange Online cmdlet, before you can view data in the audit log, your account must hold the Exchange View-Only Audit Logs or Audit Logs role. These roles are part of the Compliance Management and Organization Management role groups and can be assigned to [other role groups](#) as needed.

Running a Simple Audit Search

The simplest form of audit search looks for events of a specific type (referred to as an operation or event) for a single user (referred to as a *UserId*) over a short period. For example, to discover who last updated a document, we can search the audit log with a command like the one shown below:

```
Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-90) -EndDate (Get-Date).AddDays(1)
-RecordType SharePointFileOperation -Operations FileModified, FileModifiedExtended -ObjectIds
"Important File.docx" -ResultSize 5 -Formatted -SessionCommand ReturnLargeSet | Sort-Object Identity
-Unique | Format-Table UserId, CreationDate, Operations
```

UserId	CreationDate	Operations
-----	-----	-----
tony.redmond@office365itpros.com	11/11/2021 14:35:44	FileModified

In this case, we can limit the number of audit records to retrieve by passing precise parameters:

- The **search period**: State the full date and time to delimit the start and end of the search. You can pass a date on its own, in which case the search uses 00:00 as the time to begin (or end) the search. You can specify a start date more than 365 days ago, but the search results only contain events allowed by the Purview Audit licenses assigned to accounts.
- The **object name**: Pass the full name of the document. You don't need to include the URL of the SharePoint Online site or OneDrive for Business account storing the document. Files with the same name can be found in multiple sites, so you might need to check the information stored in the *AuditData* property of the returned audit records to identify records belonging to a specific document. The same is true if you use a partial document name (such as ".docx") and the audit search returns events for modifications made to several documents. Audit searches don't support wildcard matching against object names.
- The **operation**: The action performed to generate the audit event. SharePoint Online generates *FileModified* and *FileModifiedExtended* events (operation) when someone updates a file in a document library. Every audit event has an operation, and you can filter audit records by specifying one or more operations to find.
- The **record type**: By passing *SharePointFileOperation* in the *RecordType* parameter, we tell *Search-UnifiedAuditLog* that we want to retrieve audit records for SharePoint Online file operations like uploading a new file to a document library. The other valid record types [are listed here](#).
- [The *SessionCommand* parameter is present because we are asking for 1,000 records.](#)

The *ResultSize* parameter is set to 5 to tell *Search-UnifiedAuditLog* that it only needs to find the first five records. Because Microsoft 365 usually returns audit records sorted by date, the first record is the latest update. To make sure, the code sorts the returned audit records by the creation date.

If a search finds audit records for multiple documents, a quick way to extract the records for a specific document is to store the found data in an array and then scan the records. For example, this search recovers all document modification events for 90 days.

```
[array]$Records = Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-90) -EndDate (Get-Date).AddDays(1) -RecordType SharePointFileOperation -Operations FileModified, FileModifiedExtended -ObjectIds ".docx" -ResultSize 1000 -Formatted -SessionCommand ReturnLargeSet
$Records = $Records | Sort-Object {$_.CreationDate -as [datetime]} -Descending
```

To scan the records for a specific document, use the *Contains* method to check the contents of the *AuditData* property:

```
[array]$DetailedRecords = $Records | Where-Object {$_._AuditData.Contains("Managing Reporting")}
```

You can also use a free text search against audit records. This is slower than finding records of a certain type and filtering the records to find the right ones but might be helpful at times. Here's an example:

```
[array]$Records = Search-UnifiedAuditLog -FreeText "*Reporting*" -Formatted -StartDate (Get-Date).AddDays(-90) -EndDate (Get-Date).AddDays(1) -ResultSize 1000 -SessionCommand ReturnLargeSet
```

Finding the Right Events: When searching the audit log, it's important to know what you're looking for. This sounds trite but given the number of audit events captured in any reasonably-sized tenant, looking for records for a specific action can be like searching for the proverbial needle in a haystack unless you know the name of the event. A good approach is to take steps to force the workload to generate an audit event, wait for 30 minutes or so, and then run an audit log search for the period to find the events which appear in the audit log. Delaying the search gives Microsoft 365 time to ingest audit records into the log. You can then examine the audit records captured for the period to find the events you want to analyze and use the *Operations* values logged for these events to perform further searches.

Removing Duplicates and Sorting from Retrieved Audit Data

When using the *Search-UnifiedAuditLog* cmdlet to retrieve audit data, consider these points:

- When using the *SessionCommand* parameter, the retrieved data is unsorted. If it's important to have the data sorted in a specific order (for instance, to review audit data in date order), remember to sort the data after retrieval.
- It's possible that Purview will include some duplicate audit records in the set fetched by *Search-UnifiedAuditLog*. Each audit record has a unique identity, so to remove duplicates, sort the data by the *Identity* property to find unique records.

In this example, audit records retrieved by a search are sorted to remove potential duplicates and then by creation date. In a production scenario, the output would contain many more properties extracted from audit records.

```
# Sort fetched audit records to put in date order and remove duplicates.
$Records = $Records | Sort-Object Identity -Unique | Sort-Object {$_.CreationDate -as [datetime]}

# Example of sorting by the audit record identifier
$outputReport = [System.Collections.Generic.List[Object]]::new()
ForEach ($Rec in $Records) {
    $AuditData = $Rec.AuditData | ConvertFrom-JSON
    $ReportLine = [PSCustomObject][Ordered]@{
        UserPrincipalName = $Rec.UserIds
        Timestamp         = $Rec.CreationDate
        Operation         = $Rec.Operations
        Id                = $AuditData.Id
    }
    $outputReport.Add($ReportLine)
}
```

Workload Audit Data

Audit records consist of two parts:

- A set of general properties populated in the same way by all workloads. These properties include the record type, creation date, operation, and user identifier.
- The *AuditData* property contains information specific to the workload generating the audit event. In most cases, you need to interrogate *AuditData* to discover the most important information about an event. Workloads use schemas to describe the properties they insert into audit records. The schemas are [documented here](#). Some trial and error are often necessary to interpret the payload in audit events. The guide to [detailed properties in audit log records](#) is helpful in this respect.

The *AuditData* property consists of a set of multiple attribute-value pairs separated by a comma (in JSON format). The property can extend to several thousand characters. To format the information and make it easier to follow, specify the *Formatted* parameter with the *Search-UnifiedAuditLog* cmdlet. The audit data is more legible, and we can see many items of interest, including:

- **RecordType:** The workload that generated the record. Examples of values include:
 - AzureActiveDirectory: For example, add a member to a group.
 - MicrosoftTeams: For example, a user logs onto Teams.
 - ExchangeAdmin: For example, an update of mailbox properties.
 - SharePointFileOperation: For example, a client downloads a file.
- **CreationTime:** The date and time in UTC format when the user performed the activity. If your time zone isn't UTC, you must adjust this value to get to a local time.
- **Operation:** Workloads log audit events for different actions. For example, SharePoint Online logs a *FileCreated* event when a user creates a new file and a *FileModified* event when someone edits a file.
- **OrganizationId:** The unique GUID for the tenant.

- **UserKey:** The identity (in this case, achieved through membership of a group) used to gain access to the item.
- **Workload:** The name of the workload that captures the event.
- **ClientIP:** The IP (V4 or V6) address of the client workstation where the action originated. See earlier note about when the IP address might not be for the workstation.
- **ObjectID:** The full path to the object.
- **UserID:** The object identifier for the user account that caused the action to occur.
- **UserAgent:** The client used to invoke the action.
- **SourceFileName:** The name of the file.
- **UserType:** The type of user that performed the action. "0" indicates a normal user; "1" indicates an action taken by an administrator, while "2" means that the action a Microsoft data center administrator or data center system account performed the action. Because we used the *Formatted* switch for the *Search-UnifiedAuditLog* cmdlet, the numeric value 0 becomes "Regular."
- **EventSource:** Only SharePoint Online uses this field. It is either SharePoint or ObjectModel.

The *ResultIndex* and *ResultCount* properties for audit records are interesting if you need to keep track of a large record set. *ResultIndex* tells us the record number within the set returned. *ResultCount* tells us the total number of records returned. If the search encounters an internal timeout, *ResultIndex* will be -1.

It takes time for administrators to become accustomed to the information contained in audit records and to figure out how best to use this data when confronted with questions such as "who interacted with a document" or "who created new documents in this period." Experience with the PowerShell cmdlets and some trial and error soon shows that the audit log is a surprisingly useful source of information.

Fetching Large Amounts of Audit Data

In large tenants, or where you need to retrieve information about multiple operations over an extended period or if you run a search to find all audit records generated within a tenant for a day, it is likely that a search will find more than 5,000 audit records. In these scenarios, to make sure that the search retrieves all records, it should fetch audit data in pages holding up to 5,000 records at a time until no more data is available. This technique supports the retrieval of up to 50,000 audit records. If more than 50,000 matching records exist, you need to split the work across multiple searches, each of which uses different criteria. You store the results of the searches in an external repository (many organizations use Splunk for this purpose) and run the analysis against that repository.

Search-UnifiedAuditLog has two parameters to support the retrieval of large data sets:

- The **SessionId** parameter holds a string value to identify a search session. You can use any value you like from a simple number to a GUID generated with the *New-Guid* cmdlet. The presence of a session identifier tells *Search-UnifiedAuditLog* that it might need to fetch several pages of data.
- The **SessionCommand** parameter tells *Search-UnifiedAuditLog* how to handle large amounts of audit data. The returned data might contain duplicate records. This parameter can be set to:
 - *ReturnLargeSet:* The audit records returned are unsorted. Include this parameter for all operations where a search fetches more than 100 records. Remember to sort the data after retrieval. For example:

```
$Records = $Records | Sort-Object {$_.CreationDate -as [datetime]} -Descending
```

- *ReturnNextPreviewPage:* *Search-UnifiedAuditLog* returns audit records sorted by date. You can fetch only a maximum of 5,000 records using this method. If more matching records exist, attempts to fetch the data will result in an error.

The essential steps to fetching large amounts of audit data are:

1. Create a session identifier.
2. Set up a loop to fetch data in pages.
3. Run *Search-UnifiedAuditLog* several times to fetch all available data.
4. For each run of *Search-UnifiedAuditLog*, store the retrieved data.
5. After fetching all pages, sort the data by date and write it out to a CSV file.

In this example, *Search-UnifiedAuditLog* fetches audit data about SharePoint Online file operations in batches of 4,500 records at a time. The only data stored is in the *AuditData* payload from the audit record. The output of statistics after each page is purely for informational purposes.

```
$StartTime = Get-Date; $SessionName = (New-Guid).Guid; $OutData = @()
$EndDate = (Get-Date).AddDays(+1); $StartDate = (Get-Date).AddDays(-90); $i = 0
Write-Host "Searching the Audit Log..."
Do {
    $ThisSearchStart = Get-Date; $i++
    [array]$Records = Search-UnifiedAuditLog -StartDate $StartDate -EndDate $EndDate -SessionId
    $SessionName -SessionCommand ReturnLargeSet -ResultSize 4500 -RecordType SharePointFileOperation
    If ($Records) { # The audit data returned is bad
        Write-Host "Error occurred fetching audit data. Resetting search and pausing before retrying"
        -foregroundcolor Red
        Start-Sleep -Seconds 240 # Wait for 4 minutes
        $i = 0 ; $SessionName = (New-Guid).Guid; $OutData = @() # Go back to zero
        Continue
    }
    If (($Records.Count -gt 0) -and ($Records[0].ResultIndex -ne -1)) { # Got a good page
        $OutData += $Records | Select-Object -ExpandProperty AuditData | ConvertFrom-Json
        Write-Host ("Completed Page #{1}, returned {2} records in {0} seconds. Total records found so
far {3}" -f [math]::Round((New-TimeSpan -Start $ThisSearchStart).TotalSeconds), $i, $Records.Count,
$OutData.Count)
    } Until ($Records.Count -eq 0) # Until we find no more records

$OutData = $OutData | Sort-Object {$_.CreationDate -as [datetime]}
Write-Host ("All done {0} records found in {1} minutes." -f $OutData.Count, [math]::Round((New-
TimeSpan -Start $StartTime).TotalMinutes,3))
```

The check against the *ResultIndex* property handles the situation where *Search-UnifiedAuditLog* sometimes returns duplicate information due to an internal timeout when fetching data. In this situation, *ResultIndex* is set to -1 (minus one). The search is invalid, and the results are possibly duplicated. The only solution is to zeroize everything and restart the search after a short delay.

Even in smaller tenants, you might want to use *Search-UnifiedAuditLog* to fetch audit data to store in an external repository to keep the data for longer than it is in Office 365. A scheduled job could be run daily to fetch all events for the last day for ingestion into the external repository, which could be another cloud service like Splunk or an ISV reporting product like [Quest Nova](#) (ISV products usually employ a range of Microsoft APIs to fetch audit and other data to log details of workload activity). Organizations often find compliance problems months after an event occurs and if you rely only on the audit log you might not be able to find all the evidence required for an investigation.

High Completeness Searches

In April 2024, Microsoft introduced the preview for high completeness audit log searches. Since the introduction of the unified audit log, the number of auditable events and the number of users generating events has grown enormously. The volume of data processed by audit log searches is such that searches that retrieve large numbers of audit records are susceptible to timeouts, which can lead to incomplete results. To address the problem, the high completeness option performs a more exhaustive search by prioritizing the retrieval of every possible matching record. Because of the additional checks performed when fetching records, these searches are slower than normal searches.

To run a high completeness search, include the *HighCompleteness* switch in the search parameters. Even when a search expects to retrieve tens of thousands of events, you do not need to use the *SessionCommand* parameter. I have retrieved over 120,000 audit records with a high completeness search.

Here's an example command:

```
[array]$Data = Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-30) -EndDate (Get-Date).AddDays(1) -HighCompleteness -Formatted
```

To conserve resources, Purview limits the number of high completeness searches per administrator account to approximately five searches over a 20-minute period. If Purview rejects a search with a "Too Many Requests" error, wait ten minutes and retry.

Processing the results of a high completeness search uses the same methods as for normal searches.

Azure Automation and Audit Searches

Given the large quantity of audit data that might need to be searched on a regular basis, it makes sense to use Azure Automation and its scheduling capabilities for this purpose. An example of how to use the Exchange Online management PowerShell module with a managed identity in an Azure Automation runbook [is available online](#). The script scans the audit log for several events designated as high priority because they might be used by attackers to compromise a tenant. If the search finds any matching events, the script emails details to administrators for them to check out. More details covering the use of Azure Automation with PowerShell are available in the PowerShell book.

Discovering What Audit Operations Exist

As explained above, you can filter audit records by specifying the type of operations to see. For instance, to see who sends emails on behalf of a shared mailbox, you can look for audit events with the *SendAs* operation. New operations appear in the audit log on an ongoing basis as workloads enable auditing for new features. The question of how best to discover new events therefore exists. Here's what we do to find if a new feature is captured in an audit event.

- First, use the new feature. Ideally, perform actions several times with different accounts.
- Second, wait for at least an hour to allow the ingestion of audit events from the source workload and appear in the audit log.
- Next, run a search to find all audit events for the current day and group and sort the results by operation. Make sure to specify the user principal name of the account which performed the accounts in the *UserIds* parameter.

```
[array]$Records = Search-UnifiedAuditLog -StartDate (Get-Date) -EndDate (Get-Date).AddDays(1) -ResultSize 2000 -Formatted -SessionCommand ReturnLargeSet -UserIds Ken.Bowers@office365itpros.com  
$Records | Group-Object Operations | Sort-Object Count -Descending | Format-Table Count, Name
```

You should now be able to browse the sorted list of operations to find unfamiliar actions, such as *Set-LabelPolicy* (logged when someone updates a sensitivity label policy). You can take the same approach with the Audit search feature in the Compliance portal, but not all audit events show up there.

Searching the audit log to find new events also uncovers audit events logged when Microsoft updates tenant settings as part of their normal operations. For instance, Microsoft often updates OWA mailbox policies to introduce a control for a new OWA feature. When this happens, you'll find audit events logged for a user called *NT AUTHORITY\SYSTEM (Microsoft.Exchange.ServiceHost)* for the policy updates.

Activity Name Changes: Microsoft can change the name given to activities (operations) in the unified audit log. For instance, Microsoft changed the name for file deletion actions in SharePoint Online and

OneDrive for Business from *FileDeleted* to *FileRecycled* in mid-2023. Because these changes usually happen without warning, it's a good idea to periodically check that audit log searches return the data you expect.

Practical Examples of Using Audit Information

Audit records hold a wealth of information in the *AuditData* property. To make the information more approachable, we must break out the important pieces from the JSON-formatted data in this property and use the different elements for whatever analysis is required.

Deciding What Audit Data is Output

All the examples in this section use a generic PowerShell list called *\$Report* as the output for information about audit data. You can use PowerShell to sort, group, or otherwise process the table to display the audit data as you like. Naturally, because each workload generates both a set of common audit data and some information of its own, you might want or need to adjust the code in the examples to meet your specific requirements by adding new outputs to the object or changing what is written into it.

For instance, somewhat confusingly, audit records have two timestamps to record when an action occurred. The date is the same, but the format is different. The *CreationDate* property outputs the timestamp in the locale defined for the workstation where you run the PowerShell script.

9 Jan 2019 12:18:47

The *CreationTime* property in *AuditData* holds the timestamp in ISO 8601 format, as in:

2019-01-09T12:18:47

The ISO 8601 format is not dependent on the locale and is what PowerShell uses when it outputs the current date and time using a command like:

Get-Date -Format s

You can use either timestamp as they both store the same data. If you prefer to use a different date format in the reports to match whatever format the consumers of the report like to see, change the line that writes the timestamp into the report. For instance, if you use the *CreationTime* property, you can output it in the general date/time pattern in short form – like 9-Jan-2019 12:18:

TimeStamp = Get-Date \$AuditData.CreationTime -format g

Using Input Arrays

If you are searching for audit events for multiple operations, it is convenient to populate an array with the operations and use the array as input for the search. For example:

\$Operations = @('FileAccessed', 'FileDownloaded', 'FileModified', 'FileRecycled', 'FileUploaded')

An array can also hold user identifiers as input. This example populates an array with user principal names fetched by calling the *Get-ExoMailbox* cmdlet.

[array]\$Users = Get-ExoMailbox -Filter {CustomAttribute1 -eq "Sales"} | Select-Object -ExpandProperty UserPrincipalName

Once populated, pass the arrays in the same way as you would pass individual operations or user identifiers:

Search-UnifiedAuditLog -Operations \$Operations -UserIds \$Users -StartDate \$StartDate -EndDate \$EndDate -ResultSize 5000 -SessionCommand ReturnLargeSet

Examining Retrieved Audit Information

Three options exist to examine the information generated by the search and held in the *\$Report* object.

1. If the number of audit records found is small, you can examine the data on the screen.
2. An alternative is to pipe the information in the table to the `Out-GridView` cmdlet. This makes it much easier to review (and sort) the data.

```
$Report | Out-GridView
```

3. Once the number of records grows, it is usually easier to export the data as a CSV file:

```
$Report | Export-Csv c:\temp\Report.csv -NoTypeInformation
```

We can then open the CSV file with Excel to format the data as desired or load the CSV file into a tool like Power BI to generate graphs, views, and reports from the audit data.

Tracking Group Creation

The first example creates a report about who created groups, including the workloads used to create the groups. The relevant event to look for is "Add Group." In this example (code [downloadable here](#)), we search for groups created over the last 180 days. The script processes the records to extract information about who created each group, the group name, and the workload used.

The output for the report should look something like the example below. In this case, we see details of the creation of six groups using a variety of workloads including Planner (*ProjectWorkManagement*) and Teams. The *Microsoft.Exchange* workload means that an Exchange client (like OWA) created the group. If you see a workload named with a value like "12128f48-ec9e-42f0-b203-ea49fb6af367," it is the Teams PowerShell module.

TimeStamp	Workload	User	GroupName
9 May 2019 19:44	ProjectWorkManagement	James.Ryan@office365itpros.com	0365Grp-James Plan
8 May 2019 22:11	Microsoft Teams Services	Kim.Akers@office365itpros.com	0365Grp-Acquisitio
8 May 2019 19:01	Microsoft.SharePoint	Joe.Richards@office365itpros.com	Nice Airport Watch
8 May 2019 12:36	Microsoft.Exchange	Brian.Weakliam@office365itpros.com	Brian's Nelson Gro
7 May 2019 17:45	Microsoft.Exchange	Vasil.Michev@office365itpros.com	Sandboxes

If you run this script, you might notice that Microsoft has updated some of the workload names. For instance, the current name for Exchange is "Office 365 Exchange Online" while SharePoint is "Office 365 SharePoint Online."

User Sign-ins

In another example of how to use the same technique to interpret audit events, here's what you might do to report user sign-ins to different workloads. To make things more complicated, we use two different events, one from Entra ID (to handle most workloads) and the other from Teams. Because we can expect to retrieve many audit records for these operations, we also pass the `ReturnLargeSet` value to the `SessionCommand` parameter and specify that we will accept up to 5,000 records. The code is [available on GitHub](#). Another way to get user sign-in information with PowerShell is via the `Get-MgAuditSignInLogs` cmdlet.

Understanding failed user login events is also interesting because these events might be the result of attempts by attackers to penetrate your tenant. You can find code to search for audit events for failed user sign-ins [on GitHub](#).

Who Updated That File?

People often want to know who made changes to a document. The example search in the script (see link below) finds audit events created when someone creates or edits a specific file over the last 180 days. The script prompts the user for a file name to search for and stores its name in the `$FileName` variable. Depending on the document's history, we could find:

- A single *FileUploaded* event when the document is uploaded to SharePoint Online or OneDrive for Business.
- A *FileAccessed* event when a user opens the document.
- A *FileModified* event when a user updates the document. Events also appear from the background process used by SharePoint Online to maintain files. These appear as the *app@sharepoint* user.

If the AutoSave feature is enabled for the document, multiple *FileModified* events can accumulate over a short period. We can extract information about who did what to the document from the *AuditData* field for the audit events, which contains information about the site (including its URL) where the document is stored.

After analyzing the set of audit records found for the document (use the script [downloadable from GitHub](#)), we can list the results:

```
$Report | Select-Object Timestamp, User, Action
```

TimeStamp	User	Action
-----	-----	-----
22 Apr 2024 14:40:41	Jane.Maloney@office365itpros.com	FileModified
21 Apr 2024 15:19:03	Jane.Maloney@office365itpros.com	FileModified
21 Apr 2024 15:02:34	Kim.Akers@office365itpros.com	FileModified
21 Apr 2024 15:01:39	Jane.Maloney@office365itpros.com	FileUploaded

SharePoint Online and OneDrive for Business move deleted files through a two-stage recycle bin. Three different audit events capture each stage:

- **FileRecycled**: The original deletion (by a user, a retention policy, or system process).
- **FileDeletedFirstStageRecycleBin**: A user removes a file from the first stage recycle bin. Any member of a team or group can do this. Normally, files stay in the first stage recycle bin for 30 days.
- **FileDeletedSecondStageRecycleBin**: A site administrator (group or team owner or the owner of a OneDrive for Business account) removes a file from the second stage recycle bin. Usually, files remain in the second stage recycle bin until 93 days after their original deletion. At this point, SharePoint Online removes the file permanently and it is irrecoverable (unless a retention label or policy forces SharePoint Online to keep a copy in the site preservation hold library).

Reporting file deletion events is a straightforward process. An example script to illustrate the process [is available in GitHub](#).

SharePoint Sharing Events

SharePoint logs audit events when users generate sharing invitations with people inside and outside the tenant. Three separate events are recorded for secure links (those that specify specific individuals to share with):

- *SharingSet*: Someone shares a document with someone else (inside or outside the tenant).
- *SecureLinkCreated*: SharePoint creates and sends a secure link to the target user. This only happens for external users as users with accounts in the tenant directory can use their accounts to access the shared document.
- *SecureLinkUsed*: The target user uses the secure link to access the document. Again, this only happens when external users access a shared document.

You can search for these audit records with a command like:

```
[array]$Records = Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-30) -EndDate (Get-Date).AddDays(+1) -Operations SharingSet, SecureLinkUsed, SecureLinkCreated -ResultSize 2000 -Formatted -SessionCommand ReturnLargeSet
```

If you extract the data from the payload in the audit events and interpret the information, you see this kind of sequence when an external person uses a sharing invitation.

- A SecureLink is created for a document. In this case, the document is in a SharePoint Online document library.
- The sharing settings for the link are set.
- The sharing link is used. Because the sharee is outside the tenant, SharePoint Online creates a guest account in the tenant directory to allow the sharee to authenticate.

```

CreationDate : 14-Jun-2024 16:25:59
Operation     : SecureLinkCreated
User          : tony.redmond@office365itpros.com
File          : Contoso Sponsor Content.docx
URL          : https://office365itpros.sharepoint.com/sites/0365ExchPro/Shared Documents/2025
Edition (11th)/Contoso Sponsor Content.docx
EventData     : <Type>Edit</Type><MembersCanShareApplied>False</MembersCanShareApplied>
Sharee        :

CreationDate : 14-Jun-2024 16:25:59
Operation     : SharingSet
User          : tony.redmond@office365itpros.com
File          : Contoso Sponsor Content.docx
URL          : https://office365itpros.sharepoint.com/sites/0365ExchPro/Shared Documents/2025
Edition (11th)/Contoso Sponsor Content.docx
EventData     : <PermissionsGranted>Limited
Access</PermissionsGranted><MembersCanShareApplied>False</MembersCanShareApplied>
Sharee        :

CreationDate : 14-Jun-2024 16:41:02
Operation     : SecureLinkUsed
User          : Joan_smith_contoso.com#ext#@office365itpros.onmicrosoft.com
File          : Contoso Sponsor Content.docx
URL          : https://office365itpros.sharepoint.com/sites/0365ExchPro/Shared Documents/2025
Edition (11th)/Contoso Sponsor Content.docx
EventData     :
Sharee        : Joan_smith_contoso.com#ext#@office365itpros.onmicrosoft.com

```

A script showing how to extract similar data from audit records is [available from GitHub](#). The script also reports details of company links (those that grant access to anyone in the organization) and anonymous links.

Guest User Access to Documents

Our next example shows how to search the audit log for File Accessed events for guest users. The idea is to understand the files in document libraries guest users have opened. We could expand the search to include File Modified events if you want to know what files guest users update, but this search is enough to prove the point. After finding the data using the [script available from GitHub](#), here's how to sort it to discover the set of documents accessed by each guest.

```
$Report | Sort-Object User, Document | Format-Table TimeStamp, User, Document -AutoSize

TimeStamp      User                                Document
-----        -----
21 Dec 2023 11:39  john_contoso.com#ext#@Tenant.onmicrosoft.com  Summit 2018.one
5 Jan 2024 11:12   mary_contoso.com#ext#@tenant.onmicrosoft.com  Summit 2016.one
6 Jan 2024 09:44   mary_contoso.com#ext#@tenant.onmicrosoft.com  Updates.docx
9 Jan 2024 08:15   terry_contoso.com#ext#@tenant.onmicrosoft.com  Amazon Blurb.docx
```

We can view the audit data in different ways. For example, to find out how many accesses occurred to each document, you could do this:

```
$GroupData = $Report | Group-Object -Property Document
$GroupData | Sort-Object Count -Descending | Select-Object Name, Count

Name          Count
----          ----
```

Ch 5 - SharePoint Online and OneDrive For Business - Final.docx	17
Project Ambush.docx	11
Interesting data.docx	10
Financial Arrangements 2019.docx	9
Ch 8 - Clients.docx	8
Ch 3 - Basic Workloads.docx	6
Budget 2019.docx	1

Reporting the Assignment of Retention Labels

The same technique of grouping and sorting data from audit records is useful to report other aspects of Microsoft 365. If you have Office 365 E5 or Microsoft 365 Compliance E5 licenses, you can use the Activity Explorer (see the compliance chapter) to discover what's happening with retention and sensitivity labels.

PowerShell gives you another way to do the job. For instance, to know what the most popular retention label applied to documents is, search for *TagApplied* events, extract the audit data, and put the events into the *\$Report* output. Because audit events often hold different information, this process is slightly complicated by the need to accommodate labels applied as a default for a library and those assigned manually by users. An example script can be [downloaded from GitHub](#). The script generates a list in the *\$Report* variable, and a little grouping and sorting reveals what the most popular retention label is:

```
$GroupData = $Report | Where-Object {$_ .Type -eq "File"} | Group-Object -Property Label | Sort-Object Count -Descending | Select-Object @n="Retention Label"; e={$_ .Name}, Count
```

Retention Label	Count
eBook Content	222
Audit Material	34
Approved	25
Confidential	12
GDPR Personal Data	10
Commercially Sensitive	4

If you see a blank entry in the list, it is for audit events logged when a user removes a retention label from a document. Note that the audit log does not capture events for when documents receive retention labels when created in or uploaded to document libraries with a default retention label.

Who Used the SendAs Permission?

Unlike Exchange on-premises, where all *SendAs* events are generated by delegates sending messages for another mailbox, Exchange Online processes messages sent by other workloads that can show up as *SendAs* actions in audit searches and skew results unless adjustments are applied. Here are some things to consider:

- Audit records with S-1-5-18 captured in the *UserId* property record the generation of a welcome message for a new team.
- Audit records are generated when Teams sends a welcome message.
- Audit records are generated for the group mailbox when a member posts a message to a conversation in an Outlook group using OWA. Records are not generated when messages are posted with other clients or arrive from guest members.
- Audit records are generated for the group mailbox when someone updates a task in Planner.

With these caveats in mind, the script to search for *SendAs* records, process the audit records, and identify events belonging to user or shared mailboxes and those belonging to group mailboxes can be [downloaded from GitHub](#). The former category is normally what people are concerned with because they're looking for instances where someone sent a message from a mailbox rather than posting to an Outlook group or adding a comment with Planner. As you can see in the script, to distinguish between the two categories, we create a hash table of primary email addresses for mailboxes and groups and look up that table for each audit event to decide if it belongs to a user/shared mailbox or a group mailbox.

Searching for Audit Records Tracking Actions Against an Object

Most auditing attempts to answer “who did what” questions. In other words, you want to know who performed a specific action. Sometimes you need to know what happened to a particular object, like a document or a user. Finding audit events for one or more documents is easy – all you need to do is pass the document names in the *ObjectIds* parameter. In this example, we create an array of document names to search for and then pass the array as the *ObjectIds* parameter for the call to *Search-UnifiedAuditLog*:

```
[array]$docs = "New Signature API for Email Signatures.docx", "Controlling default creation of online meetings with OWA.docx", "Anticipating Microsoft Ignite 2020.docx"
[array]$Records = Search-UnifiedAuditLog -ObjectIds $docs -StartDate (Get-Date).AddDays(-90) -EndDate (Get-Date).AddDays(+1) -ResultSize 500 -SessionCommand ReturnLargeSet
```

The events found are for all actions performed against the documents, such as being modified or downloaded. The same technique works for users.

```
[array]$Users = "Oisin.Johnston@office365itpros.com", "Kim.Akers@office365itpros.com"
[array]$Records = Search-UnifiedAuditLog -ObjectIds $Users -StartDate (Get-Date).AddDays(-90) -EndDate (Get-Date).AddDays(+1) -ResultSize 500 -SessionCommand ReturnLargeSet
```

To emphasize, this search returns events for actions performed for these users (like being added to a group membership) rather than events performed by the users.

Microsoft 365 Groups are not users, so if we want to find the actions performed against a group, we must use the *FreeText* parameter to search audit records for instances of unique values that identify the group we’re interested in. Fortunately, the object identifier for a group is a good search term. In this example, we extract the object identifier for a Microsoft 365 group and use it to search for audit events. We then group the audit events to get an overview of the kind of activity performed against our target:

```
$ObjectId = Get-UnifiedGroup -Identity "Office 365 for IT Pros" | Select -ExpandProperty ExternalDirectoryObjectId
[array]$Records = Search-UnifiedAuditLog -FreeText $ObjectId -StartDate (Get-Date).AddDays(-90) -EndDate (Get-Date) -ResultSize 1000 -SessionCommand ReturnLargeSet
$Records = $Records | Sort-Object Identity -Unique | Sort-Object { $_.CreationDate -as [datetime] } -Descending
$Records | Group-Object Operations | Sort-Object Count -Descending | Format-Table Name, Count
Name          Count
----          -----
RecipientChange    17
TabUpdated        10
TabAdded          4
Remove member from group. 3
MemberRemoved     3
Add member to group. 3
Update group.     2
MemberAdded       2
TabRemoved        1
Set-UnifiedGroup   1
```

The technique also works for finding audit records for security groups (but not for distribution lists). It also works for user accounts, including guest users, but it’s much slower than using the *ObjectIds* parameter. As the name implies, *FreeText* means that a free text search is used to find matching audit events. In a large tenant, a free text search across potentially millions of records won’t be fast.

Remember that a single action can result in multiple events. For instance, if you add someone to a group, the *MemberAdded* and *Add member to group* events are captured by different workloads and ingested into the audit log. The duplication is easily detected by comparing the creation date for the events.

Microsoft 365 Copilot Audit Records

When a user in a Microsoft 365 application uses Copilot, the application captures an audit record for an operation called *CopilotInteraction*. Interpreting the audit event reveals the application used and the application resources (like a document or video) used by Copilot to respond to the user prompt. This article explains [how to find and analyze Copilot audit records](#).

Scoped Audit Searches with Administrative Units

It's possible to limit audit searches to find audit records limited to those generated by the membership of Entra ID administrative units. This type of audit log searches are scoped to one or more administrative units while regular audit log searches are scoped to the organization. For instance, administrators based in Germany might receive the permission to search for audit events generated by German users while global administrators can search across all administrative units.

The basics of the solution are as follows:

- Exchange Online synchronizes information about administrative units and their membership with Entra ID. This synchronization occurs after changes happen in Entra ID and makes sure that Exchange Online can process audit searches accurately.
- User accounts must hold a suitable Purview compliance role such as Audit Reader to search the audit log using the Compliance portal or the AuditLog Query Graph API. When assigning a compliance role, an administrator can be limited to one or more administrative units. The Audit log search in the Purview compliance center applies the limitation to the administrator when they create new searches.
- To facilitate searching based on administrative units, Purview stamps new audit events generated for user accounts with their membership of administrative units. The information recorded is accurate at the point in time. Changes in administrative unit membership are not retrospective.

You can see details for administrative units by selecting an audit record found by a search in the GUI or in the *AssociatedAdminUnits* property of the *AuditData* payload in an audit record found with PowerShell:

```
"AssociatedAdminUnits": [  
    "8a703400-7086-4e13-943a-7ed8df9ecd41",  
    "4d3ae8ee-212b-4be4-965c-8b5111d4488e",  
    "150dccad-f8b8-4e54-9246-89834b8b5a25"]
```

To convert the identifiers into the display names for the administrative units, save the information in an array and use the *Get-AdministrativeUnit* cmdlet to resolve the identifiers:

```
$AdminUnits = ($Records[0].AuditData | ConvertFrom-Json).AssociatedAdminUnits  
ForEach ($AU in $AdminUnits) { (Get-AdministrativeUnit -Identity $AU).DisplayName }  
  
Group HQ dynamic administrative unit  
United States  
Group HQ Users
```

The scoping enabled by use of the Purview compliance roles does not apply to searches performed with the *Search-UnifiedAuditLog* cmdlet. Instead, two perquisites must be met:

- The account that runs the audit log searches must be able to run cmdlets from the Exchange Online management module. Accounts holding the Exchange administrator role have this right automatically.

- An Exchange Online management role assignment must link the user running the search with the administrative unit. For instance, this role assignment links Ken Bowers to the administrative unit with the identifier used in the command:

```
New-ManagementRoleAssignment -User Ken.Bowers@office365itpros.com -Role "Audit Logs"
-RecipientAdministrativeUnitScope "66faad17-cc6d-45bb-8d88-35789b9b3c00"
```

To find the identifier of an administrative unit, run the *Get-AdministrativeUnit* cmdlet:

<code>Get-AdministrativeUnit Where-Object {\$_.DisplayName -eq "German Employees"}</code>	
Name	DisplayName
---	-----
<code>66faad17-cc6d-45bb-8d88-35789b9b3c00</code>	<code>German Employees</code>

Obviously, audit searches limited by administrative units only find audit records stamped with the target administrative units. System-generated audit records are not included in the set returned by Purview.

Premium Auditing and Crucial Events

Microsoft Purview Audit (Premium) is available to users with Office 365 E5 or Microsoft 365 E5 licenses or the Microsoft 365 E5 compliance add-on. The solution covers:

- **Longer retention of audit data.** Instead of purging audit events after 180 days, the retention period for events for Exchange Online, SharePoint Online, and Entra ID is 365 days. The [Microsoft Purview Audit \(Premium\) solution](#) can keep audit data for up to 10 years with an additional per-user license.
- **Audit log retention policies.** Because tenants might not want to hold some audit events for 365 days, they can apply audit log retention policies to remove selected events from the audit log.
- **Crucial or high-value audit events.** These are audit events designed to expose in-depth information for forensic investigation. You don't need to enable the collection of crucial audit events as this happens automatically for all accounts with the appropriate licenses.

Among the set of crucial events are:

- **MailItemsAccessed:** Items in a mailbox are accessed (opened) or synchronized.
- **Send:** A message is sent from a mailbox.
- **SearchQueryInitiatedExchange:** A mailbox search is initiated using Outlook desktop or OWA.
- **SearchQueryInitiatedSharePoint:** A search is initiated for a SharePoint site.
- **Other workload events from Forms, Stream, and Teams** (see [this link](#)).

Examples of Teams crucial events are:

- **MeetingDetail:** A Teams meeting occurs.
- **MeetingParticipantDetail:** A participant joins a Teams meeting. See [this article](#) for information about how to find and analyze Teams meetings audit events.

The relevant workloads automatically capture the crucial mailbox events once an account has the necessary license. To capture the search events in Exchange Online, you must update the owner audit configuration for individual mailboxes. For example:

```
Set-Mailbox -Identity Kim.Akers -AuditOwner @{Add="SearchQueryInitiated"}
```

In July 2023, [Microsoft decided](#) to make 30 critical high-value audit events (including *MailItemsAccessed*) previously only generated for accounts with Microsoft Purview Audit (Premium) licenses available to accounts with Microsoft Purview Audit (Standard). The decision was provoked by a realization that restricting these kinds of events was unwise in the context of growing worldwide threat from attackers. Deployment to make the events available to tenants started in May 2024.

After Microsoft updates a tenant to generate the additional high-value audit events, administrators can check, and if necessary, update the audit configuration for a mailbox to add events like *MailItemsAccessed* by running *Set-Mailbox*:

```
Set-Mailbox -Identity Lotte.Vetler -AuditOwner @{Add="MailItemsAccessed"}
```

Like other changes to mailbox auditing, it's a good idea to periodically validate that mailboxes have the correct audit configuration and update the configuration if necessary.

The MailItemsAccessed Event

Exchange Online generates the *MailItemsAccessed* event when licensed users access mailbox items using any connectivity protocol from any client. The events are uploaded to the audit log along with other Exchange events. Exchange Online logs two kinds of *MailItemsAccessed* events: *Sync* (synchronization) and *Bind* (access to a message).

- **Sync events** occur when an Outlook desktop client synchronizes messages from the mailbox to its local cache (the OST for Windows or OLM for Mac). During synchronization, the client downloads copies of all new or changed items from the mailbox and notes any deletions from the server to apply in its local copy. The sync event records that synchronization occurred for a folder. Over a working day, many events record synchronization for folders like Inbox, Sent Items, Deleted Items, and the Calendar, plus any other folder messages are moved into. In terms of investigation, the assumption is that if a breach occurs and someone can use Outlook to synchronize a folder to a local cache, potentially all items in that folder are copied.
- **Bind events** record access to an individual message. To reduce the number of audit records, Exchange Online generates a single bind event covering access to messages within two minutes. Thus, a bind event might cover access to a single message or ten messages.

To give an idea of the volume of events a user might produce, over two days, 443 *MailItemsAccessed* events were generated for a single mailbox. The majority were Bind events (394), and of these 312 were in the Inbox and 32 in Sent Items. Twenty-five events were captured for the Outbox, which is a transient folder where items exist while awaiting processing by the Exchange transport service. It's also used when Outlook posts to a conversation in an Outlook group, which is why the events for the Outbox folder were captured. The number of events captured by other mailboxes will vary depending on:

- The amount of inbound traffic. For instance, executive mailboxes often have a higher level of traffic. Organizations that use Teams for internal collaboration might find that the level of traffic is lower.
- The actions taken by the mailbox owner (or delegates).
- The number of clients signed into the mailbox.

In the case of very active mailboxes, if more than a thousand events are generated for a mailbox in less than 24 hours, Exchange Online stops generating *MailItemsAccessed* events for that mailbox for 24 hours. Microsoft says that less than 1% of Exchange Online mailboxes are throttled.

Forensic Investigations of Mailbox Breaches

[Microsoft's documentation](#) lays out the steps that forensic investigators can use to interpret the information captured in *MailItemsAccessed* events if they suspect that an attacker gains access to a mailbox. The basic idea is to:

- Identify when a user's mailbox might have been compromised.
- Discover what folders an attacker might have accessed in the mailbox (*Sync events*). It is possible that the attacker downloaded (synchronized) the entire mailbox to Outlook.
- Discover the individual messages accessed by the attacker (*Bind events*). The events store the internet message identifier for messages, which can be used to find the messages in the mailbox.

- Investigate if the attacker sent any messages were sent from the mailbox. *Send* events record each message sent. The message subject and its internet message identifier are recorded. Investigators can use this information to discover the recipients of the messages and decide if any information has been sent to an unauthorized address.
- If the account is compromised, the attacker might have performed searches to look for confidential or sensitive information. The *SearchQueryInitiatedExchange* and *SearchQueryInitiatedSharePoint* events record details of searches performed against the mailbox and SharePoint sites. Any evidence of unusual search activity deserves further investigation to identify if the searches are performed by the account owner or an attacker.

Given the number of audit events that an investigator might have to examine in the steps described above, it's not realistic to use the audit log search GUI. Instead, most investigators use PowerShell to find and analyze audit records to extract relevant and useful information. An example script to parse *MailItemsAccessed* events, including using the *Get-MessageTrace* cmdlet to find the subject of messages (within the last 10 days), can be [downloaded from GitHub](#). Examples of how to parse audit records for the send and search events [are also available](#).

Audit Log Retention Policies

Microsoft Purview's premium audit functionality includes the ability for tenants to configure audit log retention policies. You define a [retention policy for selected audit events](#) with a set retention period and those items will be purged after that period. A tenant supports up to 50 audit log retention policies.

Management of audit log retention policies is through the [Audit section of the Microsoft Purview Compliance portal](#) or PowerShell (after connecting to the compliance endpoint). This example runs the [New-UnifiedAuditLogRetentionPolicy](#) cmdlet to create an audit retention policy to remove any *SearchQueryPerformed* event executed by the background *app@sharepoint* process after three months instead of the twelve-month retention of audit events if the tenant has E5 licenses:

```
[PS] C:\> New-UnifiedAuditLogRetentionPolicy -Name "90-day Retention SearchQueryPerformed by app@sharepoint" -Description "Remove SearchQueryPerformed events from the app@sharepoint process after 90 days" -RecordTypes SharePoint -Operations SearchQueryPerformed -UserIds "app@sharepoint" -RetentionDuration ThreeMonths -Priority 8
```

Purging the Audit Log

You can choose to apply retention for any of the events captured in the audit log and keep them for three, six, nine, twelve months, or 10 years. It's a good idea for tenants who either want precise control over the retention of audit data or want to clean up events that don't add much value in terms of investigations. SharePoint is a notoriously "chatty" application when it comes to the capture of audit events, so tenants might decide to keep important events like *FileUploaded* or *FileAccessed* for as long as possible while removing some of the chatter after 180 days.

Activity Alerts and Alert Policies

Searching the audit log to find items of interest rapidly becomes boring. It also creates the potential that you might overlook important audit events. Microsoft 365 has two methods to automate checking of user activity within a tenant and alert administrators when something out-of-the-ordinary occurs:

- **Activity alerts** are available to all business tenants. An activity alert checks events recorded in the audit log for specified conditions defined by administrators and fires when those conditions occur.
- **Alert policies** build on the concept of activity alerts and apply extra intelligence to the events recorded in the audit log. Instead of firing when events occur, policies look for patterns of events such as a certain number of file downloads over a brief period. Microsoft includes a set of default alert

policies to help tenants understand their use and handle common conditions, including notification of malware attacks or instances when someone gains administrative permissions for Exchange Online. [Several predefined alert policies](#) are available to Office 365 E1 and E3 tenants while other policies (mainly handling malware and phishing campaigns) are available to tenants with Office 365 E5, Defender for Office 365 Plan 2, or Microsoft 365 E5 Compliance licenses. Tenants can create additional alert policies to meet specific needs or included with apps. For instance, communication compliance policies create alert policies to advise administrators when a threshold of *SupervisionRuleMatch* events match the conditions monitored to detect possible policy violations occur in a set period.

In both cases, administrators receive notifications via email, and it is then up to the people notified to act to resolve the detected problem. Only accounts that hold the Organization Configuration compliance role can create activity alerts or alert policies.

Activity Alerts and Alert Policies

Experienced administrators know when something is not quite right. At least, their suspicions heighten when they see certain things happening. [Activity alerts](#) help administrators keep up to date with what is happening inside the tenant. The alert engine packages activity alerts into policies to create the mechanism to inform nominated individuals when certain events occur. Alert policies try to capture the instinct of experienced administrators to detect patterns of problematic activity, using the ability of software to keep looking for matching patterns repeatedly. When a match occurs between real-time activity as captured in the audit log and the settings defined in a policy, The alert engine triggers an incident and notifies the recipients defined in the policy. The recipients are then responsible for resolving the incident. Conceptually, you can break down alert policies into four stages:

- **Understand** the normal ebb and flow of user activity to know what you expect to happen within the tenant. This is the activity baseline and can be set manually through your observations and experience or automatically by Microsoft.
- **Define** the characteristics of activity that cause concern and watch for incidents when those characteristics occur. These characteristics are the activity, condition, and threshold checked by an alert policy.
- **Monitor** the events recorded in the audit log against the conditions defined in alert policies.
- **Alert** administrators through email notifications when policy violations occur.

One thing to remember is that Alert policies don't support filtering based on a file or folder name, so you cannot use them to check changes made to a specific item. For instance, if your search is for file check-ins for a document called "Budget" and you use the search to create an alert, The alert engine generates alerts for all file check-in operations and not just for that document. In addition, activity alerts do not support date ranges, so the alert will fire for any matching activity from when you create it. An alert policy can check for multiple actions across multiple accounts. You can select any of the events logged in the audit log for monitoring. For example, you could have an alert that fires when someone checks a file into a document library or uses the *Send As* permission to send email on behalf of another user.

Purview can trigger alerts for every instance of a certain activity, such as when an administrator grants elevated permissions to another user. It can also trigger alerts based on event aggregation. For instance, users download 50 files from a SharePoint library within 30 minutes. That might be evidence of a hard-working user. On the other hand, it might be a sign that someone is grabbing some valuable intellectual property that they plan to take with them to another job. A more complex form of aggregation is when the threshold for a trigger is set by analyzing up to a week's worth of activities to understand the normal level of activities within

the tenant. If something then happens that greatly exceeds the expected norm, the recipients defined in the policy receive notifications.

Purview monitors the stream of audit data flowing from workloads to detect events matching those defined in alert policies. If Purview detects a match, it sends an email notification to the accounts registered for the alert.

Purview creates a set of default alert policies for tenants (see [this page](#) for the most current list and the licensing requirements for some advanced policies). Microsoft introduces new alert policies and updates existing policies as the need arises.

The default alert policies cover some generic situations that might or might not apply to your tenant, which is why you can define custom policies. You can only create custom alert policies if your account holds the Manage Alerts role (included in a compliance role group like Organization management). To create a new alert policy, go to the **Policies** section of the Microsoft Purview compliance portal and select **Policies**, then **Alert policies**, and then **New alert policy** (Mail flow alert policies are managed through the Exchange admin center). You can then add the following information to create the new alert:

- **Name and Description:** These settings are for administrative convenience, and you can enter anything you like. The name appears in dashboards, so it should convey the intent of the alert policy. The description is useful to note who created or last amended the policy and what the policy does.
- **Category:** To help track alerts, you can classify policies into the following categories, which you can use to sort alerts in the **View alerts** page:
 - Information governance. For example, users download more than a certain number of files to their PC over a defined period.
 - Permissions. For example, the elevation of permissions.
 - Mail Flow. For example, Exchange Online Protection detects malware in an email.
 - Threat management. For example, malware outbreaks.
 - Others. This category exists for tenants to use as they wish.
- **Severity:** You can assign alerts detected by the policy to be *Low*, *Medium*, or *High*. The more destructive a condition is, the higher its severity should be.
- **Activity:** The activity that the policy tracks. Alert policies do not yet cover all the activities recorded in the audit log because the intention is that alert policies can deliver near real-time notifications about problems and not all workloads feed events into the audit log that quickly. Microsoft will probably extend coverage across workloads over time. For now, policies can cover most activities in the SharePoint, OneDrive, and Exchange workloads. You can only select a single activity per policy. If activity policies do not support an event you want to check, you can create an activity alert to do the job.
- **Conditions:** For most activities, you can define conditions that must exist before Purview signals an alert. For example, a user downloads a file to a computer with a specific IP address. It is also possible to configure alerts to fire every time a user performs the activity or when users download files from a specific site.
- **Threshold:** How often an activity must occur within a period before a problem condition exists (thresholds aren't available for all types of alerts). The threshold can also be an unusual activity, which is when Purview compares activity for a period against the baseline for the tenant. Setting a threshold too low usually results in many notifications, which can hide real problems (the lowest threshold is 3 activities). Setting the threshold too high means that Purview might not send notifications in situations when administrators need to act. It is easy to tune a threshold after noting how many notifications administrators must process to reach a point where notifications arrive when real problems exist.
- **Email notifications:** You can define that alert notifications go to a list of recipients. Notifications can go to accounts within or outside the tenant. The account that creates a new policy automatically

receives notifications while the default policies send notifications to the tenant administrators. You can also set a daily limit for an alert policy so that a policy can only ever generate a certain number of notifications in a single day.

The new policy wizard steps through these sections to create a new alert policy. Figure 20-4 shows how to set conditions in an alert policy. In this instance, the organization wants to know when external users access information in a specific SharePoint Online site.

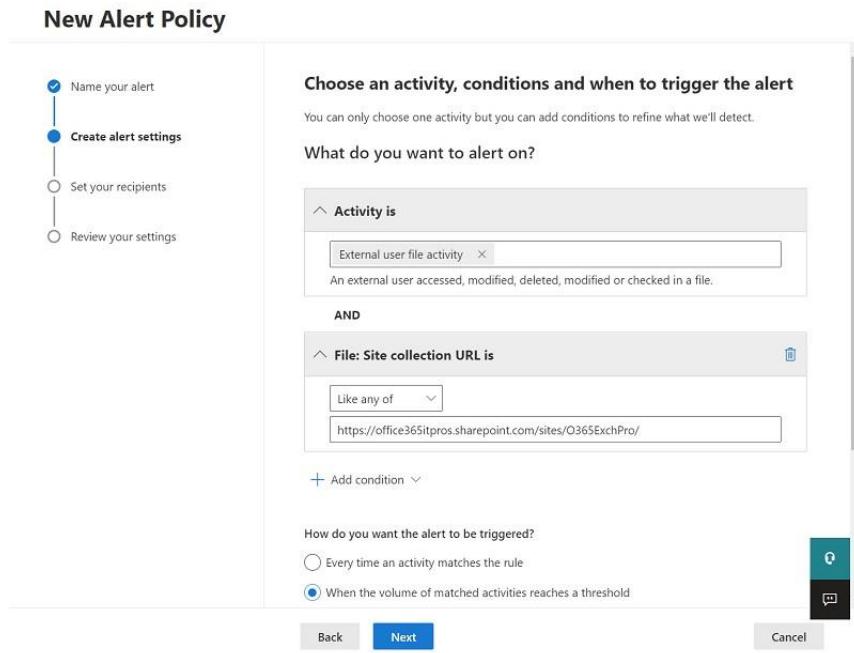


Figure 20-4: Defining the conditions for an alert policy

OneDrive Synchronizations and Alerts: If you implement alert policies for files downloaded from SharePoint or OneDrive for Business, you should set the threshold for the volume of matches to be higher than the largest number of files in a library synchronized with the OneDrive sync client. If you set a lower number, you will receive alerts each time the OneDrive sync client refreshes its copy of the library.

Handling Alerts

When Microsoft Purview detects a pattern of events matching the threshold and conditions set in an alert policy, it triggers an alert and generates an email to the recipient list defined in the policy. The notification tells the recipient:

- The severity level for the alert.
- The policy that triggered the alert.
- The date and time of the alert in UTC.
- The activity that triggered the alert.
- The details of the alert. For example, how many matched activities occurred in what timeframe.

The alert message has a **View incident page** link to open a page with the details of the Defender incident. Purview automatically creates for the alert. You can also view alerts through the Alerts section of the Microsoft Purview compliance portal. After viewing the incident, you can manage the alert to decide if the alert is a real incident by recording a status for the alert (*Active*, *In progress*, or *Resolved*) together with any comments to justify the status. You can also classify the incident to indicate if the event is normal behavior or a false or true positive. This feedback helps to refine the automatic detection of similar incidents in the future.

Figure 20-5 shows details of an alert generated when a user created a rule to forward email to an external recipient. This is an important alert that might indicate that an attacker has access to a compromised account and is preparing for a Business Email Compromise (BEC) exploit or to exfiltrate some data.

The screenshot shows the Microsoft Purview interface with the 'Alerts' module selected. The main pane displays an alert titled 'Creation of forwarding/redirect rule'. The alert details show it was triggered by a user named Terry.Hegarty@office365itpros.com performing a 'Created mail forward/redirect rule 1 times' activity. The alert is categorized under 'Threat management' and has a severity of 'None'. The status is 'Active, Investigating'. The right pane provides a detailed view of the alert, including options to 'Resolve', 'Suppress', or 'Notify users'.

Figure 20-5: Investigating an alert

A busy tenant might see many alerts daily. Filters are available to focus on alerts belonging to a certain category or severity level.

Activity Policies and PowerShell

Because of their complex nature, it is usually best to manage alert policies through the Purview compliance portal. A set of cmdlets is available in the compliance module:

- *Get-ProtectionAlert*: Reports the alert policies defined by the tenant.
- *Set-ProtectionAlert*: Amends an alert policy.
- *New-ProtectionAlert*: Creates an alert policy.
- *Remove-ProtectionAlert*: Removes an alert policy. You cannot remove one of the default alert policies.

For example, to list the set of default alert policies in a tenant, connect to the compliance endpoint with PowerShell and run the command shown below (output edited for space).

```
PS C:\> Get-ProtectionAlert | ? {$_._IsSystemRule -eq $True} | Format-Table Name, Category, AggregationType, AlertScenario
```

Name	Category	AggregationType	AlertScenario
Malware campaign detected after delivery	ThreatManagement	AnomalousAggregation	Protection
Unusual increase in email reported as phish	ThreatManagement	AnomalousAggregation	Activity
Unusual volume of external file sharing	DataGovernance	AnomalousAggregation	Activity
Elevation of Exchange admin privilege	AccessGovernance	None	Activity
Creation of forwarding/redirect rule	ThreatManagement	None	Activity

The *AggregationType* property tells us whether alerts trigger for every occurrence (*None*), based on the volume of the activity in a time window (*SimpleAggregation*), or when the volume of activity greatly exceeds the baseline for the tenant (*AnomalousAggregation*).

Searching for Alerts with PowerShell

Alerts are also recorded in the audit log and can be searched for using the `Search-UnifiedAuditLog` cmdlet. A [script available in GitHub](#) illustrates how to use the technique previously explained to interrogate the audit log for alert records and extract their content. As usual, the contents of the `AuditData` property of the audit records vary from activity to activity. Although this information is useful, the events do not contain details of the status of an alert and interpreting the `AuditData` property can be challenging. Better data is available through the Security/Alerts endpoint in the Graph. An example script showing how to extract current alerts from the Graph and post them to Teams is [available in GitHub](#).

Office 365 Cloud App Security

Office 365 Cloud App Security (OCAS) is a solution in the Microsoft 365 Defender portal. Previously known as Advanced Security Management, Cloud App Security is included in the Office 365 E5 product. It is a subset of the full Microsoft Defender for Cloud Apps product [tailored to process Office 365 audit data](#). Unless you use groups to scope the coverage of policies (see the section later), every user in the tenant must have a license for OCAS as it is not possible to exclude the audit data for individual users from the anomaly detection and analysis. OCAS keeps up to six months of data about user activities. Data collection begins after you enable OCAS for a tenant.

When a tenant opts to use OCAS, Microsoft uses the Office 365 app connector to link your tenant to a store in the Cloud App Security infrastructure. The link allows OCAS analytics to extract and analyze the tenant's audit data, which detects suspicious activity and other potential problems. It takes about a week after a tenant is enabled before a satisfactory model exists of its normal activity and builds a baseline to measure suspected anomalies against.

OCAS aims to give customers much better oversight about what is happening in their tenant based on the data accumulated in the audit log, with the major advantage of the approach being that no need exists to deploy agents or other software to support the gathering and analysis of the data to detect the threats that might lie in detected anomalies. Analyzing the audit data also reveals how the actions taken by individual users might compromise the security of the organization through suspicious behavior, such as someone downloading all the documents from a library holding confidential information within a brief period. During its analysis, OCAS considers other indications, such as suspicious IP addresses that might originate from anonymous proxies or known botnets.

OCAS allows administrators to create tenant-specific policies to fire alerts when specific events happen or when a specific pattern of action occurs. For instance, you could create a policy that will alert administrators by email or SMS whenever certain conditions occur. Microsoft includes many preconfigured anomaly detection policies to get the ball rolling. These policies cover common conditions that should cause suspicion, such as a user logging in from two places widely separated by distance within a brief period. You can add other anomaly detection policies to highlight specific activities that are of concern to the organization. For example, you could create a policy to look for attempted logins from IP addresses outside the corporate IP range. You can tailor policies to turn off or on different risk factors or to increase sensitivity to a risk.

In some respects, apart from the analytics used by OCAS to pick up suspicious activity by correlating events, the technology is not rocket science. You could argue that a skilled administrator who knows what is happening in their tenant can detect and resolve the same kind of issues highlighted by OCAS. The advantage of a solution like OCAS is its ability to handle massive quantities of information of the type generated by audit events and to reduce the mass down to what is important. A human can do this too, but will struggle with:

- The volume of data to process (especially as the environment scales).

- The time needed to recognize complex suspicious audit events and to learn the characteristics that mark new threats.
- The need to be consistent in the treatment of events.

It is also likely that the human administrator will forget that some events have happened (or not) in the past, so when something happens, they must consider the event on its merits. Computers are better at remembering things, so OCAS quickly recognizes when an event is rare (and therefore potentially out of the norm) or normal.

In addition, the machine learning that lies behind analytics is much faster at correlating events to detect suspicious activity. Once software learns what it should be looking for, it generally produces more consistent results than a human can, 24 hours a day, 365 days a year, which is why applying technology to automate the collection and validation of information drawn from multiple sources is a good approach to understanding the kind of threat introduced by how individuals behave.

Non-Analytics OCAS Features

In addition to its analytics function, Office 365 Cloud App Security includes:

- [Cloud App Catalog](#): Listing known cloud applications used when analyzing audit data to detect problems. You can sanction known and approved apps and highlight apps that you don't want tenant users to use.
- Files: List files shared by users in the tenant and the people who have access to those files. Filters allow administrators to focus on specific sets, such as files shared with external people from OneDrive for Business.
- OAuth Apps: List the set of registered and enterprise apps known in Entra ID and used within the tenant, together with their OAuth permissions and the accounts that use the apps. You can mark apps as sanctioned and ban others that you don't want people to use.

Remember that the zero trust principle means that everything is considered a potential problem unless verified by an administrator. Many of the items highlighted in these lists are perfectly safe.

Alerts

The Alerts section in the Microsoft 365 Defender portal lists alerts generated from OCAS analytics. Figure 20-6 shows a set of alerts. The highlighted alert is for a user who signed in from an unfamiliar location. This kind of alert often happens when people travel.

A variation on the theme is an alert for *"activity from infrequent country."* In other words, a user performs some activity from IP addresses that geolocation identifies for a country that the user doesn't normally work in. The alert shown in Figure 20-7 is an example. My normal location is in Ireland, but some activity originated in Denmark. As it happens, I know that this occurred because I attended a conference in Copenhagen. What is interesting here is the four IP addresses noted by Defender. The IP addresses and their geolocations are:

- 2603:10a6:10:d4::21 (Washington, USA).
- 212.129.76.29 (Offaly, Ireland),
- 62.199.211.12 (Copenhagen, Denmark),
- 212.129.87.106 (Offaly, Ireland).

When considering an alert, it's important to consider knowledge about the user (for instance, do they normally work from home or a company location and do they travel?) as well as the distributed nature of Microsoft 365. SharePoint Online embraced IPv6 addresses first, and the Washington (state) address is likely from a Microsoft datacenter located there. The two Offaly IPv4 addresses are for an Irish ISP that my home modem connects to, while we can account for the address in Denmark through known travel. All of this

proves that although Defender does a good job to surface potential issues, its intelligence does not cover all bases. Human insight and knowledge allow us to interpret the evidence presented by Defender and decide what alerts need action and those to disregard.

The screenshot shows the Microsoft 365 Defender interface. On the left, there's a sidebar with various icons. The main area is titled "Alerts" and displays a list of detected incidents. One specific alert is highlighted with a blue selection bar, which is for an "Unfamiliar sign-in ...". To the right of this list is a detailed view of this specific alert. The title of this view is "Unfamiliar sign-in properties". It includes a summary section with a lightning bolt icon, indicating "Medium" severity, "Unknown" status, and "New" type. Below this are sections for "Entity Name" (217.112.226.141), "Alert description" (mentioning unfamiliar sign-ins involving one user), "Incident details" (showing incident severity as Medium), and a summary of active alerts (4/4), devices (0), users (1), mailboxes (0), and apps (0). A "Linked by" section is also present.

Figure 20-6: Reviewing alerts signaled by Microsoft 365 Defender

This screenshot shows the Microsoft 365 Defender interface focusing on investigating unusual activity for a specific user. The top navigation bar shows "Alerts > Activity from infrequent country". The main pane displays an "Alert story" for a user named "tony.redmond" who has performed 4 logins. Below this is an "Important information:" section listing several points about the user's activity, such as being an administrator and using multiple IP addresses. To the right, there's a detailed view of the user "Tony Redmond" (Principal Architect at Redmond & Associates). It shows "User threat" metrics: 3 open incidents, 3 active alerts, 0 investigation priority, and an Azure AD identity risk level of "No user risk". There's also a "Go to user page" button.

Figure 20-7: Investigating unusual activity by a user

Resolving Alerts

Cloud App Security assigns alerts a severity of high, medium, or low risk and calculates the risk level using behavioral analytics to compare normal user interaction against audit data. The analytics are based on

Microsoft's collected knowledge about the threats that exist, and their origin gathered from across Microsoft 365 and other cloud services. Assigning a risk value allows an administrator to filter high-risk alerts and prioritize their resolution.

Another example of an alert is when Defender detects an account to have elevated permissions (a "New admin user" alert). Again, if the permissions were assigned purposely, the alert can be resolved, and OCAS knows that it does not have to signal the issue again. However, it could be the case that someone gains permissions in error or that they hold permissions for too long, in which case the resolution is different and might need the account to be suspended or to have its permissions adjusted. User accounts can also be suspended as an action contained in a policy to ensure that action is taken to protect the organization without needing an administrator to do something manually. Suspended users show up as blocked users. If this turns out to be the wrong thing to do, you can reverse the suspension from OCAS or the Microsoft 365 admin center.

An alert may highlight an event that is uninteresting or invalid. In these instances, you can dismiss the alert or mark it as a false positive. These actions are recorded in the Activity Log and the fact that the user's location or their admin status is valid is considered by OCAS when it processes audit events and other data to detect anomalies and suspicious activity in the future.

Filtered Alerts

OCAS supports activity log filters to focus an investigation on one or more of the Microsoft 365 applications or selected users. The latter filter is valuable when you might be concerned about the activities of a certain individual. You can also search for high, medium, or low severity alerts or for closed alerts. You can also filter by risk category (for example, access control or privileged accounts). The filters can be combined to focus on certain actions, meaning that even a very large volume of alerts can be quickly refined to produce a set of alerts that need to be examined. You can also export alerts to a CSV file if needed.

Activity Log

The screenshot shows the Microsoft 365 Defender Activity log interface. At the top, there's a navigation bar with icons for Home, Security, Compliance, and Admin, followed by 'Microsoft 365 Defender' and '55 for'. A search bar and a user profile for 'Tony Redmond' are also at the top right. Below the navigation bar, the title 'Activity log' is displayed. A message 'Investigate.6.months.back' is shown on the right.

The main area has a sidebar on the left with various icons for different services like SharePoint, OneDrive, and Teams. The main content area shows a table of activities:

Activity	User	App	IP address	Location	Device	Date
Modify file: file ...	Vasil Michev (Tec...)	Microsoft Share...	46.249.81.143	Bulgaria		9 May 2023 ...
Modify file: file ...	Vasil Michev (Tec...)	Microsoft Share...	46.249.81.143	Bulgaria		9 May 2023 ...

Below the table, there are sections for 'ACTIVE INCIDENTS' (1), 'MATCHES' (0), and 'ACTIVITIES' (122). It also shows 'USER ACTIVITIES (30 DAYS)' with a line chart and 'FREQUENT LOCATIONS' with a world map. A 'User' tab is selected in the navigation bar.

Figure 20-8: Browsing the OCAS Activity Log to review specific user activity

The activity log contains data from the audit log along with other logged items, such as those recorded when an administrator resolves or dismisses an alert. Data is available for the previous 30 days. Many activities generate a large volume of audit log entries, so you'll probably need to use filters to reduce the set to a manageable amount. In the example shown in Figure 20-8, filters extract events relating to file modification activities in SharePoint Online for a certain user. Note the **Save as** option to create a new policy based on the search criteria.

The active incident occurred because Vasil reviews all the chapter files for the book in depth yearly. This generates a spike in his activity that OCAS considers suspicious. Again, if you know what happens inside a tenant, it's easy to resolve these kinds of incidents.

Policies

The ability to create customized policies to check events and trigger alerts when predetermined conditions occur is one of the most powerful features in OCAS. Using templates or from scratch, you can create various policies to check for various kinds of activity captured in events, including:

- Access policy.
- Activity policy.
- App discovery policy.
- Cloud discovery anomaly detection policy.
- File policy.
- OAuth app policy.
- Session policy.

These policies help administrators to master the vast quantity of events that busy tenants generate. For example, a file policy can check for events when users share documents holding sensitive information with people outside the tenant. You can enable some Data Loss Prevention (DLP) checking to look for specific forms of data, like credit card numbers, and take governance actions, like reporting the problem to a site owner, if the checks discover someone sharing a file when they should not. Administrators can see the results of the policy in the dashboard and opt to receive updates via email or SMS text messages.

It is important to emphasize that OCAS does not replace the DLP policies that you can deploy for workloads. Investigators often review alerts sometime after the fact rather than being actioned at once rather than being brought to the attention of users through visual clues embedded in clients like Outlook or applications like Word. Instead, checking audit events for problems gives the tenant an added layer of protection. The same is true for governance as actions to prevent users from making mistakes are usually better taken through classification and retention policies deeply integrated into individual workloads.

One issue for customers located outside the U.S. is that OCAS is based on an Azure data store running in a [U.S., U.K., or European data center](#). Only audit data and information about tenant users and groups are moved to the Azure data store and personal information belonging to tenant users stays within the originating workloads. Microsoft plans to extend OCAS so that its data is stored in other data center regions in the future. When this happens, OCAS data for a tenant will reside in the same region as their other data.

SIEM integration with OCAS: You can integrate OCAS with third-party SIEM servers. A SIEM agent runs on the server to pull alerts from OCAS so that you can integrate its alerts alongside alerts generated from other parts of your IT infrastructure. Details of how to perform this integration [are available online](#).

Scoping Policies to Groups

If you only want to use OCAS to check the activities of a limited set of people, you can tailor policies to limit them to defined groups. These are OCAS groups rather than Entra ID groups. If you want to use Entra ID groups, you must import them into OCAS through the **User groups** choice in the Cloud Apps menu in the Defender portal. Once imported, you can edit OCAS policies and add a group as a filter. Because OCAS then scopes the alerts to just the users in the group, the licensing requirement for OCAS only extends to those users. Make sure that all policies are scoped to groups as otherwise you need to license every user in the tenant.

Third-Party Auditing Alternatives

Microsoft encourages ISVs to use the [Management Activity API](#) to access audit data through the Microsoft Graph and develop solutions that generate in-depth activity reports, including suspicious or out-of-norm actions, data visualization and analysis to aid planning and oversight for tenants, and to incorporate audit activity in operational dashboards. In short, these solutions will help tenants understand who is accessing their content and whether their compliance framework is working. Quest On Demand Audit is an example of a third-party solution that consumes audit data.

Apart from taking a different approach to reporting, ISV products often allow tenants to store audit data for longer periods. This is a big advantage for large enterprises that often need to hold audit information for years to meet regulatory requirements. Third-party solutions do not include some of the high-end machine-learning functionality and policy-driven event checking found in OCAS, but they are usually much cheaper and are therefore an interesting choice to investigate if you think a tenant needs more audit reporting and analysis functionality than found in Microsoft 365.

Exchange Online Administrative Auditing

Exchange administrative auditing is the mechanism used to track the operations performed by administrators when they invoke cmdlets to manage Exchange Online. Another way of putting this is that the audit entries allow the age-old question of “who did that?” to be answered. Administrative auditing is enabled by default for Exchange Online and tenants have little control over what is audited because Microsoft does not allow updates for most of the settings in the audit configuration.

Auditing is performed by the Admin Audit Log agent, which is active on every Exchange Online server. The agent evaluates cmdlets as they run against the audit configuration to decide whether the use of the cmdlet needs to be logged. If so, the agent creates an item holding details of the cmdlet and its parameters in the Inbox of the audit mailbox. The audit agent creates separate reports for each object if you execute an action that is performed against several objects. For example, if you use *Get-Mailbox* to fetch a list of mailboxes from a database and then use *Set-Mailbox* to place the mailboxes on litigation hold, the audit agent creates a separate audit event for each mailbox as it is updated.

The best methods available for searching Exchange administrative audit events are to use the Compliance portal or the *Search-UnifiedAuditLog* cmdlet.

Exchange Online Mailbox Auditing

While administrative auditing helps you understand who changed an administrative setting, mailbox auditing is the way to discover “who did what in that mailbox?” For instance, what account used delegate access to send a message on behalf of a mailbox, or who removed a message from a folder. The audit events captured by mailbox auditing are in three categories of access, each of which has a separate configuration:

- **Owner:** Operations performed by the mailbox owner. Normally, there is little point in auditing owner operations as the owner has full control over their mailbox. This was the situation in the on-premises world for many years, but when Microsoft decided to enable mailbox auditing by default, they also decided to enable auditing for owner actions to collect a complete set of audit events for mailboxes. The default configuration for owner actions includes *MoveToDeletedItems*, *SoftDelete*, *HardDelete*, *UpdateFolderPermissions*, *UpdateInboxRules*, *ApplyRecord*, *Send*, and *UpdateCalendarDelegation*. Where mailboxes are potentially exposed by a Business Email Compromise (BEC) attack, the *MailItemsAccessed* audit event provides more information about owner actions within a mailbox.
- **Delegate:** Operations performed by another user who has delegate access to the mailbox via the *SendAs*, *SendOnBehalfOf*, or *FullAccess* permissions. These actions are the usual focus for auditing, especially when multiple delegates have access to a shared mailbox or for mailboxes that hold confidential information, such as the copies of items retrieved by eDiscovery searches that are stored in discovery mailboxes.
- **Administrative:** Operations performed by programs that connect to the mailbox using special administrative access such as a content search.

When auditing is enabled for a mailbox, Exchange captures audit entries for a set of default events for each of the three access categories listed above and stores the data in the Audits sub-folder of Recoverable Items.

Mailbox Auditing by Default

Microsoft enables mailbox auditing by default for all mailboxes with appropriate licenses (Office 365 E3 and above). This means that Exchange Online captures audit records for a default set of actions performed by owners, delegates, and administrative processes in user, shared, and group mailboxes. Exchange Online doesn't support auditing for other kinds of mailboxes such as resource, public folder, and system mailboxes.

Apart from ensuring the consistent capture of audit records for mailboxes (including newly created mailboxes), the benefit of enabling mailbox auditing by default is that Microsoft manages the auditing configuration to make sure that the audit log ingests events for new mailbox actions as they become available. This situation happened in May 2024 when Microsoft added the *MailItemsAccessed* and *Send* events to the default audit configuration.

Before mailbox auditing is managed automatically, an administrator must update the Exchange Online organizational configuration to update the *AuditDisabled* setting to false. Here's an example of updating the setting and checking it afterwards:

```
Set-OrganizationConfig -AuditDisabled $false
Get-OrganizationConfig | Select-Object AuditDisabled

AuditDisabled
-----
False
```

To opt-out of default mailbox auditing and stop Exchange capturing any mailbox audit data for the audit log, make sure that the setting is *\$True*.

```
Set-OrganizationConfig -AuditDisabled $true
```

When the organization setting is *False*, auditing is enabled by default. In this state, you do not need to enable auditing for new mailboxes with Purview Audit advanced licenses because Exchange Online takes care of this action. It also means that Exchange Online captures the default set of audit records for all mailboxes, even if the *AuditEnabled* setting for a mailbox is *\$False*. In other words, Exchange ignores the *AuditEnabled* property for a mailbox when default auditing is enabled. If you want Exchange not to capture audit records for a mailbox, you run the *Set-MailboxAuditBypassAssociation* cmdlet as explained later.

Transmission of Mailbox Events to the Audit Log

When auditing is enabled for a mailbox, Exchange Online captures audit events in the *Audits* sub-folder of the *Recoverable Items* folder in the mailbox and transmits the events to the audit log. Administrators can then use the audit search functionality in the compliance portal, the *Search-UnifiedAuditLog* cmdlet, or the Graph *AuditQueryLog* API to search mailbox audit records along with the records generated by other workloads.

Microsoft documentation says that you must enable mailbox auditing for mailboxes belonging to accounts with Office 365 E3 licenses. Although mailbox auditing is enabled to allow the audit events to accumulate in the mailbox, using *Set-Mailbox* to enable mailbox auditing for a second time flips a switch to instruct Exchange Online to send the audit events to the audit log. Use [the steps described in this article](#) to make sure that all mailbox audit events flow as expected into the audit log.

Multi-geo audit searches: The Microsoft 365 substrate stores audit events in special Exchange Online mailboxes. For this reason, if you perform mailbox log searches with PowerShell for multi-geo organizations, make sure that you "anchor" the search in a region by [connecting to a mailbox in the target region](#). To create results from multiple regions, you can combine the events found in each region into a single array.

Audit Actions for User Mailboxes

Table 20-1 lists some of the actions configurable for capture in each access category. The [complete list of mailbox audit actions](#) is available online.

Action	Description	Owner	Admin	Delegate
<i>ApplyRecord</i>	Mark an item as a record by applying a record or regulatory record retention label.	Yes	Yes	Yes

Create	An item is created in the mailbox.	Yes	Yes	Yes
Copy	An item is copied to another folder.	No	Yes	No
FolderBind	A client opens a mailbox folder, including the original logon to the mailbox. Exchange consolidates folder bind actions and posts a single entry per folder every 24 hours.	No	Yes	Yes
SendAs	A message is sent from the mailbox using the SendAs permission.	No	Yes	Yes
SendOnBehalf	A message is sent from the mailbox using the Send On Behalf Of permission.	No	Yes	Yes
SoftDelete	An item is moved into Recoverable Items.	Yes	Yes	Yes
HardDelete	An item is permanently removed from Recoverable Items.	Yes	Yes	Yes
Update	The properties of an item are updated.	Yes	Yes	Yes
MailItemsAccessed	Messages are synchronized or opened by clients.	Yes	Yes	Yes
Move	An item is moved into another folder.	Yes	Yes	Yes
MoveToDeleteItems	An item is moved into Deleted Items.	Yes	Yes	Yes
MailboxLogin	The owner logs into the mailbox.	Yes	No	No
RecordDelete	An item marked as a record is soft-deleted.	Yes	Yes	Yes
Send	An email is sent (a crucial event). Must be configured before events are gathered.	Yes	No	Yes
UpdateCalendarDelegation	Record delegate permissions assigned to the calendar.	Yes	Yes	No
UpdateComplianceTag	A different retention tag is applied to an item.	Yes	Yes	Yes
UpdateFolderPermissions	Record changes to folder permissions, such as allowing a user to view a calendar.	Yes	Yes	Yes
UpdateInboxRules	Record changes to inbox rules.	Yes	Yes	Yes

Table 20-1: Mailbox actions captured for auditing purposes

The *HardDelete* action does not record audit events for items removed using the *Shift+Delete* key combination as this operation only bypasses the Deleted Items folder to move items directly into the Recoverable Items folder. *Shift+Delete* operations are logged as *SoftDelete* actions, which also happens when users remove items from the Deleted Items folder individually or by emptying the entire folder.

Odd Delegate Audit Records: You might find some audit records for *SendAs* operations by a delegate for a mailbox that you know has no delegates and wonder what's going on. The answer is usually when a background process impersonates the user to send email. For instance, this happens when Planner generates email notifications when creating new tasks or completing a task (the *ClientInfoString* property is "Client=REST," showing that Planner used the Graph API for this action). The messages that Planner sends are in the Sent Items folder of the mailbox. You can match them with the audit records.

Updating Mailbox Audit Configurations

To see what actions are captured for a mailbox, run *Get-Mailbox* to fetch details of the *AuditAdmin*, *AuditDelegate*, and *AuditOwner* properties together with the default audit setting for the mailbox:

```
Get-Mailbox -Identity "Customer Services" | Format-List Audit*, DefaultAuditSet
```

```
AuditEnabled      : True
AuditLogAgeLimit : 90.00:00:00
AuditAdmin        : {Update, MoveToDeleteItems, SoftDelete, HardDelete...}
AuditDelegate     : {Update, MoveToDeleteItems, SoftDelete, HardDelete...}
AuditOwner        : {Update, MoveToDeleteItems, SoftDelete, HardDelete...}
```

DefaultAuditSet : {Admin, Delegate, Owner}

The audit configuration listed above tells us that:

- Auditing is active for the mailbox.
- Exchange keeps audit items for 90 days.
- The set of actions captured for the three categories of access.
- Exchange uses the default audit set for each of the three categories. We know this because the three audit categories (Admin, Delegate, and Owner) are present. If any of the audit categories are missing from the list, you know that the mailbox has a custom audit configuration.

Arrays store the audit events configured for each type. To see the complete set of audit actions for a category, expand the property holding actions for the chosen type like this:

```
Get-Mailbox -Identity "Customer Services" | Select-Object -ExpandProperty AuditDelegate
```

```
Update
MoveToDeletedItems
SoftDelete
HardDelete
SendAs
SendOnBehalf
Create
UpdateFolderPermissions
UpdateInboxRules
ApplyRecord
```

You can change the set of actions by running the *Set-Mailbox* cmdlet. In this example, we add the *UpdateComplianceTag* action to the set of actions already configured for capture. It can take up to an hour before an updated configuration is effective. Remember that customizing the set of actions captured for an audit category stops Exchange from updating the set of default actions should Microsoft introduce new actions in the future.

```
Set-Mailbox -Identity James.Ryan -AuditOwner @{Add="UpdateComplianceTag"}
```

To disable auditing for a category, input “None” for the action list. Remember that if mailbox auditing is enabled by default for the organization, Exchange still captures the default set of actions in all three categories.

```
Set-Mailbox -Identity "Customer Services" -AuditDelegate None
```

Managing Default Mailbox Audit Configurations

When mailbox auditing is enabled by default for an organization, Exchange populates the *DefaultAuditSet* property. This property indicates if an admin has changed the default audit configuration set by Microsoft for the Owner, Delegate, and Admin categories for a mailbox. To examine the value run:

```
Get-Mailbox -Identity Kim.Akers | Select-Object DefaultAuditSet
```

```
DefaultAuditSet
-----
{Admin, Delegate, Owner}
```

Because the three categories are listed, you know that no change has been made. On the other hand, if you see:

```
DefaultAuditSet
-----
{Admin, Delegate}
```

You know that an administrator has added or removed an action from the Owner set. If an audit category is missing from the default set, you know that changes have occurred. When the default set is updated, Exchange Online won't update the audit configuration when Microsoft introduces new actions, so it's important to keep to the default set whenever possible and only make changes when necessary. If you want, you can reset mailboxes by running *Set-Mailbox*. In this example, we scan for mailboxes where the default set is not used and reset those mailboxes.

```
[array]$Mbx = Get-Mailbox -RecipientTypeDetails UserMailbox -ResultSize Unlimited | Select-Object
Alias, DisplayName, DefaultAuditSet
$Updates = 0
ForEach ($M in $Mbx) {
    $FullSet = $M.DefaultAuditSet[0] + $M.DefaultAuditSet[1] + $M.DefaultAuditSet[2]
    If ($FullSet -ne "AdminDelegateOwner") {
        $Updates++
        Write-Host "Updating" $M.DisplayName
        Set-Mailbox -Identity $M.Alias -DefaultAuditSet "Admin", "Delegate", "Owner" }
}
If ($Updates -eq 0) {Write-Host "No mailboxes updated"} Else {Write-Host $Updates "mailboxes updated
with default audit configuration"}
```

Mailbox Auditing Bypass

If you want to exclude mailboxes from auditing, you use the *Set-MailboxAuditBypassAssociation* cmdlet to tell Exchange Online not to collect audit events. For example:

```
Set-MailboxAuditBypassAssociation -Identity "Kim Akers" -AuditBypassEnabled $True
```

Set the value to \$False to disable mailbox audit bypass.

Tenant administrators often use the *Set-MailboxAuditBypassAssociation* cmdlet to stop audit events from service mailboxes flooding the audit log. This might have been acceptable in an on-premises environment when the cmdlet first appeared in Exchange 2010. Today, it is not recommended to exclude any Exchange Online mailbox from auditing in this manner. First, Microsoft 365 has much better tools available to search the audit log and a few extra audit events will make no difference. Second, when an account is excluded from mailbox auditing, Exchange does not capture events for any mailbox the account can access. An account could therefore open a shared mailbox and remove items in that mailbox without the recording of any audit data. Last, if you experience something like a Business Email Compromise attack, you need as much audit data as possible to collect to understand how the attack develops and what was its impact.

To see if any mailbox auditing bypasses are in place, run the *Get-MailboxAuditBypassAssociation* cmdlet and filter for accounts with a bypass. It is quite normal to have many mailbox association records returned, including records for guest user accounts and system accounts as these are created when new accounts are created in the tenant. For example, this command finds accounts with mailbox audit bypass enabled.

```
Get-MailboxAuditBypassAssociation | Where-Object {$_.AuditBypassEnabled -eq $True} | Format-Table
Name, WhenCreated, AuditBypassEnabled
```

Name	WhenCreated	AuditBypassEnabled
Kim Akers	02/12/2014 15:20:42	True

Auditing for Group Mailboxes

When mailbox auditing by default is enabled for an organization, Exchange Online captures audit records for the group mailboxes belonging to Microsoft 365 Groups. Although this includes the groups used by Teams and Viva Engage, most audit records come from groups accessed through Outlook. Unlike other mailbox types, you can't change the auditing configuration for group mailboxes. Table 20-2 lists the configuration used to capture audit records for group mailboxes.

Mailbox action	Owner	Delegate	Admin
Create		Y	Y
HardDelete	Y	Y	Y
MoveToDeletedItems	Y	Y	Y
SendAs		Y	Y
SendOnBehalf		Y	Y
SoftDelete	Y	Y	Y
Update	Y	Y	Y

Table 20-2: Audit configuration for group mailboxes

Reporting Workload Activity

Despite many requests over the years, Microsoft has never delivered good reporting facilities for on-premises applications. This statement was true in the early years of Office 365, but things have improved recently with analytics and usage data appearing in different admin portals. What hasn't changed is the fact that if you want to have truly flexible reporting over extended periods, you should consider ISV products. The Microsoft Graph is increasingly the source of truth for workload activity data, but other sources such as the audit log are also useful.

Graph Usage Reports: Microsoft generates a range of workload activity data [accessible through the Microsoft Graph](#). Data for all workloads is not yet available, but you can access information for Exchange Online, SharePoint Online, Teams, and OneDrive for Business.

Standard Usage Reports

The Microsoft 365 admin center includes a Reports section (Figure 20-9) offering a set of reports covering various workloads for fixed 7, 30, 90, and 180-day periods. Users do not need full administrative access to access the standard usage reports. Anyone assigned a workload administrator role like the Teams Service administrator, or the Global Reader or Report Reader administrative roles can access the usage reports (see the tenant management chapter).

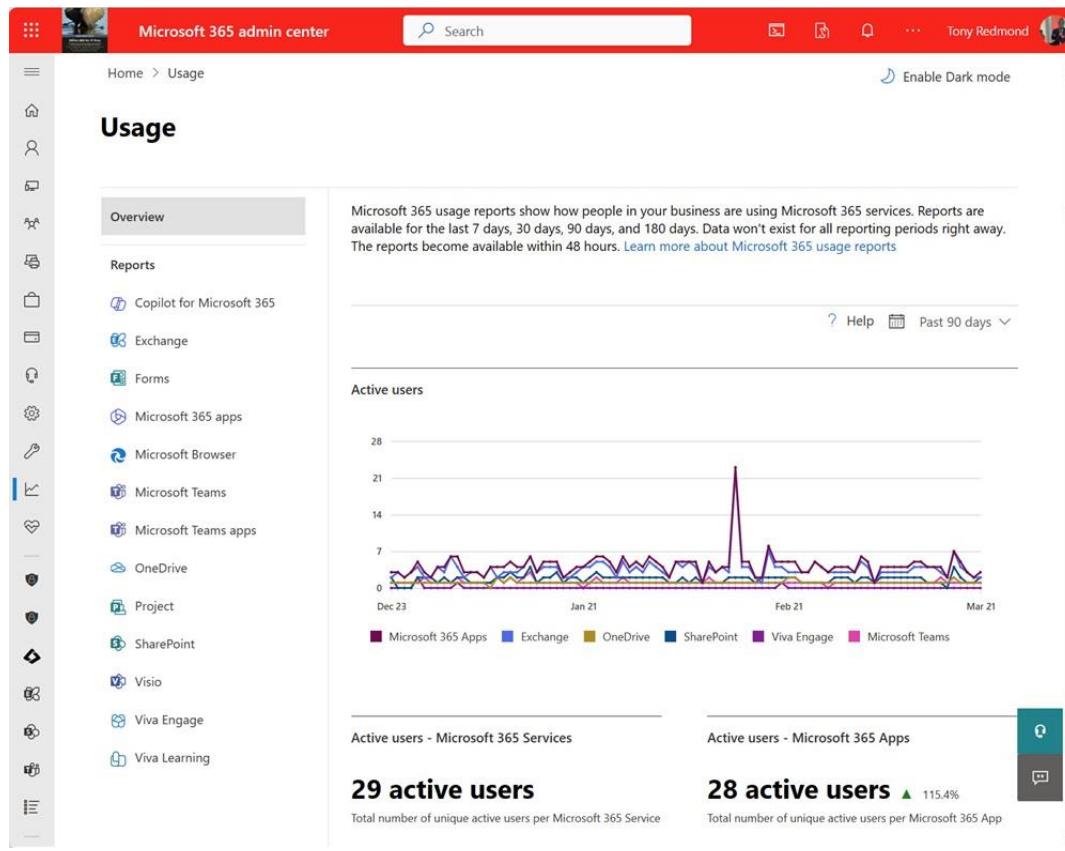


Figure 20-9: Standard workload usage reports for a tenant

The Microsoft 365 admin center features two types of reports:

- **Usage:** How much use people make of different workloads, like how many messages users send and receive using Exchange, meetings attended in Teams, or files viewed or edited with SharePoint. Some applications, like Planner, do not have usage reports, and some which do, like Teams, report a limited set of actions (mainly in chat and meetings) and don't include any insight into the other ways people interact with the app.
- **Adoption Score:** covering remote work elements. Microsoft introduced this section to help tenants understand the impact of employees working from home. The data focuses on collaborative activities (Exchange Online, Teams, Forms, and Viva Engage) and online document use (SharePoint Online and OneDrive for Business).

The detail and coverage of the reports available in the Microsoft 365 admin center have improved over time and deliver enough information to gain insight into user activity. Microsoft makes up to 180 days of reporting data available to tenants.

The reports for the individual workloads include a grid table containing individual user data. The table holds up to 2,000 entries and can be sorted by the different columns. You can also **Export** to save the report data to a CSV file (you'll need to export the data to sort and analyze user activity if your tenant has more than 2,000 accounts). If you want to preserve the graphics, you can either take a screenshot or use the browser's print to PDF choice to create a PDF file. It is also worth mentioning that you can access additional reports in other admin portals. For example, the Entra admin center has reports focusing on directory-centric activities such as password resets, anomalous sign-ins, and rights management, but they are useful in understanding the complete operating environment. The Teams admin center also includes a set of reports about various aspects of Teams usage.

The standard usage reports include a lot of information about how a tenant consumes resources, but the information is often quite high-level and not as granular as you might like. In addition, the reporting service makes data available for a limited timeframe, usually with a maximum horizon of 180 days, which makes the reporting information provided by the service difficult to use for long-term planning. You cannot go back any further to explore questions such as how much growth occurred in the last year or the last two years.

Reporting products often use PowerShell to retrieve more information from workloads and Entra ID to build out the data necessary to fill in the knowledge gaps. For example, it is all very well to know that a total of 55 distribution lists exist within a tenant, but it is even better to know the membership of each group and whether the groups are in active use or just taking up dead space in the GAL. To make long-term reports possible and to assure speedy access to information, reporting vendors often download tenant data periodically to repositories that they manage. The data is useful for analyzing trends such as the growth in mailboxes or messaging activity over time. Each product has its set of reports and its unique way to interpret and present information.

Extra reporting capabilities are enabled by Entra ID P1. For example, if you want detail about a [password-based activity](#) such as user account resets, your account must have an Entra ID P1 license to access that report. See the documentation for the [latest information about available reports](#).

Microsoft 365 Usage Reports Graph API

The [Usage Reports Graph API](#) supports programmatic access to many forms of Microsoft 365 activity data for different workloads including Exchange Online, SharePoint Online, OneDrive for Business, and Teams. This is the same data used for usage reports in the Microsoft 365 admin center, the Teams admin center, and the Microsoft 365 Usage Analytics for Power BI.

An example of using the API with PowerShell is [described in this article](#) about reporting the storage consumed by OneDrive for Business accounts. The technique used to download and interact with the OneDrive usage data can be replicated for other workloads. The PowerShell book contains more information about the Usage Reports Graph API.

Third-Party Reporting Products

Third-party reporting products make their money by offering a wider range of reports with a more granular level of detail than is available in the standard reports. They also usually give access to information gathered for more than the standard 180-day reporting window or incorporate data gathered from a variety of sources within a customer's IT environment. In comparison to the standard reports, which tend to focus on increasing usage of applications like SharePoint Online or Teams, ISV products often place greater emphasis on understanding what the data means and how to be more effective in areas like license management.

To stay in business, ISV offerings must be better than the reports delivered by Microsoft. Better analysis and insight into business operations are always welcome and this is exactly the advantage that you hope to gain by using a third-party product. To address the need to dive deeper into how workloads and users are performing, ISVs can use the same data from the Microsoft Graph used by the Microsoft 365 admin center to build tailored solutions to satisfy specific customer needs that the standard reports do not address. Some ISVs implement the concept of actionable reports, meaning that the report gives administrators the opportunity to take immediate action to address a problem highlighted in the report.

Anonymized Usage Reports Data

Some organizations are uncomfortable with the idea that people holding many administrative roles (including Report Reader) might be able to see sensitive data about user activity. For example, it is easy to discover how many messages the CEO sends and receives or how many Teams meetings he or she attends. Until September

1, 2021, the default for Microsoft 365 reporting was to show full information about users and groups. From that date, the usage reports in the Microsoft 365 admin center, Teams admin center, and anywhere else which uses the Microsoft Graph usage reports API display anonymized values. Figure 20-10 shows anonymized data in a usage report.

Details	Username	Last activity date (UTC)	Send actions	Receive actions	Read actions	Export
	F67CC8C15246EDCCA289C9A40...	14 September 2018	1,575	2,692	2,698	
	784DC33C0AA659D3342FBD75...	08 May 2017	0	233	0	
	ADEC9FD53F428E35D902BCAF1...	14 September 2018	35	227	574	
	E0E7E73A882A0726D7AAA872B...	25 July 2018	0	160	0	
	E885D8F6B229530E97F74C85D0...	14 September 2018	9	148	556	
	8ED6F13F8C692AA248DB43C3...	05 February 2018	0	111	0	
	D37C99D5BD92387FB8D6EDFB...	26 May 2016	0	100	0	
	B19ECE62B156C7C468E37F5B7...	18 May 2018	0	26	0	

Figure 20-10: Anonymized user data in the email activity report

Anonymization (also called deidentification, concealment, or obfuscation) means that the Microsoft Graph replaces the personal information for user accounts (like display names and user principal names), groups, and sites with system-generated obfuscated values (MD5 hashes) that cannot be easily associated with the underlying objects, including the object identifiers for items such as user accounts and groups.

If the organization decides that it is acceptable to display full user information, a global administrator can update the *Display concealed user, group, and sites names in all reports* setting in the **Reports** section of **Org settings** in the Microsoft 365 admin center. You can also update the setting programmatically.

Changing the concealment setting generates an *UpdatedUsageReportsSettings* audit record in the audit log. Because the setting governs the Microsoft Graph usage reports API, the concealment setting also applies to usage data fetched by scripts and programs which use the API. This code searches for instances where the concealment setting is updated. When this happens through the Microsoft 365 admin center, the audit record captures details of the user making the change, but changes made through a Graph API request do not.

```
$Records = Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-90) -EndDate (Get-Date).AddDays(1)
-Formatted -Operations UpdatedUsageReportsSettings
-ResultSize 5000 -SessionCommand ReturnLargeSet
If (!$Records) {
    Write-Host "No audit records found"
    Break
}
$Records = $Records | Sort-Object Identity -Unique | Sort-Object { $_.CreationDate -as [datetime] } -
Descending
$Report = [System.Collections.Generic.List[Object]]::new()
ForEach ($Rec in $Records) {
    $AuditData = ConvertFrom-Json $Rec.AuditData
    If ([string]::IsNullOrEmpty($Rec.UserIds)) {
        $UserId = "Graph API Request"
    } Else {
        $UserId = $Rec.UserIds
    }
    $ReportLine = [PSCustomObject]@{
        CreationDate      = (Get-Date $Rec.CreationDate -format "dd-MMM-yyyy HH:mm:ss")
        UserId            = $UserId
        Operation         = $Rec.Operations
        'Old Value'       = $AuditData.ModifiedProperties.OldValue
        'New Value'       = $AuditData.ModifiedProperties.NewValue
    }
    $Report.Add($ReportLine)
}
```

Note that some administrative roles such as Usage summary reports reader or Global reader can never see details of user activity, anonymized or not.

Using PowerShell to Create Reports

Administrators have used PowerShell for years to generate reports and many examples of scripts to produce nicely-formatted reports are available on the web. You can certainly use PowerShell to create custom versions of some of the standard reports to meet your specific needs. For example, we might want to know the size of user mailboxes. A quick PowerShell query reveals the answer:

```
Get-ExoMailbox -RecipientType UserMailbox -ResultSize Unlimited | Get-ExoMailboxStatistics | Sort-Object ItemCount -Descending | Format-Table DisplayName, TotalItemSize, ItemCount -AutoSize
```

DisplayName	TotalItemSize	ItemCount
Tony Redmond	4.116 GB (4,419,110,350 bytes)	36529
Jeff Guillet	1.62 GB (1,739,456,346 bytes)	10411
Vasil Michev (Technical Guru)	1.081 GB (1,161,234,561 bytes)	7019
Deirdre Smith	933 MB (978,334,934 bytes)	6207

Reports like this hold valuable data and are useful on an ad-hoc basis. However, when you set out to use PowerShell, you should realize that:

- PowerShell is an excellent method to query data but is less good when the time comes to format reports for printing. PowerShell can output data in CSV format for later processing in Excel to create charts or to do deeper analysis but generating a report and a few charts in Excel is different from creating a clear and well laid-out report.
- PowerShell has limited ability to analyze data over an extended period (the cmdlets that retrieve data from the reporting data mart sometimes do not give a very granular level of information).
- Microsoft 365 workloads often apply throttles to PowerShell scripts that attempt to process details of large numbers of objects. Throttling ensures that no job soaks available resources and so reduces service to other tenants. It is good if your script can avoid the need to call the *Get-ExoMailbox* cmdlet to create a set of mailbox objects for processing as this is a resource-intensive activity that becomes a candidate for throttling. One way around this is to create lists of mailboxes and store them in CSV files that other scripts can open and process.
- Some Microsoft 365 workloads do not support PowerShell or make their data available to PowerShell. Exchange Online has good coverage, but you will not be able to generate reports for other workloads except through the Graph. An example PowerShell script showing how to use the Usage Reports Graph API to generate activity reports for Exchange Online, SharePoint Online, OneDrive for Business, and Teams workload data and Entra ID user sign-in data is [available in GitHub](#). Even if the Graph usage data is always a couple of days behind, interrogating the usage data is usually much faster than attempting to retrieve statistics from a workload (an example of speeding up reporting of mailbox statistics is [described in this article](#)).

Finally, if you do create custom PowerShell reports, you must be prepared to check and potentially update them regularly to ensure that code does not break when Microsoft introduces updates to cmdlets, new functionality, or new versions of PowerShell. On the upside, some will like the challenge of writing and updating reports, others will find that it is easier and more efficient in the end to buy a reporting package from a company that specializes in this space, and it is always great to be able to reuse the many contributions of PowerShell scripts and code snippets that people make to the community to form the basis of your solution.

Microsoft 365 Usage Analytics for Power BI

Tenants can install a [Power BI template app](#) (previously known as the Office 365 adoption content pack) to help understand the usage patterns for several Microsoft 365 workloads. Usage analytics is a pre-built

dashboard of graphs and charts. You only need a basic Power BI license to access the dashboard. Together, the graphs and charts form a dashboard for a tenant divided into five areas:

- Executive Summary: A general view of workload usage across the tenant (Figure 20-11).
- Overview: A general overview of workload usage across the tenant.
- Activation/Licensing: How many licensed accounts are in the tenant, how many are active, and what devices they use.
- Product Usage: Usage of individual workloads like Exchange Online, SharePoint Online, Teams, Microsoft 365 Groups, and OneDrive for Business.
- User Activity: Different views of user activity within the tenant.

The current iteration includes good coverage of Exchange Online, SharePoint Online, OneDrive for Business, and Teams. It does not cover other applications like Stream or Planner (but does include Skype for Business Online). In effect, the dashboard covers usage of the base workloads rather than giving a comprehensive view of activities across all workloads.

The dashboard helps tenants understand the adoption rate and usage for various aspects of usage over the prior twelve months. For instance, how many people use SharePoint Online, Teams, and Exchange Online – or all the covered applications. This kind of information can tell you if you have a license management problem where people have licenses for an application that they do not use.

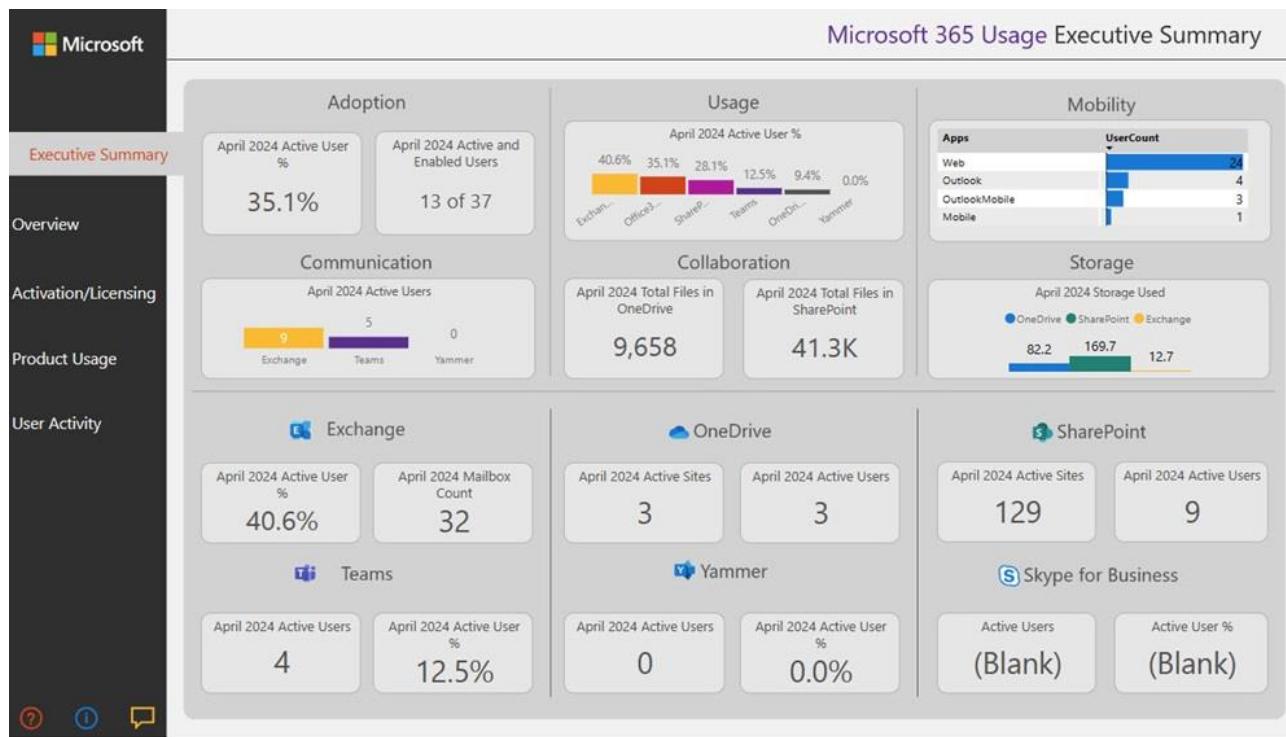


Figure 20-11: Microsoft 365 Usage Analytics dashboard

Another use of the dashboard is to look at usage trends, such as whether email traffic increases over time. These insights into what is happening within the tenant can help you to understand changes in user behavior. For instance, if you make a determined effort to convince people to store documents in SharePoint and OneDrive and access the files there rather than attaching them to email for circulation within the company, a steady uptick in file storage should result. If it does not, then the campaign is unsuccessful, and you might need to take a different approach to convince people to use “cloudy attachments.” Another example is in Teams, where a reduction in email traffic should match an increase in minutes consumed in instant messaging and conversations. Still another is to measure whether the introduction of Teams causes users to move some of their collaboration with fellow employees away from email to conversations within team channels.

Microsoft gathers data from across workloads to aggregate and refines the data to refresh the dashboard. The content pack updates weekly by default, but the backend service refreshes data daily, so a tenant can amend the dataset scheduled refresh interval to receive daily updates. The actual data lags the current date by between 36 and 48 hours as Microsoft needs this time to gather information and process it for the dashboard. Given the scale of Microsoft 365 and the amount of data that must be processed to generate aggregate statistics for tenants, this delay is understandable. The setting for anonymized data for reports governs whether usernames or anonymous identifiers appear in the dashboard.

Independent Reporting Products

Few tenant administrators are skilled at generating easy-to-read reports that highlight important data. Programmatic access to the Reporting DataMart is available to allow software developers to use the data belonging to tenants if tenants grant permission for this access. The intention is to allow vendors who specialize in software monitoring and reporting to incorporate usage data into their products to give customers a much better view of what happens inside a tenant than you can get using the basic reports. Apart from the obvious goodness inherent in having a common repository to consult to retrieve operational data about Microsoft 365, the combination of Reporting DataMart and choice of APIs (including PowerShell and the Microsoft Graph) avoids the need for people to create personal methods to extract information.

The number of independent software vendors who create reporting solutions continues to expand. Most of the ISVs that offer reporting solutions focus on pure cloud environments while some include monitoring and reporting for on-premises servers or non-Microsoft cloud workloads. Each product plays to its strengths and employs different approaches to data extraction, analysis, and reporting. Among the criteria you can use to figure out whether you need to use a third-party product instead of the standard usage reports include:

- **Data longevity:** Microsoft stores tenant reporting data for 180 days. This might be insufficient for your needs if you want to chart the usage of applications over a longer period for planning and analysis purposes. Ask for how long the vendor stores tenant reporting data. In addition, ask about the security and privacy controls that are in place to ensure that tenant data cannot be compromised. Ask about how often the product refreshes data from Microsoft 365 workloads to understand how up-to-date the reports are.
- **The number and type of reports:** A limited set of standard usage reports are available in number and in what they report. For example, there are no reports for mobile device usage, perhaps because Microsoft would prefer tenants to use Microsoft Endpoint Manager for mobile device management. A third-party reporting vendor is likely to have hundreds of different reports in their product.
- **Intelligent views:** Looking at a single workload is interesting if you want information about that application, such as the number of active mailboxes in Exchange Online. Things become more interesting when you can compare data extracted from one workload against another. For example, if you have a project to make more use of OneDrive for Business, you will be interested in the number of sites in use and the files and quota used in those sites. It is also interesting to know if the growing use of OneDrive affects email volume and usage.
- **Filtering and Pivoting:** Viewing tables of data through a browser is acceptable for small tenants but rapidly becomes problematic when the number of reported objects grows. For instance, it is difficult to make sense of a table holding details of thousands of mailboxes. The ability to use filters and to view data through pivot tables are huge advantages for large tenants.
- **Access:** The reports available in the Microsoft admin center need some level of administrative access. This is inconvenient when users other than administrators want access too. For instance, a company might want to charge back costs for Exchange Online mailboxes to the operating units of the business. This activity is usually performed by accountants, not tenant administrators, so removing the requirement to have administrative permissions to be able to access reports can be very useful.

- **Delivery:** Not everyone wants to browse a website to access reports. Some products allow reports to be automatically extracted and emailed to users on a scheduled basis.
- **Scale:** How well does the product scale up to deal with the predicted full load of the tenant? Good demos performed against a 5-user tenant might not be so impressive when confronted with the data generated by 20,000 users.
- **Support:** How is support provided? Is support available locally?
- **Cost:** How is the cost of the product calculated?
- **Deployment:** Is any extra software needed to create or view the reports? Is the product fully web-based or do you have to install some software on a workstation or servers to access the reports?

No one product is the best choice for every situation. The best approach is to spend the time to test the software in your environment and make the decision based on what you discover there.

Gaps and changes: All third-party reporting products and Microsoft's reports use a single source of truth: the reporting data collected for a tenant. Some third-party products copy that data so that it is retained for longer periods and to perform additional analysis. You should be aware of two issues regarding reporting. First, the data can change because of a change made by Microsoft. This is what happened when Microsoft changed the way that the *Get-MailboxStatistics* (or *Get-ExoMailboxStatistics*) cmdlet reported system messages stored in user mailboxes (described in the Exchange Online chapter). Second, hiccups and operational glitches sometimes prevent the ingestion of workload data to the reporting data mart, which then creates gaps in reports. Sometimes the gaps are filled in after normal service is restored, sometimes the gaps remain. Keep your eyes open and make sure that if a gap appears, you make Microsoft and/or the third-party reporting vendor aware of the issue.

Chapter 21: Power Platform

Christina Wheeler

The Microsoft Power Platform helps individuals and organizations develop and deploy business applications. In an era where agility and innovation are key to staying competitive, the Power Platform provides a suite of tools that enable the creation of robust solutions with minimal coding effort. This platform is designed to democratize the app development process, empowering professional developers and business users, often called citizen developers, to create, automate, and optimize business processes.

Building No-Code/Low-Code Solutions

The Microsoft Power Platform is a suite of no-code/low-code tools and services that enable users to build custom business application solutions. It encompasses five main products: Power BI, Power Apps, Power Automate, Copilot Studio, and Power Pages (Figure 21-1). These services allow individuals and organizations to create solutions to automate processes, analyze data, and develop intelligent applications without extensive coding knowledge or expertise. The Power Platform is based on Dataverse, an underlying data platform built on SQL Server and used by [Dynamics 365](#). Dataverse provides a unified data schema that ensures applications and services can interoperate seamlessly, allowing for efficient data management and integration across the platform.

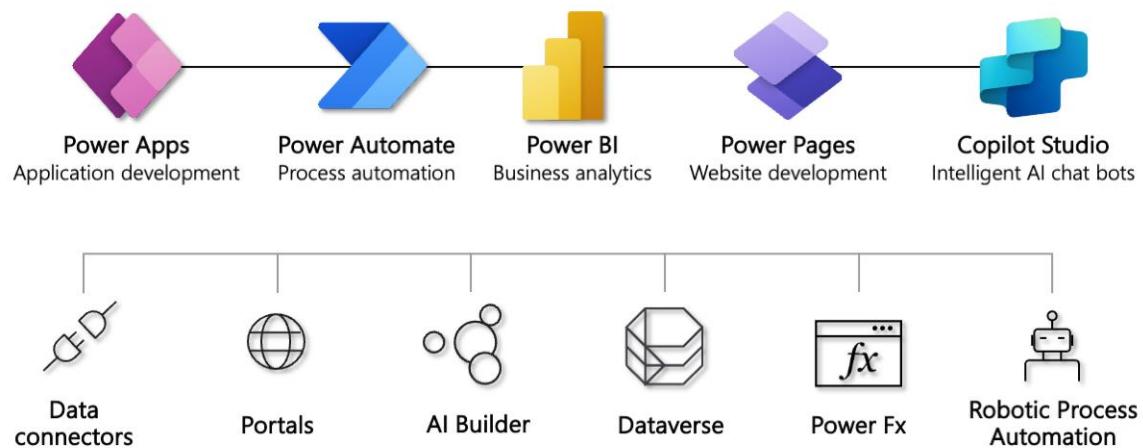


Figure 21-1: Power Platform components

The main Power Platform components are:

- **Power Apps**: Allows app makers to create web and mobile applications using a visual (drag-and-drop) interface that can connect and interact with over 1,400 data sources.
- **Power Automate**: A workflow automation service enabling users to create automated workflows that integrate processes across different systems and applications.
- **Power BI**: A data visualization and business intelligence tool that allows users to connect to data sources, create interactive dashboards, and generate reports and insights.
- **Copilot Studio**: Enables the creation of chatbots without writing code using a graphical interface, natural language understanding capabilities, and pre-built templates.
- **Power Pages**: A website-building tool enabling users to build external-facing websites backed by Dataverse that can have anonymous and authenticated users.

The Power Platform services can connect to different data sources through data connectors. Data connectors are wrappers around REST APIs (Application Programming Interfaces) to connect other services and interact

with the Power Platform components. Over 1,400 prebuilt connectors are available to connect to Microsoft and non-Microsoft services, including SharePoint Online, OneDrive for Business, ServiceNow, Salesforce, Dropbox, and more. If there is a service you need to communicate with that doesn't have a prebuilt connector, you can create your own custom connector in the Power Platform.

This suite of tools and services allows for a wide range of automation and integration possibilities, making it a powerful platform for businesses looking to streamline their operations and improve efficiency without extensive coding knowledge.

Microsoft 365 Developer Program

Before diving into the Power Platform, the Microsoft 365 Developer Program is worth mentioning. By signing up for this program, you can access a free, pre-configured Microsoft 365 tenant (without Windows) that includes 25 E5 licenses. This tenant is renewable every 90 days based on usage, providing an excellent sandbox environment for learning, building prototypes, or testing new features. It includes all necessary tools for Power Platform development.

As of February 2024, this program is available to developers and organizations with an active Visual Studio Developer Enterprise subscription. Additionally, you can sign up for a free Power Apps Developer Plan, which can be added to a free development tenant, another existing tenant, or set up as new. For more information and to sign up, visit the [Microsoft 365 Developer Program](#) and the [Power Apps Developer Plan](#).

Power Platform Administration

It is essential to understand the administration side of the Power Platform, even if your role may not include being the Power Platform Administrator. The [Power Platform admin center](#) is the centralized portal for administration tasks related to the Power Platform. However, there are other areas within Microsoft 365 where administrators interact with the Power Platform, including:

- **Power Apps Maker Portal:** [The Power Apps Maker portal](#) provides non-administrator accounts access to Power Apps, enabling users to create and manage their applications.
- **Microsoft 365 Admin Center:** This center manages various aspects that affect the Power Platform, such as user accounts, licensing, and auditing. This ensures administrators can control and monitor how the Power Platform is used across the organization.

The Power Platform admin center constantly evolves, with new features and capabilities added regularly. Here are the current capabilities you will find in the latest release:

- **Environments:** Displays a single list of all environments within your tenant. You can sort on properties, search across environments, create/open environments, and access environment settings.
- **Environment Groups:** This allows you to organize your environments into groups and govern them in bulk by applying rules.
- **Advisor:** Provides personalized recommendations to optimize your Power Platform tenant. It analyzes Managed Environments and the apps within these environments to suggest solutions that enhance security, reliability, and overall health.
- **Security:** Currently in preview, the Security hub offers recommendations for admins to improve their security posture.
- **Analytics:** Provides detailed reports for Dataverse, Power Automate, and Power Apps, with key metrics such as user activity, entity usage, flow runs, errors, and service performance. It also includes data export capabilities to Azure Data Lake.
- **Billing:** Provides a summary of tenant environments requiring licensing attention.
- **Settings:** Administrators can configure tenant-wide settings, such as enabling/disabling Copilot (preview) features, configuring who gets weekly digest notifications, and managing who can create

developer, production, and trial environments. Additional settings include allocating add-on capacity to environments, enabling/disabling tenant-level analytics, customer lockbox, publishing bots with boosted conversations, and configuring desktop flow actions in DLP policies.

- **Resources:** Allows administrators to view and manage the capacity used across [storage types](#) within the tenant. This includes Dataverse, Teams, trial environments, and managing add-ons. It also lists available Dynamics 365 apps for installation and configuration in enabled environments.
- **Help and Support:** Provides a list of self-help support and recommendations for Dynamics 365, Power Apps, and Power Automate, including the ability to open a support ticket if necessary.
- **Data Integration:** Enables administrators to [integrate data into Dataverse](#), supporting data integration between Dynamics 365 Finance and Operations and Dataverse, as well as integrating data into Finance and Operations and Dynamics 365 Sales.
- **Data (Preview):** This allows administrators to view a list of DirectQuery and Import datasets and dataflows used via the cloud or on-premises data gateway. Administrators can also manage gateways, including setting up gateway clusters for load balancing.
- **Policies:** This section allows for creating and maintaining Data Loss Prevention policies, defining what data can be shared with which connectors, and controlling usage in flows and apps. Additional settings include tenant isolation, customer lockbox, enterprise policies, and billing policies.
- **Admin Centers:** This section contains links to Entra ID, Microsoft 365 Admin Center, and the Power BI admin portal.

Power Platform Admin Center Updates

Recent Power Platform admin center includes the following:

- **Improved Analytics for Dataverse, Power Automate, and Power Apps:** The admin center offers comprehensive analytics, including metrics for user activity, entity usage, flow runs, errors, and service performance. These metrics help administrators gain insights into the usage and performance of their Power Platform environments.
- **Data Export to Azure Data Lake:** Administrators can export analytics data directly to Azure Data Lake. This feature supports advanced data analysis and reporting using Azure's powerful analytics tools.
- **Security Enhancements:** The Security hub, currently in preview, provides recommendations for improving the security posture of Power Platform environments. It includes features like IP restrictions, enhanced encryption, and advanced auditing capabilities.
- **Billing and Licensing Management:** The billing section includes a detailed summary of tenant environments requiring licensing attention. Administrators can manage licenses more effectively, ensuring compliance and optimizing costs.
- **Resource Management:** Resource management tools allow administrators to view and manage the capacity used across different storage types within the tenant. This includes managing add-ons, monitoring storage usage, and ensuring environments operate within capacity limits.

These updates increase the administrative capabilities within Power Platform, providing more control, visibility, and security for organizations.

Environments

Power Platform environments are logical containers that enable organizations to manage and isolate their business applications, data, and users. An environment serves as a space to store and organize the organization's flows, apps, chatbots, connections, custom connectors, and gateways in a geo-located manner. This means the flows and apps that live within an environment are available in the region where the environment is located. Environments separate resources based on different roles, security requirements, or

target audiences. This is especially important if the organization must observe a region-specific regulation such as the EU General Data Protection Regulation (GDPR).

When a flow or app is created in a specific environment, it is routed to all data centers in that geographic region, which could enhance performance. Multiple environments can be created in one physical region to establish boundaries within the same geographic area, allowing different users and policies to be assigned to environments in the same region.

If the environment is deleted, all resources (flows, apps, connections, custom connectors, and gateways) within the environment are removed. Likewise, because the environment is the isolation boundary for all resources that reside in a specific environment, you can never refer to resources across environments. For instance, you cannot create a custom connector in one environment and use it in a flow in a different environment. However, exporting a flow or app from one environment and importing it into another is possible.

The types of environments available are:

- **Sandbox:** A non-production, isolated environment for development and testing separate from production. Requires 1 GB of available database capacity.
- **Production:** Intended as a permanent environment for production apps, flows, and chatbots. Requires 1 GB of available database capacity.
- **Trial (subscription-based):** This type of trial has an extendable end date and is intended for developing more extensive, multi-user solutions and proofs-of-concept.
- **Trial:** This is a standard trial intended for trying new features. It is limited to one user and expires after 30 days. The trial plan allows users to extend the trial period two more times after the initial 30 days have ended for an entire trial period of up to 90 days. After the full trial ends, Microsoft disables and deletes the environment.
- **Developer:** Available for users with a Developer Plan license, intended for building and testing premium features of Power Automate, Power Apps, and Dataverse. You can create up to 3 developer environments. In the Power Platform administration center, administrators can control the creation of developer environments by imposing restrictions. Developer plan environments will stay active as long as they are actively being used. Any developer environment that remains unused for 90 days will be automatically deleted after notifying the respective environment owners. For features and capacity limits of developer environments, visit [Which features are included in the Power Apps Developer Plan?](#).
- **Dataverse for Teams:** These environments are created automatically when a Power App is created within Teams for a selected team. To learn more about Dataverse for Teams environments, visit [About the Microsoft Dataverse for Teams environment](#).

You can create an environment with or without a Dataverse database. To learn more about creating an environment in the Power Platform admin center, read [Create and manage environments in the Power Platform admin center](#) and [7 Mistakes To Avoid When Creating A Power Platform Environment](#).

Managed Environments

Managed Environments is a premium suite of capabilities designed to help admins manage the Power Platform at scale, offering greater control, reduced effort, and enhanced insights. Admins can apply Managed Environments to any type of environment. When a Managed Environment is enabled, specific features can be configured. Once an environment is managed, it unlocks additional features across the Power Platform.

Here is a list of key features of Power Platform managed environments:

- **Enhanced Security and Data Isolation:** This option offers stronger security controls and data isolation, including data loss prevention policies, data residency options, and compliance certifications, to ensure data privacy and regulatory compliance.
- **Data Policies (DLP):** Enforces data loss prevention policies to control which connectors can be used and how data can be shared within and across environments.
- **IP Firewall:** Limits access to Dataverse data by restricting IP addresses that can connect.
- **IP Cookie Binding:** Enhances security by binding session cookies to IP addresses to prevent cookie replay attacks.
- **Customer Managed Key (CMK):** Allows customers to manage their own encryption keys for data security.
- **Extended Backup:** Provides extended data backup options for better disaster recovery.
- **Limit Sharing:** Admins can restrict app and flow sharing to certain security groups or set a maximum number of individuals an app can be shared with.
- **Solution Checker:** Enforces best practice rules for solutions, ensuring compliance and quality before deployment.
- **Pipelines in Power Platform:** Supports deployment pipelines for managing the application lifecycle.
- **Weekly Usage Insights:** This feature provides admins with a weekly digest of usage insights, helping them identify inactive resources that can be cleaned up.
- **Export Data to Azure Application Insights:** Enables exporting of monitoring data to Azure for detailed analysis.
- **Administer the Catalog:** Facilitates administration of app catalogs for better resource management.
- **Default Environment Routing:** Allows routing of default environments to ensure appropriate usage.
- **Tenant-Level Administration:** Allows organizations to have dedicated administrators who can manage the environment and its resources at the tenant level, with elevated permissions to configure settings, manage security, and control access to applications and data.
- **Environment Lifecycle Management:** Provides capabilities for environment lifecycle management, including creation, cloning, refresh, and deletion of environments, facilitating the creation of sandbox environments for development and testing, and seamless movement of applications between environments.
- **Service-Level Agreement (SLA):** This comes with a service-level agreement that guarantees a certain level of availability and performance for the platform services within the environment, ensuring a reliable and consistent experience for users and applications.
- **Centralized Administration and Governance:** This is managed centrally through the Power Platform Admin Center or the Power Platform Management API, offering a unified view of all managed environments and enabling consistent administration, governance, and monitoring practices.
- **Cost Management:** Cost management features allow organizations to track and control the usage and consumption of resources within the environment, helping optimize costs and ensure efficient utilization of Power Platform resources.
- **DLP for Desktop Flow:** Extends data loss prevention policies to desktop flows.

With the latest updates, Managed Environments have capabilities designed to enhance the governance and control of Power Platform environments at scale. Here are the most recent feature updates and improvements:

- **Advanced Data Loss Prevention (DLP) Policies:** Managed Environments now support more granular DLP policies, allowing administrators to control data flow between connectors more precisely. This ensures sensitive information is handled according to organizational policies and regulatory requirements.

- **Managed Environment Analytics:** Administrators can access detailed analytics and reports on the usage and performance of environments within the Managed Environments suite. These insights help identify trends, monitor resource utilization, and optimize performance.
- **Solution Histories:** This new feature allows administrators to track changes made to solutions over time. It provides a historical view of modifications, making it easier to audit changes and maintain compliance.
- **Environment Insights and Alerts:** Enhanced insights and alerting capabilities provide real-time monitoring of environment health. Administrators can set up alerts for critical issues, ensuring timely responses to potential problems.

Power Platform managed environments are particularly suitable for enterprise-scale deployments and organizations with strict security and governance requirements. They provide a robust and controlled environment for building, deploying, and managing Power Platform applications and services. To learn how to enable managed environments, visit [Enable Managed Environments](#).

Considerations When Creating a New Environment

Anytime you create a sandbox or production environment with a Dataverse database, you can add Dynamics 365 apps (such as Dynamics 365 Sales and Field Services) during the creation process. Below are some points to consider when creating a new environment:

- **Creating an environment without a database** - If you do not plan to use Dynamics 365 apps and only need to create Power Apps and Power Automate flows using other data sources, you can create an environment without a Dataverse database. This is suitable for scenarios where Dataverse is not required, and other data sources will be utilized instead.
- **Creating an environment with a database** - If you are using Dynamics 365 apps or plan to use them in the future, you will need to create an environment with a Dataverse database. During the creation process, if you need to use Dynamics 365 apps ensure you select the option **Enable Dynamics 365 apps**. This feature can only be enabled during the provisioning of the database for a sandbox or production environment. The account must have the appropriate permissions to install Dynamics 365 apps into the environment.

Environment Permissions

By default, Power Platform environments without a Dataverse database include two built-in permission roles that provide access within an environment:

- **Environment Admin:** This role allows users to perform all administrative actions within an environment. This includes adding or removing users or groups from the Environment Admin or Environment Maker roles, provisioning a Dataverse database, viewing and managing all resources created within the environment, and setting data loss prevention (DLP) policies.
- **Environment Maker:** This role enables users to create resources within an environment, such as apps, connections, custom connectors, gateways, and Power Automate flows. Environment Makers can also distribute the apps they build within an environment to other users within the organization by sharing the app with individual users, security groups, or all users within the organization.

In environments with a Dataverse database, the **System Administrator** role replaces the **Environment Admin** role for full administrator privileges. For users who need to create apps that connect to a Dataverse database, assigning the **System Customizer** role and the **Environment Maker** role is necessary.

Security roles determine the access levels of various users to different types of records. Managing access to data and resources involves creating or modifying security roles, which allows for adjustments to the roles assigned to users. Users may be assigned multiple security roles, with privileges accumulating across these roles. The combined privileges from all assigned roles determine the access granted to users.

Understanding and appropriately assigning these roles is crucial for effective environment management. It ensures that users have the necessary permissions to perform their tasks while maintaining security and governance policies.

To view a list of security roles in an environment, navigate to the [Center](#). Select **Environments**, then choose the desired environment. Click the **Security** roles link on the environment overview page or go to **Settings > Users+ > Permissions > Security roles**.

A security role comprises record-level privileges and task-based privileges falling into three categories:

1. **Table Privileges:** These [privileges](#) define the tasks a user with access to a table record can perform. Tasks include Read, Create, Delete, Write, Assign, Share, Append, and Append To. "Append" involves attaching an additional record, such as an activity or note, to a given record, whereas "Append To" pertains to being attached to a record. Set table privileges accordingly.
2. **Miscellaneous privileges:** These task-oriented permissions allow a user to perform specific non-record-related tasks. Examples include publishing articles or activating business rules. Explore more about miscellaneous privileges to understand their scope and application.
3. **Privacy-related privileges:** These privileges authorize a user to execute tasks involving data integrated, downloaded, or exported outside of Dataverse. Examples include exporting data to Microsoft Excel or printing.

Every category of privilege type has its own tab. Within each tab, you can filter the view according to all privileges, assigned privileges, or unassigned privileges specific to the chosen security role.

To learn more about how to configure user security in an environment, visit [Configure user security in an environment](#).

Default Environment and Environment Details

When a tenant is provisioned, a default environment is created regardless of the license type. All users share this default environment, and any licensed user can create flows and apps within it. You cannot delete, backup, or restore the default environment. The default environment includes:

- 3 GB of Dataverse database capacity
- 3 GB of Dataverse file capacity
- 1 GB of Dataverse log capacity

The Environments page allows you to view the properties of the default environment or any other environment you created. To do this, select the environment you want to view from the Environments list to open its properties page. The first panel exposes **Details**.

It's important to note that the default environment does not automatically include a Dataverse database. You will know a database hasn't been created if you see the **Add Dataverse** section (Figure 21-2). When a database is not created, the **Access** section (defining who has access to the environment) offers two options for environment roles: *Environment Admin* and *Environment Maker*.

To create a database, click **+ Add Dataverse**, select the desired options, and click **Add**. This process provisions the necessary Dataverse database within the environment, enabling further capabilities for managing and storing data.



Figure 21-2: Environment properties of a Trial environment with Add Dataverse section

After creating the database, you will see the **Version** and **Updates** sections (Figure 21-3). Notice that the **Access** section changes from **Environment Admin** and **Environment Maker** to **Security Roles, Teams, Users**, and **S2S Apps**. The third panel (**Resources**) shows Flows, Power Apps, Portals, and Dynamics 365 apps configured in the environment.

The screenshot displays two panels. The left panel, titled 'Version', contains the 'Dataverse version' (9.2.24044.00222). The right panel, titled 'Updates', shows '2024 release wave 1' status ('On'), a link to 'See what's new in the release', and a 'Deployment Schedule' link.

Figure 21-3: Environment properties with Version and Updates sections

Best Practices for Setting Up Environments

It is common practice to set up separate environments for development, testing, and production. Microsoft recommends the following best practices: use the default environment for personal productivity apps, use a production environment for enterprise apps, and create separate environments for development, testing, and production stages to ensure proper management and deployment workflows.

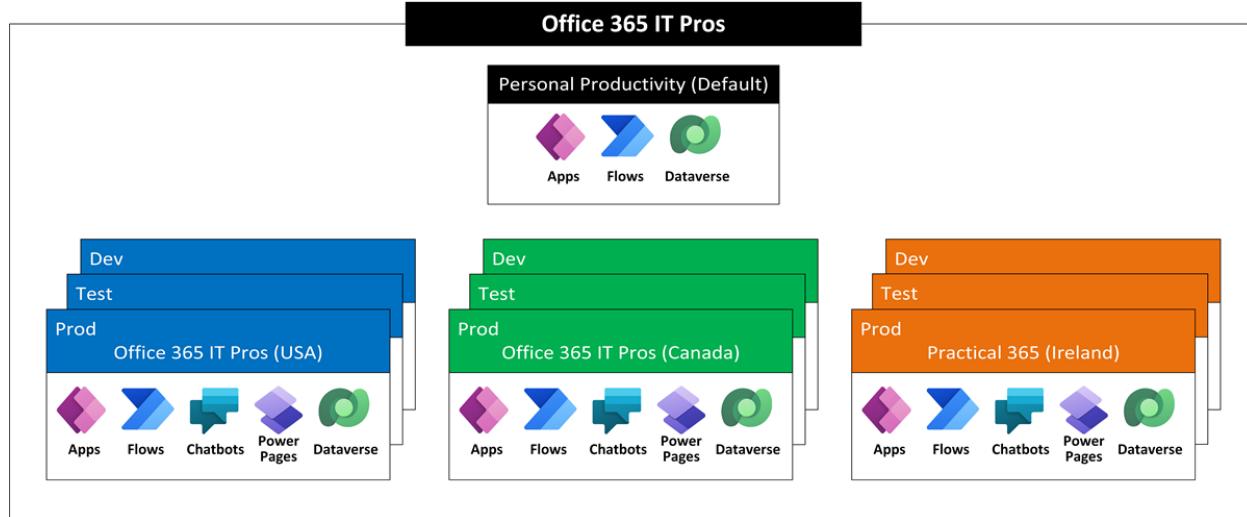


Figure 21-4: Environments example for dev/test/prod and Personal Productivity (Default)

By structuring environments in this way, you can isolate different stages of application development and deployment, which helps maintain control, security, and compliance across your organization. For example, you can create environments for each region of your organization, with each region having its own development, testing, and production environments (Figure 21-4).

This approach allows for a clear separation of concerns, ensuring that changes in development do not affect the stability of the production environment and that testing can be conducted in an environment that mirrors

production as closely as possible. By following these best practices, you can achieve better organization, improved security, and more effective management of your Power Platform resources.

Storage

Dataverse (formerly known as the Common Data Service or CDS) is a secure, cloud-based storage solution used by the Power Platform. It utilizes a combination of Azure SQL Server and Azure Blob Storage, hosted in the Azure Cloud, to store data. Dataverse includes a standard set of tables, columns, and rows, such as Accounts, Contacts, and various activity types, that are extensible, allowing tenants to add additional data columns to meet their business needs. Tables can create relationships with each other, and business rules can be established to make fields required, hide fields, and set default values. Each environment can have zero or one Dataverse database.

The Power Platform environment requires at least 1 GB of storage space. Each tenant has one default environment, which initially includes 3 GB of Dataverse space. Additional environments require extra storage that can be purchased in 1 GB increments. If the default environment exceeds its storage capacity, the administrator receives a notification about over-capacity usage, and a message is displayed in the admin center. When a tenant exceeds the storage quota, it is impossible to create a new environment, copy an environment, or restore it until additional capacity is purchased.

Sign into the Power Platform admin center to review current storage and choose **Resources > Capacity**. The *Summary* tab provides a tenant-level view of how the organization uses storage capacity. The *Dataverse* tab offers similar information but with an environment-level view of where the organization uses capacity. This tab provides statistical details about actual database usage, top database tables and their growth over time, actual file usage, top file tables and their growth over time, actual log usage, and top tables and their growth over time. The *Microsoft Teams* tab lists Dataverse for Teams capacity used within the tenant, and the *Add-ons* tab provides details on add-ons used within environments. The *Trials* tab displays the capacity used in all trial environments.

Understanding and managing Dataverse storage is crucial for maintaining the efficiency and performance of your Power Platform environments. For more information, please visit [Environment capacity management & alerting](#).

Capacity Limits

Tenants with Power Apps or Power Automate licenses automatically receive default capacity, which increases with each additional license. The default capacity provided includes the following:

- **Dataverse Database Capacity:** Storage space allocated for database tables and records.
- **Dataverse File Capacity:** Storage space allocated for file attachments and document storage within Dataverse.
- **Dataverse Log Capacity:** Storage space allocated for system and audit logs within Dataverse.

Microsoft's documentation provides detailed information about capacity entitlements and how additional capacity can be purchased. Monitoring and managing capacity is important to ensure that environments remain within limits and to plan for any necessary expansions.

For more details on capacity limits and purchasing additional capacity, refer to the [Power Platform licensing FAQs](#) and download the [full licensing guide](#).

Accessing On-premises Data with the Data Gateway

Building solutions with Power Platform apps often requires integrating data from on-premises repositories such as SQL Server databases, documents in SharePoint libraries, and other data stores. The Data Gateway is available to enable connectivity with these on-premises data sources. This gateway facilitates secure

connections between on-premises data and various cloud services, including Azure Analysis Services, Azure Logic Apps, Power BI, Power Apps, and Power Automate. It creates an HTTPS proxy connection that these cloud services can securely access. The Data Gateway, also used by Microsoft's Power BI service, supports multiple data sources like SQL Server, SharePoint, Oracle, MySQL, filesystem (files and file shares), SAP HANA, Teradata, PostgreSQL, and Web APIs. Refer to the [relevant documentation](#) for more details on software and hardware requirements.

The gateway uses outbound connections; meaning connections are always initiated from the internal network towards the cloud, not vice versa. Traffic is routed through Azure Service Bus, a hidden component of the gateway's overall architecture. A good practice is downloading the Data Gateway executable and deploying it on at least two servers that can access your required data sources. This setup ensures high availability, as load balancing between the two machines happens automatically. Note that you cannot install Data Gateway on an AD Domain Controller. The machines hosting the Data Gateway can have shared services, but they should be servers, not workstations.

To install Data Gateway, download the executable and run through its setup following this [installation guideline](#). When configuring the Data Gateway, ensure you store the recovery key in a safe place, as you will need it for recovery and when expanding your setup with multiple Data Gateway installations. Specify your region during configuration to align with where flows are executed, avoiding excess latency. If a proxy or firewall restricts outbound network connectivity, ensure the necessary ports and destinations are allowed for Data Gateway to operate correctly by following [Microsoft's instructions](#). Once your Data Gateway is installed, you can add data sources to the gateway, making your on-premises data accessible to Power BI, Power Apps, and Power Automate.

Using Data Loss Prevention Policies

It is not advisable for your Power Apps and Power Automate flows to retrieve data from sensitive internal locations (such as a SharePoint list containing salary information) and share it publicly using connectors like Google Drive. This is where Data Loss Prevention (DLP) comes into play. DLP allows you to control which services can share data within the tenant and with external sources.

DLP policies enable administrators to restrict data handling and capture for Power Automate. Organizations typically do not wish to capture or store sensitive or private data unless it is properly handled and secured. While users have the freedom to build their solutions, administrators have a reasonable need to set boundaries through DLP policies to ensure data security and compliance.

DLP policies also allow you to control connector actions and endpoint restrictions. By configuring these settings, you can ensure that only approved connectors are used within your environment and define specific endpoints that connectors can or cannot access. This helps mitigate risks associated with unauthorized data sharing and ensures that sensitive data remains secure.

Implementing DLP policies provides a robust framework to protect sensitive information by defining how data can be shared and what actions connectors can perform. Thus, you can enhance the security and compliance of your data management practices.

Creating a DLP Policy

To create a new Data Loss Prevention (DLP) policy, select **Policies > Data policies** in the Power Platform Admin Center and click **+ New Policy**. When creating a new policy, you must give the policy a name. After naming the policy, proceed to classify prebuilt and custom connectors.

Connectors are where you define the policy restrictions. In this view, you can define which connectors can share business data and which are blocked. You can also set which of these is the default – can access business data only or no business data allowed. This model then limits any flows that users create to share

data between either group. DLP policies enforce rules on which connectors can be used together by classifying the connectors as **Business** or **Non-business**. All services are placed into the "Non-business" classification group by default. You can freely add and remove connectors from either group simply by clicking on the [...] menu (Figure 21-5) and choosing **Move to Business** or **Move to Non-business**.

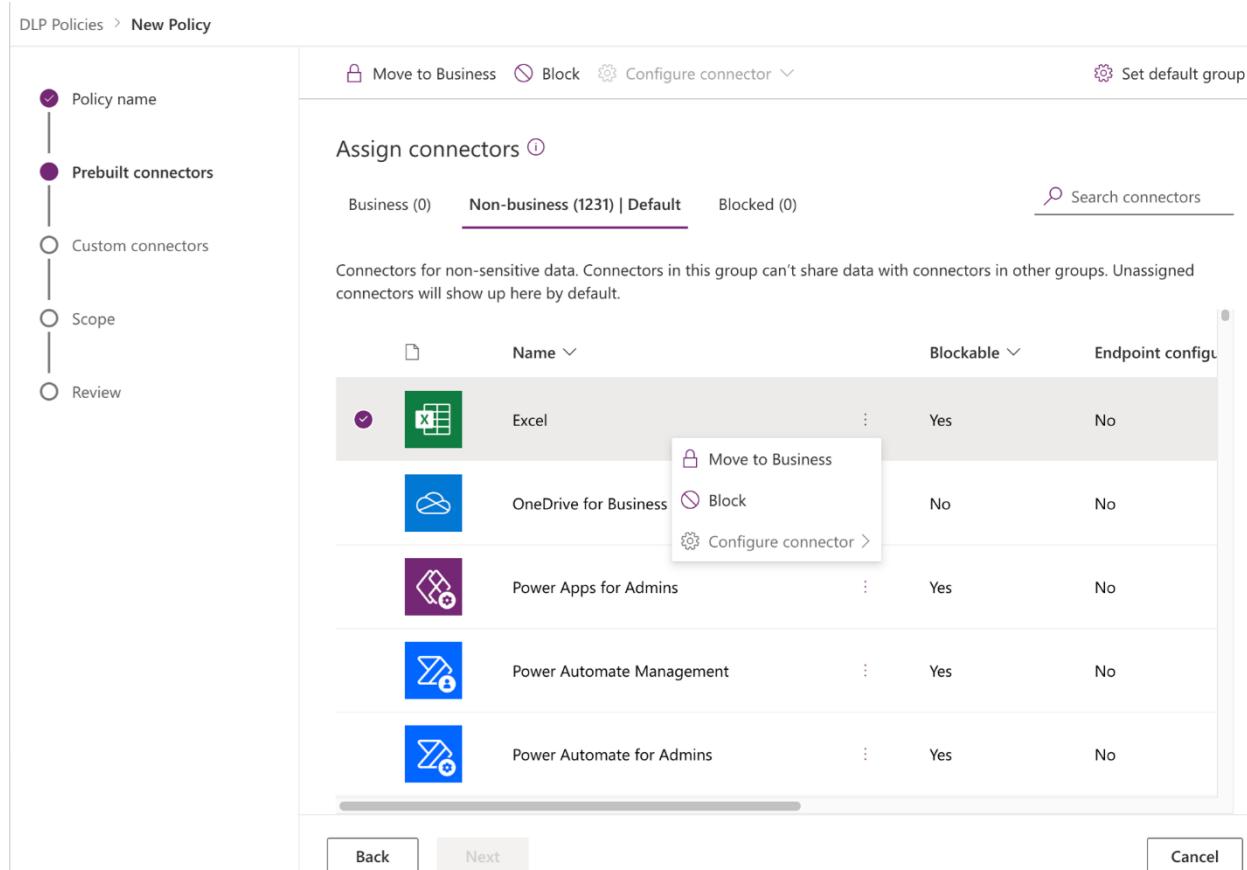


Figure 21-5: Assigning connectors in a DLP policy

This process ensures that sensitive business data is securely handled and not inadvertently shared with unauthorized or non-secure services. Data cannot be shared between services in different Data groups and can only be shared with other connectors within the same group. One Data group must be designated as the default group. Initially, the "No business data allowed" group is set as the default group. Administrators can change the default data group using the ellipse button at the top right of each group. New services added to Power Automate will be placed in the designated default group. It is recommended to keep the "No business data allowed" group as the default and manually add services to the Business data group after evaluating the impact of allowing business data to share information with the new service.

Scope defines the environment's scope for a Data Loss Prevention (DLP) policy. The "define scope" option specifies which environments the policy applies to. An environment is an isolation boundary for DLP and data locality. If you have not created any environments yet, you can create a DLP policy that applies to all environments, regardless of how many you have or plan to create in the future. Once you name and save the policy, it is automatically activated for the selected environment(s).

Several impacts occur when a user attempts to create a flow using a connector blocked by a Data Loss Prevention (DLP) policy. During the design phase, if a Power Apps maker tries to use connectors that don't belong together or have been blocked by data policies, they'll receive an error message, preventing the app from adding the connection. Similarly, Power Automate makers will encounter an error when saving a flow that violates DLP policies, resulting in the flow being marked as "Suspended" and not executing until the DLP violation is resolved.

If an admin modifies the data policies at runtime, existing apps and flows may be affected. Users who access a resource that violates the latest DLP policy will see an error message. For example, Power Apps users opening an app with incompatible connectors will encounter an error, and Power Automate users won't be able to start a flow that violates DLP policies.

Power Automate

Power Automate is a robust, cloud-based workflow service that enables users to create automated workflows and business processes across multiple applications and services. It features a visual drag-and-drop interface for designing and implementing workflows without the need for coding skills. Power Automate allows users to connect to various applications, services, and data sources within the Microsoft ecosystem, such as Office 365, SharePoint, OneDrive, Dynamics 365, and Azure, as well as third-party providers like Salesforce and ServiceNow. It offers a wide range of connectors, facilitating seamless integration with popular services and enhancing the automation capabilities of businesses.

Power Automate provides several benefits that help organizations streamline their processes and improve overall productivity:

- **Increased Efficiency:** Automating repetitive tasks saves time and reduces the potential for human error, allowing for more consistent and reliable outcomes.
- **Improved Productivity:** Power Automate allows users to focus on more strategic activities and higher-value tasks by handling routine processes.
- **Enhanced Collaboration:** Power Automate streamlines communication and coordination among team members and systems, facilitating better teamwork and information sharing.
- **Scalability:** The platform easily scales to accommodate growing business needs and integrates with various services and applications, ensuring it can support expanding workflows and increasing data volumes.

By leveraging Power Automate, organizations can create sophisticated workflows that connect disparate systems and automate complex business processes, driving greater efficiency and productivity. Here are some example scenarios on how Power Automate can be utilized:

- **Email Notifications, Approvals, and Document Collaboration:** Automatically send email notifications or trigger approval processes based on specific events or conditions. For example, a flow can send an email notification when a new item is added to a SharePoint list, automate the approval of expense reports based on predefined rules, trigger an approval request when a document is uploaded to a SharePoint library, and notify team members when a document is edited or reviewed. By integrating these capabilities, you can streamline approval and collaboration processes, enhancing efficiency and communication within your team.
- **Social Media Monitoring and Engagement:** Monitor social media platforms for specific keywords or mentions and trigger actions based on identified events. For instance, a flow can notify you when your brand is mentioned on Twitter or automatically save new social media posts related to a particular topic in a SharePoint document library.
- **Data Synchronization and Integration:** Synchronize data between different systems or services. For example, create a flow that automatically copies data from a SharePoint list to an Excel workbook or syncs data between a CRM system and an email marketing platform.
- **Task and Issue Tracking:** Track tasks and issues across various platforms and systems. For example, create a flow that generates a task in Microsoft Planner when an email with a specific keyword is received or automatically create a support ticket in a helpdesk system (such as ServiceNow) when a customer submits a form.

- **Data Collection and Forms Processing:** Collect data from different sources, process it, and take appropriate actions. For instance, a flow can gather responses from a Microsoft Form, store the data in a SharePoint list, and send a follow-up email to the respondent.
- **Data Backup and Archiving:** Automate the backup and archival processes for data stored on various platforms. Set up a flow that regularly copies files from one location to another, such as from OneDrive to SharePoint or from SharePoint to Azure Blob storage, ensuring data redundancy and preservation.

Building Automated Solutions with Power Automate

Power Automate facilitates the creation of automated workflows and business processes through three distinct types of flows: *Cloud flows*, *Desktop flows*, and *Business Process flows*. Each type is tailored to different automation needs and scenarios.

- **Cloud Flows** integrate and interact seamlessly with a broad spectrum of applications and services within Microsoft's ecosystem and third-party providers. These flows are particularly effective for automating tasks within a cloud environment, operating autonomously once configured. As a foundational component of the Power Automate platform, they streamline processes and enhance efficiency by reducing the need for manual intervention.
- **Desktop Flows** focus on automating tasks directly on your desktop. They interact with desktop applications to perform data entry and file manipulation functions, making them ideal for automating repetitive tasks on a personal computer.
- **Business Process Flows** guide users through structured business processes, ensuring consistent adherence to organizational policies and procedures. They enforce a predefined sequence of actions or decisions, which is vital for maintaining compliance and procedural accuracy.

Cloud Flows are the most frequently used, automating workflows between apps and services without requiring user intervention once set up. They enhance productivity and operational efficiency by automating routine tasks freeing up resources for strategic activities that require human expertise. Additionally, Cloud Flows ensure consistent and error-free execution of business processes, improving overall performance.

Components of Power Automate Flows

Power Automate flows consist of two main components: a *trigger* and *actions*. The [trigger](#) is an event or condition that initiates the execution of a workflow, determining when it should start. Actions are the tasks performed once the trigger is activated, including multiple steps depending on the flow's configuration. All flows require one trigger and can have one or more actions. The three flow types you can create with a cloud flow are:

- **Automated Flows:** Triggered automatically when a specific condition is met. For instance, an automated flow can start when a new item is added to a SharePoint Online list or when a lead is updated in Dynamics 365 or Salesforce.
- **Instant Flows:** Manually triggered by a user by clicking a button. For example, a flow can be initiated when a user clicks a button in a Power App.
- **Scheduled Flows:** Run on a set schedule. These flows can be configured to execute at specific times, intervals, or recurrence patterns.

Creating Cloud Flows

You'll need to follow several important steps to create a cloud flow in Power Automate. First, you'll need to access the platform and decide how you want to build your flow. The Power Automate cloud flow designer is a web-based tool that allows you to create and edit cloud flows. You can access the designer from the [Power Automate maker portal](#), the Microsoft 365 app launcher, or the Power Apps portal. To access the designer, sign in with your work or school account and make sure you have a valid license for Power Automate. You can

build, set up, and customize your cloud flows using either the classic designer or the AI-powered cloud flows designer. With the Power Automate cloud flows designer, you can create cloud flows from scratch or templates, add and configure triggers, actions, and conditions, use expressions and variables to manipulate data, test and debug your cloud flows, and share and manage your cloud flows.

Building Flows from Templates

Using templates is an efficient way to create Power Automate flows quickly, leveraging pre-built configurations that can be customized to meet your specific needs. Templates provide a great starting point for those new to Power Automate and experienced users looking to streamline the creation process. Templates are predefined flows that can be used in many different scenarios. You can quickly create new flow instances through a Power Automate template that only require access to the services defined in the template and additional configuration settings. Microsoft offers several templates to help create a flow in minutes. You can use the templates as a starting point to implement more refined flows and to see how some flow options work.

To access templates, navigate to the [Power Automate dashboard](#) and click on the **Templates** tab in the left-hand menu. This will take you to a library of pre-built templates categorized by use cases, such as email automation, data synchronization, approval workflows, and social media monitoring. You can use the search bar to find templates relevant to your needs by keywords, applications, or specific actions you want to automate. Once you find a suitable template, click on it to view detailed information about its functionality, the apps it connects to, and the steps involved.

Building Flows using Copilot

One of the features that make Power Automate unique is the **Describe it to design it** feature. This feature (available in [select regions](#)) allows you to describe your workflow scenario in natural language, and Power Automate will suggest the best actions and triggers for you. You can refine your description with keywords, parameters, and conditions for more accurate results. This innovative approach simplifies the flow creation process, making it accessible even to those without technical expertise. Using this feature is not dependent on having a Copilot license.

To learn more about creating a flow using the cloud flows designer with Copilot, visit [Create a flow using the cloud flows designer with Copilot](#). For tips on writing a good prompt, see [How to write a good prompt](#).

Advanced Features in Power Automate

Advancement beyond basic flows allows organizations to tackle more complex scenarios and enhance efficiency at scale in workflow automation with Power Automate. This section delves into Power Automate's advanced features, focusing on using loops and arrays for data processing, integrating with a diverse array of services both within and outside the Microsoft ecosystem, and implementing robust error-handling strategies. These capabilities enable users to construct dynamic, resilient workflows that can adapt to various business needs and handle sophisticated data operations effortlessly.

Using Loops and Arrays

Loops and arrays are powerful tools within Power Automate that help manage and process multiple items in a sequence or collection.

- **For Each Loop:** This loop iterates over each item in an array or collection. For example, if you have a list of customer emails, a *For Each* loop can process each email address individually, performing actions like sending emails or updating records for each entry. This loop is handy in scenarios where you need to apply the same set of actions to a large dataset, ensuring consistency and efficiency in processing.

- **Do Until Loop:** This loop is used to perform an action repeatedly until a specific condition is met. For instance, you might continue to check a folder until a specific file appears or loop through a list, incrementing a counter until it reaches a predefined limit. The *Do Until* loop is essential for workflows that depend on fulfilling certain criteria before proceeding to the next step, allowing for more dynamic and responsive flows.

These looping constructs are especially useful when dealing with data that needs bulk processing or when actions must be repeated multiple times based on dynamic data sets. By leveraging loops and arrays, you can create workflows that efficiently handle large volumes of data and perform repetitive tasks automatically.

Using Variables

Variables are essential components in Power Automate that allow you to store and manipulate data throughout the execution of a flow. They enable dynamic data handling and can be used to hold temporary values that you can reference or modify at various points within your workflow. Here's how you can create and use variables in Power Automate:

1. **Initialize Variable:** The first step in using a variable is to initialize it. You can do this by adding the *Initialize variable* action to your flow. You specify the variable name, type (such as string, integer, boolean, array, or object), and initial value.
2. **Set Variable:** Once a variable is initialized, you can change its value using the *Set variable* action. This is useful for updating the variable based on conditions or actions taken within the flow.
3. **Increment Variable:** For numeric variables, you can use the *Increment variable* action to increase its value by a specified amount. This is particularly useful in loops or when tracking counts.
4. **Append to Array Variable:** If you are working with array variables, the *Append to array variable* action allows you to dynamically add new items to the array.

By effectively using variables, you can make your flows more dynamic and flexible, enabling them to handle a wide range of scenarios.

Using Conditions

Conditions in Power Automate allow you to introduce decision-making capabilities into your flows. They enable executing different actions based on specific criteria, making your workflows more intelligent and adaptable. Here's how you can use conditions effectively:

1. **Condition Action:** The primary way to implement conditional logic is by using the *Condition* action. This action lets you define a condition with two branches: *If yes* and *If no*. The corresponding branch will execute depending on whether the condition evaluates to true or false. For example, if you want to check if the value of a variable is greater than a certain number, you can set up a condition to perform different actions based on the result.
2. **Nested Conditions:** By nesting conditions within each other, you can create more complex logic. This allows for multiple levels of decision-making within a single flow.
3. **Expressions in Conditions:** Power Automate supports using expressions within conditions to perform more advanced evaluations. You can use functions and operators to compare values, manipulate strings, and perform calculations.

By effectively using conditions, you can create dynamic and responsive workflows that handle a variety of scenarios based on the data and conditions you specify.

Using Switch Control

The Switch control in Power Automate handles multiple possible values of a variable with different actions for each value. It is beneficial when you need to execute distinct sets of actions based on the value of a single variable.

1. **Switch Action:** Add the *Switch* action to your flow and specify the variable you want to evaluate. The *Switch* control allows you to define different cases for the variable's possible values.
2. **Cases:** Each case within a *Switch* represents a possible value of the variable. For each case, you can define a set of actions that should be executed if the variable matches the case value. Example: If you have a variable representing the status of an order (e.g., "Pending," "Shipped," "Delivered"), you can use a *Switch* to perform different actions based on the status.
3. **Default Case:** The *Switch* control also allows you to define a default case that executes if none of the specified cases match the variable's value. This ensures that your flow can gracefully handle unexpected or undefined values.

By using the *Switch* control, you can simplify complex conditional logic and make your flows more readable and maintainable.

Integrating with Multiple Services

One of Power Automate's standout features is its ability to integrate with a wide array of services within and outside the Microsoft ecosystem. By connecting to services such as Office 365, SharePoint, OneDrive, Dynamics 365, Azure, Salesforce, and ServiceNow, Power Automate allows you to create workflows that bridge gaps between different systems. This seamless integration facilitates the synchronization of data across platforms, the automation of cross-platform processes, and the unification of various business operations into a single streamlined workflow. For example, you can create a flow that automatically updates a CRM system when new customer data is added to a SharePoint list or one that triggers alerts in Microsoft Teams based on activity in Salesforce. These integrations enable real-time data updates, improve communication, and ensure your business processes are cohesive and interconnected.

Run History and Error Handling in Power Automate

Power Automate is a powerful tool for automating tasks and processes, but like any complex system, it's crucial to manage and troubleshoot potential issues that arise during execution. This section delves into the essentials of Run History and Error Handling, providing you with the knowledge to monitor your workflows effectively and implement strategies to handle errors gracefully. Understanding how to access and interpret run history and utilizing robust error-handling techniques can ensure your automated workflows remain resilient and reliable, even in the face of unexpected challenges.

Run History

Power Automate's Run History is a comprehensive log that records detailed information about each execution of your flows. It is critical in monitoring, troubleshooting, and optimizing your automated workflows. Here are some essential aspects of the Run History:

- **Run Status:** Indicates the success or failure of a flow run or if it is still in progress.
- **Start and End Time:** Captures when the flow began and ended, providing a execution timeline.
- **Duration:** Measures the total time taken for the flow to complete.
- **Trigger Details:** Describe the event that triggered the flow, such as a file creation or an HTTP request.
- **Inputs and Outputs:** This section lists the data received by the flow and the results produced, which is essential for diagnosing issues and understanding data handling.
- **Run History Details:** Additional notes or observations about the flow's execution.
- **Error Information:** Critical for error handling, this section logs any errors that occur, detailing what went wrong and where. This information is invaluable for correcting and preventing future errors.
- **Retry Attempts:** If enabled, show details of any automatic retries following failures, aiding in understanding and refining recovery strategies.
- **Environment and Flow Version:** Documents the environment and the specific version of the flow that was executed. This is useful for tracking changes and performance across different setups.

To view the Run History of a specific flow, you can navigate to the Power Automate portal, select the flow, and then find the **28-day run history** section. From there, you can inspect each run, view details, and diagnose any issues that may have occurred during the execution of the flow. This information is crucial for monitoring, troubleshooting, and optimizing your Power Automate workflows.

Note: The General Data Protection Regulation (GDPR) mandates the retention of run logs for a maximum of 28 days. If you wish to preserve a more extended history, it is necessary to capture run histories before they are subject to deletion manually.

Clicking on a specific run's date link provides a detailed view of each connector's input and output and information about any exceptions or errors encountered. This detailed diagnostic view helps pinpoint why a flow failed or why certain runs were unsuccessful compared to others. Testing and debugging are further facilitated by the 'Test' button, which allows real-time observation of a flow's execution, making it easier to identify and fix issues (Figure 21-6):

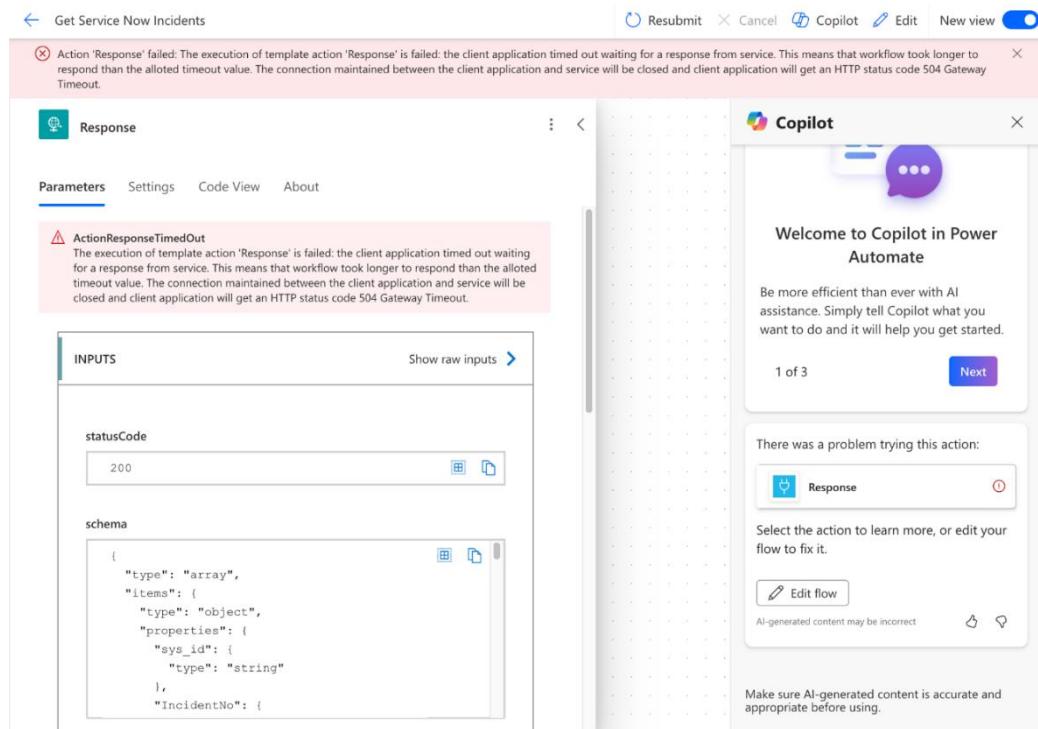


Figure 21-6: Raw output from a flow with execution errors

Error Handling

Error handling is a crucial part of creating reliable workflows in Power Automate. It ensures that your automation processes can effectively deal with unexpected issues and continue to run smoothly. This section will cover various techniques and best practices for managing errors in Power Automate. Error handling in Power Automate involves capturing, managing, and responding to errors during the flow's execution. Effective error handling ensures that your workflows are resilient and can handle expected and unexpected issues without causing major disruptions. Errors can occur in Power Automate due to several reasons, including connectivity issues (such as problems connecting to external services or APIs), data validation errors (involving issues with processed data, like missing or invalid data), service unavailability (where external services or systems are temporarily unavailable), and timeouts (when operations take longer than expected to complete).

Proper error handling is crucial for building reliable and robust flows in Power Automate. Some techniques for error handling include:

- **Configure Run After:** Power Automate lets you configure actions to run after previous actions have succeeded, failed, been skipped, or timed out. This feature is vital for managing workflow errors effectively by specifying alternate flows or cleanup processes if an error occurs.
- **Scope Actions:** Scope actions allow you to group multiple actions and manage their execution as a single unit. You can use scopes to handle errors by grouping actions and using the *Configure Run After* settings on the scope.
- **Try, Catch, and Finally:** Like traditional programming, Power Automate allows you to structure error handling with Try, Catch, and Finally blocks. This means you can define actions to attempt (Try), actions to take if an error occurs (Catch), and actions to perform in any case after trying (Finally).
- **Terminate Action:** The Terminate action can be used to end a flow with a specific status (Success, Failure, or Cancelled). This is useful for explicitly controlling the flow's outcome based on error conditions.
- **Exception Handling with Parallel Branching:** Parallel branches can be used to handle different types of errors simultaneously. Each branch can have its own error-handling logic, allowing for more granular control over various error scenarios.

Implementing best practices for error handling in Power Automate is essential for creating resilient and reliable workflows. By adopting proven strategies, you can ensure that your automation processes effectively manage errors, minimize disruptions, and provide clear insights into any issues that arise. Some best practices for error handling include:

- **Logging and Monitoring:** Implement logging actions to capture error details and monitor your flows' performance. Use connectors like Azure Application Insights or custom logging services.
- **Retry Policies:** Configure retry policies for actions that may temporarily fail due to transient issues, such as network connectivity problems.
- **User Notifications:** Send notifications to users or administrators when critical errors occur. Use email, Microsoft Teams, or other communication channels to alert stakeholders.
- **Graceful Degradation:** Design your flows to degrade gracefully in case of errors, ensuring that essential functions continue to operate while non-essential functions are temporarily disabled.
- **Documentation and Comments:** Document your error-handling logic and add comments to your flows to explain the rationale behind your error-handling decisions. This helps maintain clarity and makes it easier for others to understand and maintain your flows.

Additionally, the Flow Checker tool, accessible during flow editing, analyzes the flow and offers recommendations for improving reliability and performance.

For hands on exercises to learn best practices for error handling in Power Automate flows, please visit [Best practices for error handling in Power Automate flows](#).

Service Principal Owned Flows

Power Automate allows non-human security identities referred to as service principals to own and manage resources within Azure and the Power Platform. Service principal application users can create and manage flows, offering organizational flexibility and stability. To utilize a service principal in the Power Platform, an application user must be created to represent it. This application user can have connections shared with them and can own resources such as flows.

It is advisable to use a service principal application user for specific scenarios, such as mission-critical flows that serve departmental or enterprise-wide needs. This approach insulates flow ownership from the lifecycle of a human owner, thus preventing issues if the owner leaves the organization, changes roles, or loses their premium license. Additionally, this method is beneficial when using DevOps pipelines to deploy flows across Development, Test, and Production environments.

Since a service principal application user is a non-interactive user without a user license, it is subject to non-licensed user limits. It has specific licensing and request limit implications. The flow connections must be shared with the service principal application user to successfully run flows.

For steps to create and assign a service principal to a flow, please visit [Prerequisites](#).

Power Automate Desktop and RPA Tools

In 2020, Microsoft acquired Softomotive, a leading provider of Robotic Process Automation (RPA) with over 15 years of experience and the creator of WinAutomation. This acquisition enhanced Microsoft's Power Automate capabilities under the name UI Flows, now known as Desktop Flows, allowing bots to perform UI-based tasks based on pre-recorded interactions.

Power Automate Desktop (PAD) supports two types of RPA:

- **Attended RPA:** Requires human initiation and interaction. It is ideal for tasks where user input is necessary during the process.
- **Unattended RPA:** Runs without human interaction, perfect for automating backend processes that don't need user intervention.

Both types of flows can be created using PAD, a desktop client app that provides RPA capabilities to the Power Platform. PAD automates repetitive tasks by replicating user actions such as mouse movements, clicks, and keyboard entries. It is often used to build business applications quickly and integrate with legacy systems. Historically, people used VBA-based Macros in Excel, PowerPoint, and Word to automate tasks, but these Macros posed security risks as potential vehicles for malware. In contrast, PAD flows are more secure since the code is not embedded in Office documents, providing a versatile automation solution for various processes beyond just Office applications.

PAD is included in Windows 11. If you're running Windows 10, the PAD installer can be [downloaded directly from Microsoft](#). Although the PAD app is free, the RPA system used to create and save flows to the cloud requires a paid subscription to the Power Platform ([a free trial with limited functionality is available](#)). Power Automate with RPA add-on licensing is only required if you want to publish desktop flows to the cloud. To learn more, [visit this learning path](#) to get hands-on exercises with building Power Automate desktop flows.

Process Mining and Task Mining

Process mining is both a research area and a technological tool that empowers businesses to comprehend their actual processes, including their operations, and recognize opportunities for enhancement, automation, and digitization. Within Power Automate, the process mining capability integrates seamlessly with the existing Microsoft platform and ecosystem, offering comprehensive end-to-end solutions that facilitate quicker business decisions. Extracting event data from your system of records provides clear visualizations of the processes occurring within your organization. This feature allows you to customize process mining reports, compare different processes, pinpoint the root causes of inefficiencies, and monitor key performance indicators (KPIs). To learn more about process mining, visit [Overview of process mining](#).

Task mining aims to assist organizations in gaining valuable insights into users' interactions with software applications. By capturing and analyzing user actions, this data-driven approach enables identifying repetitive tasks, discovering inefficiencies, and effective process automation. Task mining includes:

- **Data Collection:** Power Automate Task Mining uses agents to collect user interaction data across applications and systems. These lightweight agents can be deployed on users' machines to track actions such as mouse clicks, keyboard inputs, and application navigation.

- **Data Analysis:** The collected interaction data is processed and analyzed to generate insights and visualizations. Organizations can view and understand user behaviors, commonly performed tasks, time taken for specific actions, and recurring patterns.
- **Process Automation:** By identifying repetitive tasks and bottlenecks, Power Automate Task Mining helps organizations target areas for process automation. Organizations can build automated workflows using Power Automate to streamline processes and increase efficiency.
- **User Experience Improvement:** By better understanding user interactions, organizations can enhance the user experience by identifying pain points and making data-driven decisions about software improvements.

To learn more about task mining, visit [Overview of task mining](#).

AI Builder

[AI Builder](#) for Power Automate is a segment of the Microsoft Power Platform that enables users to integrate artificial intelligence (AI) capabilities seamlessly into their automated workflows. Even without extensive AI expertise, it allows individuals to leverage AI models for predicting outcomes, extracting insights, and automating tasks.

Creating and Using AI Models

Utilizing AI Builder, individuals can craft personalized AI models through an intuitive point-and-click interface, ensuring accessibility for a wide range of users. The interface guides users through selecting data, training models, and evaluating performance, making AI model creation straightforward and user-friendly. This accessibility means that business users, analysts, and developers can build AI solutions without deep data science knowledge.

Integration with Power Automate

The integration with Power Automate enables the seamless incorporation of these AI models into automated processes and workflows. Once an AI model is created and trained in AI Builder, it can be easily integrated into a flow in Power Automate. This allows users to automate decision-making processes and enhance workflows with AI-driven insights. For example, you can create a flow that uses an AI model to predict sales trends based on historical data and automatically adjust inventory levels. Similarly, you can automate the processing of invoices by using an AI model to extract critical information from scanned documents and input the data into your accounting system.

Users can utilize AI Builder to add intelligence to various business scenarios:

- **Predictive Analytics:** AI models can predict future outcomes based on historical data. This is useful for sales forecasting, customer churn prediction, demand planning, and more. Businesses can proactively address potential issues and opportunities by integrating these predictions into automated workflows.
- **Document Processing:** AI Builder can automate extracting information from documents such as invoices, receipts, and forms. By recognizing and extracting data points, businesses can streamline data entry processes, reduce manual effort, and improve accuracy.
- **Image and Text Recognition:** AI models can analyze images to identify objects, text, or handwriting. This can be used in scenarios like automating compliance checks, processing handwritten notes, or categorizing images in a digital asset library.
- **Sentiment Analysis:** By analyzing customer feedback, reviews, or social media posts, AI models can determine the sentiment behind the text. This can help businesses understand customer satisfaction and respond appropriately to enhance customer experience.

Benefits of AI Builder

AI Builder provides a user-friendly way to harness the power of AI, making it easier for organizations to leverage intelligent automation in their applications and workflows. The benefits include:

- **Enhanced Decision Making:** AI-driven insights allow more informed and timely decision-making, improving business outcomes.
- **Efficiency and Productivity:** Automating complex tasks with AI reduces manual effort, speeds up processes, and increases productivity.
- **Scalability:** AI models can handle large volumes of data and scale with your business needs, ensuring consistent performance.
- **Accessibility:** The intuitive interface ensures that AI capabilities are accessible to users without requiring deep technical skills, democratizing the use of AI across the organization.

Integrating AI Builder with Power Automate allows businesses to create more intelligent, responsive, and efficient workflows, driving innovation and competitive advantage.

AI Builder Learning and Resources

To get started with AI Builder, you can utilize the following learning resources: AI Builder [learning paths and modules](#), which provide structured educational content; AI Builder [community forums](#), where you can engage with other users and experts to share insights and solve problems; AI Builder [hands-on labs](#), offering practical experience with building and deploying AI models; working with [sample data](#) to understand how to apply AI Builder to real-world scenarios; and reviewing the AI Builder [licensing summary](#) to understand the costs and licensing requirements associated with using AI Builder in your workflows.

Sharing Flows

Sharing Power Automate flows is a vital feature that promotes collaboration and ensures that critical automated processes are accessible and maintainable by multiple team members. Sharing flows enhances collaboration by allowing team members to work together on creating and maintaining automation processes. This collaborative approach can lead to more robust and well-designed workflows. Additionally, having multiple owners increases redundancy, ensuring critical workflows are not dependent on a single person. Other co-owners can manage and troubleshoot the flows if the primary owner is unavailable. Furthermore, sharing flows promotes knowledge sharing, helping disseminate information about how specific automation processes are set up and operated. This can be educational for team members and assist in standardizing best practices across the organization.

To share a cloud flow or desktop flow with colleagues or groups within the same tenant, follow these steps:

1. **Navigate to Your Flow:** Go to the Power Automate portal and find the flow you want to share. It could be a cloud or desktop flow.
2. **Open the Sharing Settings:** Click on the flow to open its details page. Look for the Share icon, typically found at the top of the page, and click on it to open the sharing settings.
3. **Add Users or Groups:** In the sharing settings, you can add individual users or groups by entering their email addresses or selecting them from your organization's directory.
4. **Assign Permissions:** Decide the level of access you want to grant.
5. **Confirm and Share:** Once you've added the users or groups, confirm the sharing settings. The selected users will be notified and will gain access to the flow.

Considerations When Sharing Flows

Sharing Power Automate flows can significantly enhance collaboration and efficiency within your team. However, it is essential to consider several factors to ensure that the shared flows remain secure, reliable, and

effective. Below are key considerations to keep in mind when sharing flows with colleagues or groups within your organization.

- **Co-Ownership and Permissions:** When you share a flow, the recipients become co-owners. They will be able to make changes to the flow's logic, connections, and other settings. This means they can edit the flow just as you can, so ensure you share it with trusted team members.
- **Connections and Authentication:** Any connections (such as to Office 365, SharePoint, or other services) used in the flow will be shared with the co-owners. If your flow uses personal credentials, like an Exchange Online mailbox, to send emails, these connections become accessible to the co-owners. Ensure that the connections do not expose sensitive or personal data unless necessary.
- **Maintaining Flow Integrity:** Sharing flows can help in maintaining and updating them, but it also means that changes by co-owners can affect how the flow operates. Establishing guidelines on how and when to make changes can help maintain the integrity of critical flows.
- **Collaboration and Accountability:** Shared ownership fosters collaboration, allowing multiple team members to contribute to the flow's development and maintenance. However, it's essential to keep track of changes and updates made by different users to ensure accountability and traceability.

Guest Access to Power Automate

You can assign actions in a flow to guest accounts. To use this feature, you must create the guest account and assign it a plan with a Power Automate license before assigning it to a flow. The flow is created as normal and then assigned to the guest account, which receives an email notification to act in the flow. The link in the email routes them to the host tenant. To get back to their home tenant, the guest has two options: They can either visit the My Flows page and click on the Go to your org's default environment link in the notification message, or they can log out and then log back into their tenant.

Except for SharePoint flows and Approval flows, connections to Entra ID-backed services are established within the user's home tenant, regardless of the tenant they are currently logged into. Currently, there are some limitations for guest access in flows:

- **Mobile Notifications:** Guest users cannot receive notifications on their mobile devices because the Power Automate app for iOS or Android cannot sign them in as guests.
- **People Picker:** People picker experiences do not work for guest users because they cannot query and enumerate tenant members, but typing the full email address in the selection box works.
- **Tenant Switching:** There is no way in the user interface to switch between tenants. The only way to access the flow portal as a guest is through an email link.

By understanding these limitations and how to navigate guest access, you can effectively incorporate guest users into your Power Automate workflows, enabling broader collaboration while managing the unique challenges this functionality presents.

Best Practices for Building Power Automate Solutions

Creating solutions with Power Automate becomes more intricate as flows interact with other flows or multiple decisions are made during execution. Planning a new flow carefully is crucial to ensure efficiency, reliability, and scalability. Here are key considerations and best practices for building robust Power Automate solutions:

- **Trigger Conditions:** Determine what will initiate the flow. Understanding the trigger conditions helps ensure the flow starts accurately based on specific events or criteria.
- **Expected Volume:** Assess the number of runs anticipated monthly. Knowing the expected volume of flow executions can help optimize performance and manage resources effectively.
- **Dependencies:** Identify if the flow will interact with other services or third-party APIs. Understanding dependencies is essential for establishing and maintaining all necessary connections.

- **Failure Handling:** Plan the steps to take if the flow fails. Implementing robust error-handling mechanisms ensures the flow can recover gracefully or provide helpful feedback when issues arise.
- **Activity Logging:** Decide how flow activities will be documented. Logging is crucial for monitoring the flow's performance, troubleshooting issues, and maintaining a record of its actions.

While flow definitions can be modified later, starting with a clear plan helps in building robust automations. Additionally, flows can be exported as .zip files, providing a backup before significant changes are made. This ensures that a reliable version is preserved, allowing you to revert to a previous state if needed.

By considering these best practices, you can create Power Automate solutions that are well-structured, maintainable, and capable of handling complex automation scenarios effectively. Proper planning and documentation not only streamline the development process but also enhance the overall reliability and performance of your automated workflows.

Licensing Power Automate

The licensing scheme for the Power Platform is complicated. If you need to manage several types of licenses in a tenant, you might need to consult Microsoft to understand the available options. To help, Microsoft keeps the [Licensing overview for Microsoft Power Platform](#) document updated with detailed information about pricing and licensing different components. The [Power Apps for Microsoft 365 plan](#) is included in most enterprise plans. This license allows users to run a limited number of flows per month with fewer capabilities than found in other plans. For example, it excludes access to premium connectors (all Azure and SQL connectors, HTML connectors, custom connectors, etc.). Additional premium plans for Power Automate include **Power Automate Premium per-user**, **Power Automate Process**, **Hosted RPA**, **Pay-as-you-go**, **AI Builder**, and **Process Mining**. For more information on Power Automate pricing plans, visit [Power Automate pricing](#).

Premium plans do not limit trigger frequency or flow runs but instead use a daily capacity limit (5,000 daily API requests). Organizations that need additional capacity for heavy usage scenarios can buy add-on capacity and assign it to specific users or processes.

If a user with a Power Automate per-user license runs a cloud flow in a pay-as-you-go plan, the flow won't be charged as it's part of the per-user license entitlement. However, if the same user runs an attended RPA flow, the flow run will be charged to your Azure subscription because RPA is not a part of the per-user license entitlement.

Tenant users can make self-service purchases for Power Platform licenses unless you block the capability. The steps needed to prevent this are in the tenant management chapter.

Power Apps

Power Apps is a versatile service designed to allow users to build custom business applications without the need for extensive app development knowledge or coding skills. It enables users to create web and mobile applications through a low-code or no-code approach to application development, making it accessible to business users, citizen developers, and those without a traditional programming background. The platform provides a visual interface and a wide range of pre-built templates, controls, and connectors to simplify the app creation process.

Power Apps integrates seamlessly with several Microsoft data sources, including SharePoint lists and libraries, OneDrive, Excel, Dynamics 365, and external databases. Additionally, it supports integration with non-Microsoft sources such as Dropbox, Box, Twitter, and Facebook. This flexibility allows users to create powerful and flexible applications that can access and manipulate data from multiple sources.

Key Features and Components

Power Apps offers a range of powerful features and components that enable users to build and customize business applications with ease. These features support the creation of user interfaces, integration with various data sources, the application of logic and calculations, and seamless deployment across different platforms. Here are some of the key features and components of Power Apps:

- **App Designer:** Power Apps provides a drag-and-drop app designer called Power Apps Studio, which allows users to create their applications' user interface (UI). The UI can be customized using a variety of controls, layouts, and formatting options.
- **Data Integration:** Power Apps supports integrating various data sources, including Microsoft 365 services (such as SharePoint, Excel, and OneDrive), databases (like SQL Server and Dataverse), and third-party systems through connectors. This allows users to access and manipulate data within their applications.
- **Formulas and Expressions:** Power Apps utilizes a formula language called Power Apps formulas. With formulas and expressions, users can add logic and calculations to their apps, perform data transformations, and define behavior based on user interactions.
- **Types of Power Apps:** Power Apps support two types of application: Canvas and Model-driven.
 - **Canvas apps** provide a blank canvas where users can design highly customizable applications using a visual interface. Canvas apps provide a highly customizable and flexible user interface where designers can control the app's layout and design. Users can drag and drop elements onto a blank canvas, creating bespoke applications that precisely fit their business needs. This approach is ideal for apps that require a tailored look and feel, with the freedom to design every aspect of the user experience.
 - **Model-driven apps** differ from canvas apps. In contrast, model-driven apps follow a more standardized and data-centric approach. These apps are built on top of the data structure defined in Dataverse. The interface and layout of model-driven apps are primarily determined by the data and relationships within Dataverse, which means that they are less customizable in layout but offer a robust framework for building complex, data-driven applications. Model-driven apps are ideal for scenarios where data management, workflows, and processes are at the core of the application's functionality.

Both types of apps can utilize Dataverse as their data source. Canvas apps offer the option to use Dataverse, while Model-driven apps inherently rely on it. It's possible to merge the experiences of Canvas and Model-driven apps, creating hybrid apps where the generated user interface from a Model-driven app can be modified and extended using the capabilities of Canvas apps.

- **App Sharing and Deployment:** Power Apps allows users to publish and share their applications with others within their organization or externally. Apps can be deployed across multiple platforms, such as mobile devices (iOS, Android) and web browsers, making them accessible to many users.
- **Integration with Power Platform:** Power Apps integrates closely with other components of the Power Platform, including Power Automate for workflow automation and Power BI for data visualization and reporting. This integration allows for seamless data flow and automation between these services.

Historically, developing apps has involved creating different versions for each operating system that need to run on (iOS, Android, Windows). This approach triples the development work, support costs, and resources needed to create business apps. Power Apps simplifies this by running all apps through a single platform, which manages the differences between operating systems. There is also a web version of Power Apps, which operates through any modern web browser instead of a mobile app. Additionally, Power Apps can be embedded in other applications, such as SharePoint and Teams.

Example Scenarios for Power Apps

Power Apps can be used in a wide range of scenarios to create custom applications that address various business needs:

- **Data Entry and Forms Automation:** Create custom data entry forms to streamline and digitize manual data collection processes, such as employee onboarding, customer surveys, inspection checklists, or expense reporting.
- **Field Service and Mobile Workforce:** Develop apps that enable field technicians to access job details, update work orders, capture photos, and submit reports from their mobile devices, improving efficiency and providing real-time visibility into field operations.
- **Inventory Management and Asset Tracking:** Manage inventory and track assets by creating apps that allow users to scan barcodes or QR codes, update inventory levels, track item movements, and generate reports. These apps are useful for warehouse management, equipment tracking, or supply chain optimization.
- **Employee Self-Service:** Build self-service portals or apps that empower employees to perform various tasks without manual processes or contacting HR or IT departments, such as requesting time off, updating personal information, accessing employee directories, or submitting IT support requests.
- **Document Management and Collaboration:** Facilitate document management and collaboration by creating apps that connect with SharePoint or OneDrive. These apps allow users to access, share, and collaborate on documents, automate approval workflows, or build document tracking systems.
- **Custom Business Process Automation:** Automate complex business processes with Power Apps and Power Automate. For example, create an app that guides users through steps, automates approval workflows, integrates with external systems, or triggers notifications and alerts.
- **Customer Engagement and Relationship Management:** Build customer-facing applications to enhance customer engagement and manage relationships, such as lead tracking, customer surveys, appointment scheduling, or customer support ticketing.

These are just a few examples of the many scenarios where Power Apps can be applied. The platform's flexibility and versatility allow organizations to tailor applications to their specific needs, automate processes, and improve productivity across various departments and industries.

Enabling Power Apps for Users

Microsoft enables Power Apps by default for all users in the tenant with E3 or E5 licenses. You need to pay attention to how or when Power Apps is used and the business case(s) for which to use it. Some organizations disable Power Apps upfront for all users if they do not see an immediate need for the service. Power Apps are powerful tools that can improve the adoption and usability of Office, but users need to have the necessary training to understand how to use them.

Users need a license to access Power Apps. If you're a global tenant administrator and need to learn how to enable Power Apps for your users, please visit [Manage Power Apps licenses in your organization](#).

Premium Features

Power Apps offers premium features not available with standard Office 365 licenses. These features include access to premium connectors, the ability to use Dataverse, and more advanced data integration and automation capabilities. If your organization requires the use of these premium features, you must assign premium licenses such as the Power Apps Premium plan or the Power Apps per app plan. These licenses can be managed through the Microsoft 365 admin center.

Managing premium licenses is crucial for cost management, as these licenses come with additional costs. Assigning premium licenses only to users who need access to advanced features is essential, ensuring that the

organization's budget is optimized. Regularly reviewing license assignments helps to align with the organization's needs and prevents unnecessary expenditures. For more information on licensing, please see the licensing section further in this chapter. For detailed instructions on assigning premium licenses, please refer to [Assign licenses](#).

For those who want to prototype and learn using premium features without immediately requiring a license, the [Power Apps Developer Plan](#) is available for free. This plan allows users to explore and develop applications with premium capabilities. However, when these solutions are ready to be deployed for production, appropriate licenses will be required.

Power Apps Studio Interface

Power Apps Studio is a robust web designer with a drag-and-drop interface for creating and managing your applications. Much like Power Automate, Power Apps Studio offers a dynamic and intuitive environment for app development. Here, you can design your applications' user interface (UI) with various customizable controls, layouts, and formatting options. The following sections detail the key components of Power Apps Studio (Figure 21-7), each contributing to a streamlined and efficient app-building experience:

1. **Power Apps Studio Modern Command Bar:** The dynamic command bar adjusts based on the selected control, offering a relevant set of commands. This feature streamlines development by displaying only the options pertinent to the current task. For example, selecting an app object, screen, button, or form updates the command bar accordingly.
2. **App Actions:** The command bar provides access to various app-specific actions such as renaming, sharing, running the app checker, adding comments, previewing, saving, and publishing the app. These actions facilitate effective app management and collaboration.
3. **Properties List:** When an object is selected on the canvas, the properties list displays all the properties of that object. This list allows you to customize the object's attributes easily.
4. **Formula Bar:** You can compose or edit formulas for the selected property using one or more functions. It features IntelliSense, which provides suggestions and inline help to help you write accurate formulas.
5. **App Authoring Menu:** This menu offers various options, such as switching between data sources, inserting controls, adding media, and accessing Power Automate flows. It helps you navigate through different aspects of app development efficiently.
6. **App Authoring Options:** Depending on the selection in the authoring menu, the options panel on the right displays relevant configurations. For example, selecting a data source allows you to add, refresh, or remove data connections.
7. **Canvas/Screen:** You compose the app structure in the central canvas area. It shows the currently selected screen from the authoring menu and allows you to add and arrange controls.
8. **Properties Pane:** The properties pane provides a UI format list of properties for the selected object, enabling easy customization. It includes a generic properties tab for basic settings and an advanced tab for more detailed configurations.
9. **Settings and Virtual Agent:** From the command bar, you can access app settings, such as general configurations, display options, upcoming features, and support. Additionally, the virtual agent provides real-time, in-product help, assisting you with common scenarios and questions.
10. **Screen Selector:** The screen selector allows you to switch between different screens in your app. If your app has multiple screens, this tool helps you navigate and manage them effectively.
11. **Change Canvas Screen Size:** You can adjust the canvas screen size during the authoring process. This feature ensures that your app looks good on different devices and screen sizes.

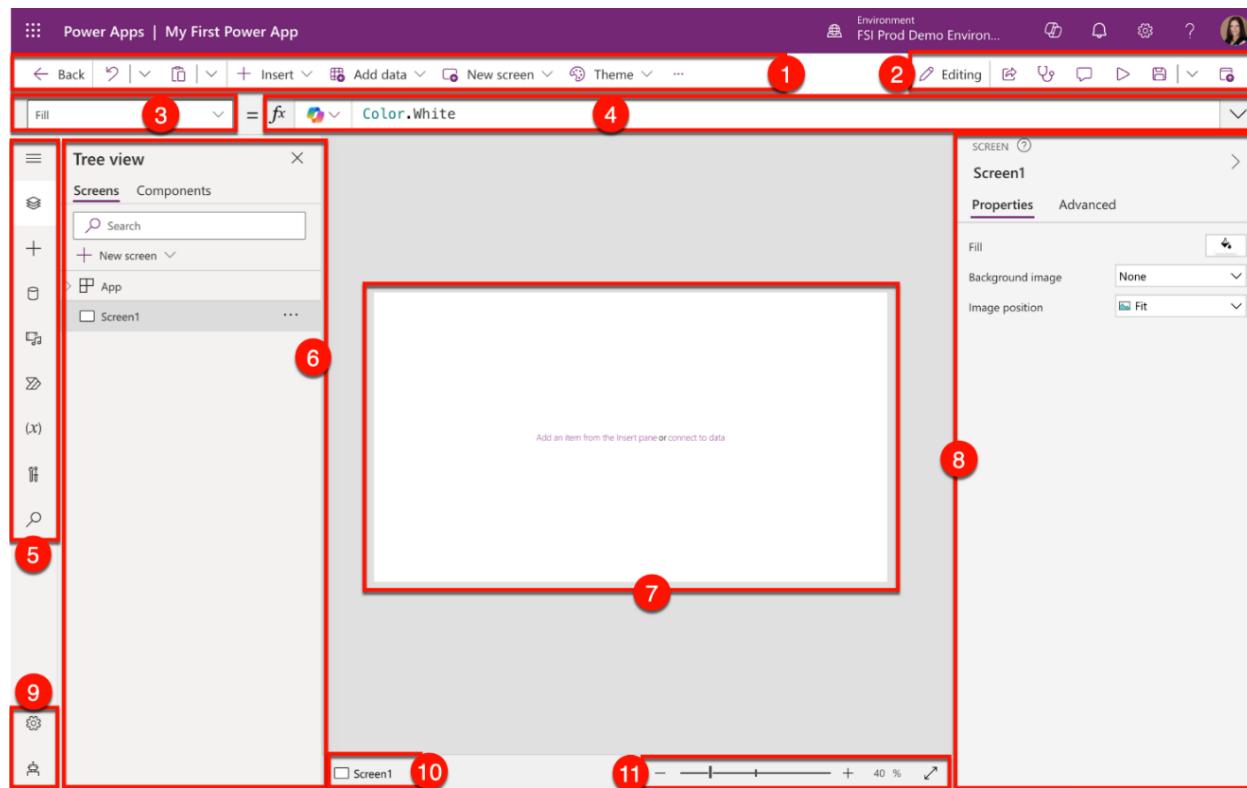


Figure 21-7: Power Apps Studio interface

For more information on the Power Apps Studio interface, please visit [Understand Power Apps Studio](#).

Power Apps Studio App Settings

Understanding the settings within Power Apps Studio is crucial for optimizing your app development process and ensuring your apps are configured correctly. Here are some key settings to be aware of, which you can access in Power Apps Studio by clicking on the gear icon on the left command bar.

General Tab

The General tab in Power Apps Studio allows you to configure fundamental settings for your app, such as its name, description, and appearance. These settings help define the app's identity and behavior, ensuring it aligns with your organizational standards and functional requirements.

- **Name and Description:** In the General section, you can set your app's name and description. The name helps users identify the app, while the description provides a brief overview of its functions. It's important to make the description clear and concise to assist end-users in understanding the app's purpose.
- **App Icon:** You can choose an app icon or upload a custom image. Custom images must be 245px by 245px and in .jpg or .png format. Ensure the image aligns with your company's branding for a consistent look.
- **Auto Save:** The Auto Save feature is enabled by default and saves changes every two minutes. This browser-level setting helps prevent data loss by automatically saving your work as you go.
- **Offline Capability:** You can enable the "Can be used offline" setting to allow the app to function without a network connection. This feature is only available for apps in a solution connected to Dataverse. You can also select an offline profile to define which data will be available offline.
- **Modern Controls and Themes:** By turning on the *Modern controls and themes* setting, you can use the latest controls and themes as they are released. When enabled, these modern controls will appear in the Modern tab of the Insert pane, and modern themes will be available in the Themes pane.

Enabling modern controls and themes ensures your apps are visually appealing and consistent with the latest design standards.

- **Data Row Limit:** This setting allows you to specify how many rows of data are retrieved from server-based connections when delegation is not supported. The default value is set to 500 rows, but this can be increased up to a maximum of 2,000 rows. Adjusting the data row limit helps manage performance and ensures your app handles large datasets efficiently.
- **Debug Published App:** This setting enables you to publish debug information with the app, providing additional telemetry and app expressions in the Power Apps Monitor. This is useful during development for debugging purposes but should be turned off before pushing the app to production to avoid performance issues.
- **Automatically Create Environment Variables:** Enabling this setting automatically creates environment variables when connecting to data sources. These variables allow you to manage data sources more effectively within solutions.
- **Enable App.OnStart Property:** This setting allows you to use the *App.OnStart* property, which can delay app loading. This setting should be used cautiously, and alternatives such as *App should be used.StartScreen* is recommended for better performance and user experience.

Display Tab

The Display tab in Power Apps Studio allows you to configure your app's screen size and orientation, which is crucial for ensuring a consistent and optimal user experience across different devices. Here are the key settings available in the Display tab:

- **Orientation:** Choose the orientation for your app, either Landscape or Portrait. The orientation determines how the app is displayed on the screen. Landscape is typically used for tablets and PCs, while Portrait is commonly used for mobile devices.
- **Size:** Select the screen size for your app from the available options. The default setting is 16:9, a common aspect ratio for many devices. Adjusting the size can help fit your app's design to specific device requirements.
- **Scale to Fit:** When turned on, this setting scales the app to fit the available space on the screen. Turning this off allows screens and controls to fill the available space without scaling, which can be useful for maintaining your app's original design and proportions.
- **Lock Aspect Ratio:** Enabling this setting automatically maintains the ratio between height and width to prevent distortion. This ensures your app's layout and design elements remain consistent regardless of screen size changes.
- **Lock Orientation:** This setting keeps the screen in its current orientation, even when the device is rotated. This is useful for maintaining a consistent user experience and preventing accidental orientation changes that might disrupt the app's usability.
- **Show Mobile Device Notifications Area:** When this setting is turned on, the mobile operating system's notifications area will always be visible at the top of the screen. This allows users to see the time, notifications, and other system indicators while using the app. Turning it off hides the notifications area, providing a more immersive app experience.

These settings help you tailor your app's display characteristics to provide the best possible user experience across different devices and use cases.

Upcoming Features Tab

With every release, Power Apps introduces new features and improvements to enhance functionality and user experience. However, it is essential to understand the stages of feature rollouts to manage their impact on your apps effectively. Power Apps features undergo several stages before becoming generally available. Here's a summary of each stage:

- **New:** These features are new and generally available (GA), fully supported, and documented. They are typically enabled by default for new apps but may take time to deploy universally. You can enable them for existing apps at your convenience.
- **Preview:** These features are nearly complete and will soon move to the New stage. However, they may still change. This stage provides the last opportunity for feedback. Preview features are generally turned off by default, are documented, and should not be used in production as they are covered by the Preview terms of service.
- **Experimental:** These early-stage features are experimental and may never reach GA. They are used to assess the feature's value proposition and design. These features can change significantly or be removed at any time. They are off by default, generally not documented, and should not be used in production. They are also covered by the Preview terms of service.
- **Retired:** These are GA features that are being phased out. They are still fully supported and documented but are either being replaced by better alternatives or have low usage. You should disable these features for existing apps at your own pace. They are generally off by default for new apps.

The duration a feature stays in each stage varies. Factors such as the number of apps using the feature, reported issues, and the urgency of the feature's release influence the timeline. Features can remain in a stage from several weeks to many months, and sometimes, stages may be skipped if deemed unnecessary.

When you access the **Upcoming Features** in settings, you will see three settings tabs: *Preview*, *Experimental*, and *Retired*. Enable *Preview* features if you want to test upcoming functionalities before they are made available to everyone. Generally, Preview features advance to the New stage after sufficient testing and feedback. Enable *Experimental* features if you're an early adopter, find something useful, or want to help test it. Experimental features are in an early-stage preview and may change significantly or be removed anytime. Activate *Retired* features only when you need to retain an older functionality. When possible, turn off these features in your existing apps.

To learn more about Upcoming Feature settings, please visit [Understand new, preview, experimental, and retired features in canvas apps](#).

Support Tab

The Support tab in Power Apps Studio provides essential information and tools to assist with app development and troubleshooting. Here are the key elements found in this section:

- **Environment:** This field displays the name of the current environment where your app is being developed or tested.
- **Authoring Version:** The authoring version indicates the version of Power Apps Studio being used, such as 3.24062.17. This version determines which features and functionalities are available. It is recommended not to change the authoring version while working on an app, as this can potentially introduce bugs in existing features. If the authoring version is updated during development, the app must be retested to ensure it operates as expected.
- **Session ID:** The session ID is a unique identifier for your current session in Power Apps Studio. This ID can be helpful when seeking support or troubleshooting issues, as it allows for precise tracking of your session activities.
- **Session Details:** Clicking on *Session details* provides more in-depth information about your current session, which can be helpful for debugging and technical support.
- **Helpful Links:** This section includes links to official Power Apps documentation, Terms of Use, Open-Source Licenses, and the Privacy Statement.

Utilizing the Support tab effectively can help ensure smooth app development by providing the necessary information and resources at your fingertips.

Best Practices for Designing Canvas Apps in Power Apps Studio

Designing an effective and user-friendly canvas app in Power Apps Studio requires a blend of strategic planning, thoughtful design, and technical best practices. Whether you are a beginner or an experienced developer, adhering to these best practices ensures that your app meets user needs, performs efficiently, and remains maintainable over time. This section outlines key guidelines to help you create robust and user-centric canvas apps, ensuring a seamless and engaging user experience.

Understand User Needs: To ensure your app meets users' needs, start by gathering detailed requirements from end-users. Developing user personas can help you understand the different types of users who will interact with your app. Additionally, incorporating user feedback throughout the development process is crucial for refining features and improving usability.

Plan Your App Structure: Before developing, plan your app's structure. Creating wireframes or sketches of your app screens can help visualize the design. Planning the navigation flow to ensure a logical and intuitive user journey is important. Organizing components in a hierarchical structure will maintain clarity and ease of use.

Design for Usability: Maintaining a consistent layout and design across all screens provides a seamless user experience. Ensure your app is accessible to all users by following accessibility guidelines, such as color contrast and screen reader support. Additionally, design your app to be responsive to different screen sizes and orientations to accommodate various devices.

Performance Optimization: Optimize your app's performance by using delegation and efficient data querying techniques to handle large datasets without compromising speed. Avoid using too many controls on a single screen, which can slow down the app and overwhelm users. Compress images and other media to reduce load times.

Maintainability: Your app will be easier to maintain if you use clear and consistent naming conventions for controls, variables, and collections. Break down complex logic into reusable components and functions to simplify maintenance and updates. Document your app's structure, data sources, and key functionalities to assist future developers in understanding and maintaining the app.

Security and Compliance: Implement security measures to protect sensitive data, such as encryption and secure data storage. Use role-based access control to ensure users can only access the data and features they need. Additionally, ensure your app complies with relevant data protection regulations, such as GDPR and HIPAA.

Testing and Validation: Regular testing during development helps identify and fix issues early. Conduct user acceptance testing (UAT) with a group of end-users to validate the app's functionality and usability. Implement robust error handling to provide meaningful error messages and maintain app stability.

Continuous Improvement: Use analytics to monitor app usage and identify areas for improvement. Adopting an iterative development approach allows you to continuously refine and enhance your app based on user feedback and performance data. Providing training and support resources will help users get the most out of your app.

By adhering to these best practices, you can create a Power Apps canvas app that is user-friendly, efficient, and maintainable, ultimately delivering a better experience for your end-users.

Building Power Apps

Creating a Power App involves several steps, from planning and design to development and deployment. Power Apps provides a robust environment that enables users to create canvas and model-driven apps, catering to various business needs.

Creating a Canvas App

To start, open <https://make.powerapps.com> or select the Power Apps icon from the app menu. From the main page, you can create new apps from scratch or start with a predefined template. Templates are helpful in learning how to build Power Apps and understanding the scenarios where Power Apps can be beneficial. To see the available templates, click **+ Create** from the left navigation menu and scroll down to the **Start from template** section. For this example, select **Power Apps Training**. A dialog box will appear, allowing you to update the app name optionally. Click **Create** to proceed. This application contains hands-on exercises that help you learn the basics of building canvas apps.

When the Power Apps designer studio opens, it will show three panels and a message with a Make my own app button. Before continuing, make this app your own by selecting the **Make my own app** button, choosing **OneDrive for Business**, and clicking **Done**. The Power Apps designer studio will reload in the browser once complete. Now save the app by clicking the **Save** icon in the upper-right corner.

The top-right menu contains two essential buttons: App Checker and Preview. The App Checker ensures there are no bugs in the application before it is published. The *Preview* button allows you to run the application for testing before publishing. For this app, use Preview to play the app and go through the training exercises instead of publishing it immediately. To begin, click the **Preview** button, which looks like a play icon, to run the application. The application will load with a start screen providing instructions for the hands-on exercises (Figure 21-8):

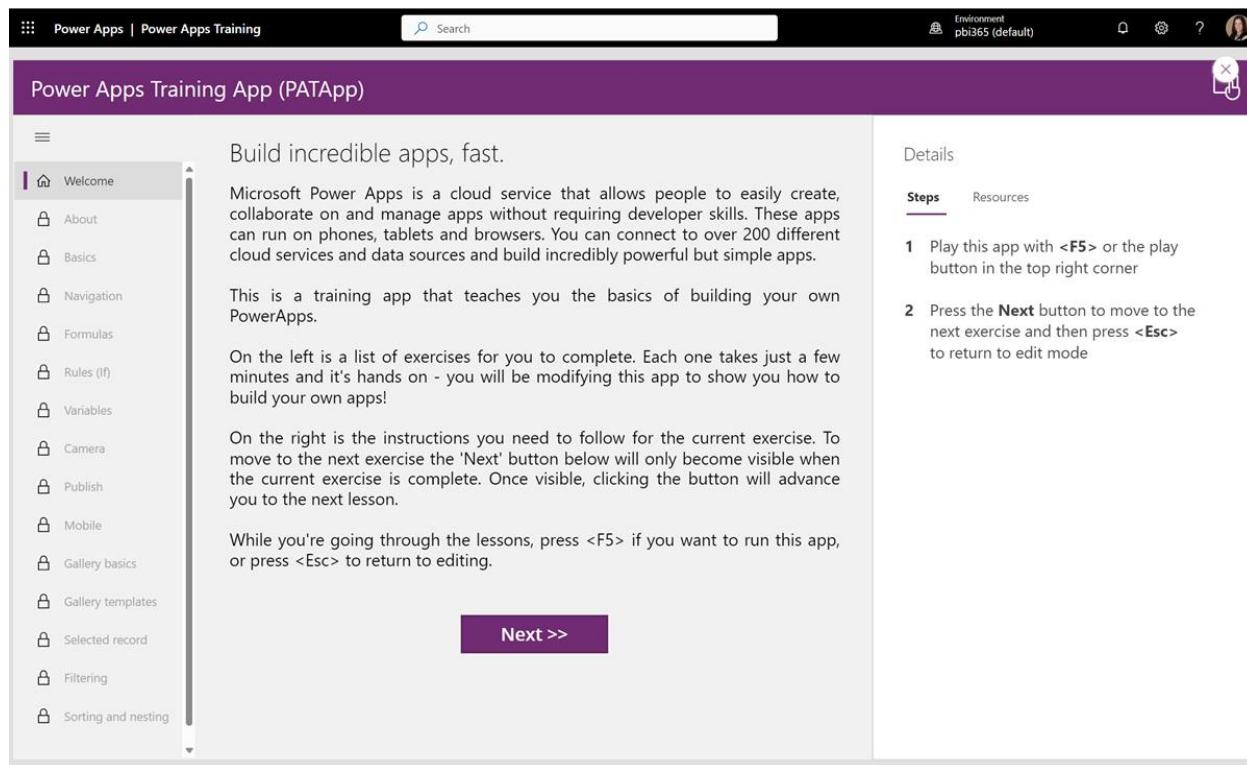


Figure 21-8: The Power Apps application running

The hands-on exercises in this application provide an excellent way to learn the basics of building canvas apps. Once you have completed the exercises, you can publish this app or save and close it. Now that you feel more comfortable with the basics of building a canvas app, you can continue to explore the other template apps or create your own from scratch. When you are satisfied with the application you're working on and ready to publish, go to Settings in the left command bar. Define the final name for the application, update any additional settings, such as the description, and then close the settings dialog. To save, click the **Save** icon located in the top menu. Click the **Publish** icon to publish the application and make it available to users. For

more in-depth documentation and how-to guides on building canvas apps, visit [Power Apps canvas apps documentation](#).

Power Apps Components

Components are the building blocks for canvas apps. They allow app creators to develop custom controls for use within a single app or across multiple apps using a component library. These components can include advanced features like custom properties that enable complex capabilities.

Components are beneficial when building larger apps with similar control patterns. When a component's definition is changed, all instances of that component within the app will reflect those changes. This approach saves time by eliminating the need to copy and paste controls, leading to better performance. Additionally, components encourage teamwork and create a consistent look and feel within an organization when a component library is utilized.

To learn how to build Power Apps Components, visit the [Canvas component overview](#).

Power Apps Express Design

Power Apps Express Design is a preview feature that allows you to create a Canvas app directly from an image, such as a wireframe or a screenshot of an existing form. To start, open <https://make.powerapps.com>, click **Create**, then click **Image**. You will be guided through a wizard that allows you to upload your image or choose from a sample image. The wizard will auto-detect what components are used, which you can easily change by clicking on a component and then select the desired component type to assign (Figure 21-9).

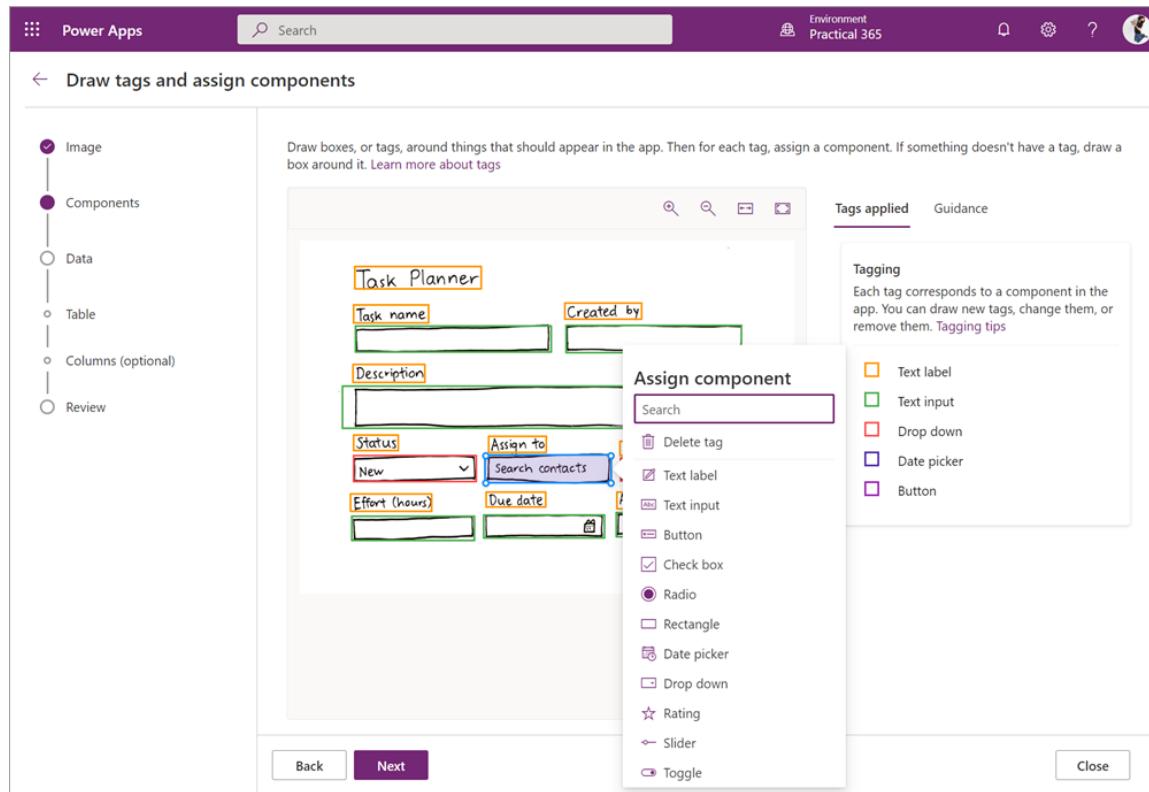


Figure 21-9: Creating app from image choosing components screen

After you define the components, you will have the option to create data using Dataverse, or you can skip and decide to connect the app to data later. Once you complete the wizard, the newly created app will open in Power Apps Studio, allowing you to continue refining the app. To learn more, visit [Create a canvas app from an image](#).

Creating Apps using Copilot

Introducing the capabilities of AI Copilot to both app developers and end-users in Power Apps. Copilot allows you to construct an application, complete with its associated data, by simply articulating your requirements through a series of conversational steps. Your applications will come with Copilot-driven features integrated from the initial screen, enabling users to unearth insights through natural conversation rather than relying on mouse clicks. To learn more about how to build an app through conversation, visit [Build apps through conversation \(preview\)](#).

Creating a Model-driven App

Model-driven Power Apps are a type of application within the Power Apps platform that provides a data-centric approach to app development. Unlike canvas apps, which start with the user interface and allow for extensive customization, model-driven apps begin with the underlying data model. They are built upon the structure of this data. This approach ensures that the app is aligned closely with the business data and processes intended to support. Key characteristics of Model-driven Power Apps:

- **Data-First Design:** Model-driven apps are built on Dataverse, which provides a scalable and secure data platform. The development process starts by defining the data model, including tables (formerly known as entities), relationships, and fields. This structured data model forms the backbone of the application.
- **Components and Logic:** Once the data model is established, developers can create and configure various components such as forms, views, charts, and dashboards. Business rules and process flows can also be added to enforce data integrity and guide users through complex business processes. These components help present data in a meaningful way and automate workflows within the app.
- **Responsive User Interface:** The user interface of model-driven apps is automatically generated based on the data model and components defined. This ensures a consistent and responsive user experience across different devices, including desktops, tablets, and smartphones. Users benefit from a familiar and intuitive interface that adapts to their screen size and device capabilities.
- **Integration with Dataverse:** Model-driven apps leverage Dataverse (formerly Common Data Service) to store and manage data. Dataverse provides robust data management features, including security, auditing, and data validation. It also supports integration with other Microsoft and third-party services, enabling seamless data flow and collaboration across the organization.
- **Business Process Automation:** Model-driven apps support advanced business process automation through business process flows and Power Automate. Business process flows guide users through predefined stages and steps to ensure data entry and task completion consistency. Power Automate workflows can be integrated to automate tasks such as notifications, data updates, and approvals.
- **Reusability and Scalability:** The components and logic defined in model-driven apps are reusable across different applications within the same environment. This promotes consistency and reduces development time for new applications. Additionally, model-driven apps are scalable, allowing organizations to handle large volumes of data and complex business requirements.
- **Security and Compliance:** Model-driven apps inherit the security features of Dataverse, including role-based access control, field-level security, and auditing. This ensures that data is protected and only accessible to authorized users. Comprehensive data governance features also support compliance with regulatory requirements.

To start building your first model-driven app, follow the instructions in [Build your first model-driven app](#).

Note: To work with model-driven apps, you need a database in Dataverse and a separate environment. You must have a paid plan account or use a developer plan environment to obtain both. For paid plan accounts, remember to assign the licenses to the users after purchasing the service from Microsoft.

As mentioned earlier in the chapter, the interface and layout of model-driven apps are built on the structured data and relationships defined in Dataverse. Model-driven apps can be used for single purposes or multiple purposes. For example, Figure 21-10 displays a model-driven app used for both a Build a Bot and a Customer Workshop process. Notice the image shows a Business Process flow at the top, which moves the process through different stages, ensuring that all necessary steps are completed systematically. This highlights the effectiveness of model-driven apps in managing data that needs to follow a specific process. In this use case, a canvas app is utilized for the intake form for users to submit bot requests, while the model-driven app manages the process of the request.

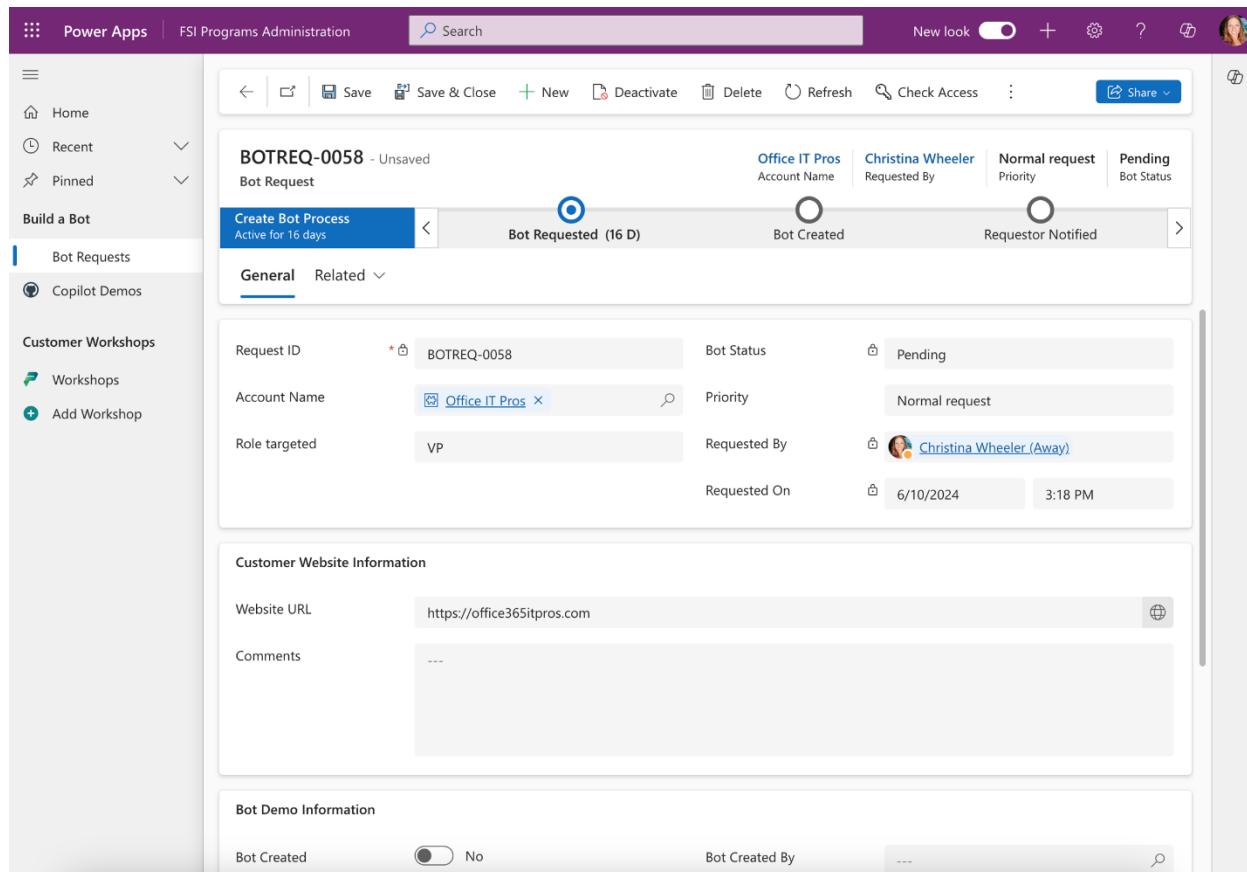


Figure 21-10: Example Model-driven app for a Bot Request process

Creating a SharePoint Integrated Power Apps app

With Power Apps, you can customize SharePoint Lists and Library forms as was possible with InfoPath before Microsoft deprecated InfoPath. Power Apps has a similar integration with Lists and Libraries and embeds its forms within the SharePoint List or Library.

To start with SharePoint Lists, you can work with an existing modern list or create a new custom list. If you create a new List, ensure it is using the Modern user experience. From the command bar of the list, select **Integrate > PowerApps > Customize forms**. You can then select the fields to show in the list from the available set (Figure 21-11).

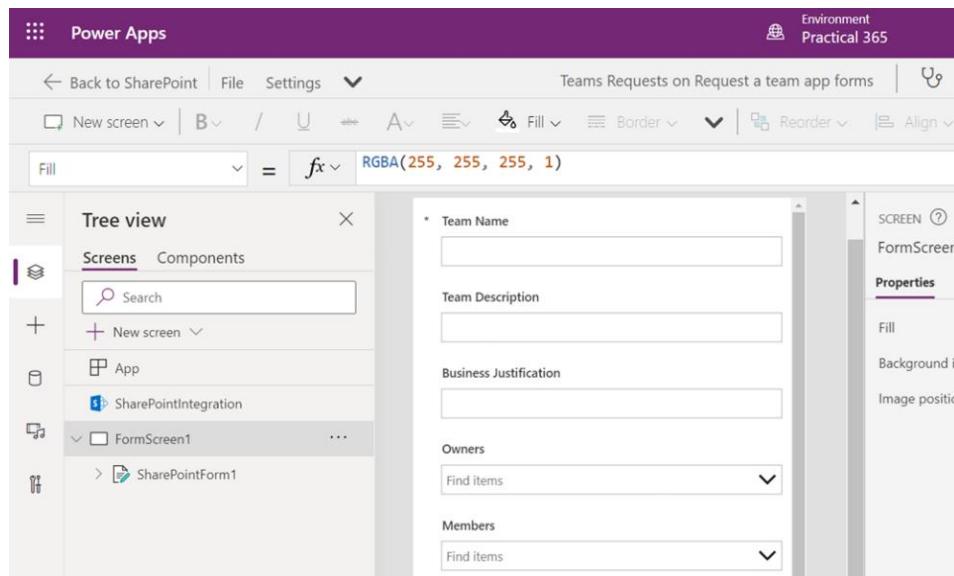


Figure 21-11: A Power Apps Canvas app to replace the default form for a SharePoint List

The complete functionality of Canvas apps is present: you can reorder the fields, change their properties, set conditional formatting to, for example, appear/disappear based on the content of other fields, etc. When you finish, test the app with the **App Checker** button, **Save** and **Publish to SharePoint** the new form.

The Power Apps form replaces the default SharePoint forms automatically. When a user clicks on **+New** to create a new item, the form appears in place of the old form (Figure 21-12):

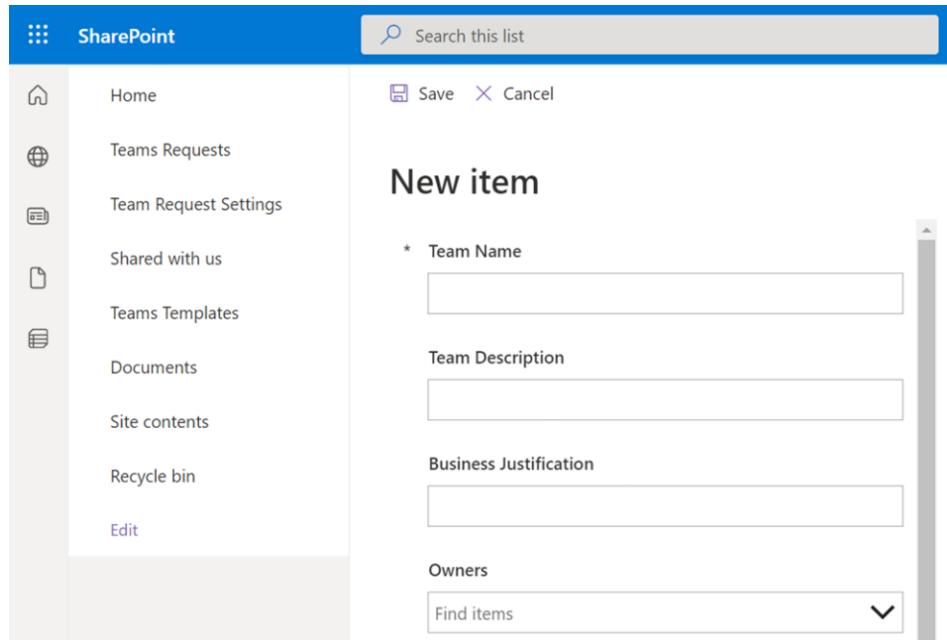


Figure 21-12: A Power Apps Canvas app replacing the default form in a SharePoint List

If changes are needed, the List owner can open the Power App to modify by navigating the same way as when creating a Power App customized form. From the command bar of the list, select **Integrate > PowerApps > Customize forms**.

If you want to change the list back to using the default SharePoint form instead of the Power App customized form, you can re-activate it through the List settings. To re-activate the original form, go to the List in SharePoint, open the **Settings** page by selecting the gear icon near the upper-right corner, and select **List Settings**. On the settings page, select the **Form Settings** link under the **General Settings** section. A new page will open. Then select **Use the default SharePoint form** and save the changes. When using the default

form, if you return to the Form Settings page, you will see an extra link **Delete custom form** in the section of Power Apps, under **See versions and usage**. Use this option to remove the Power Apps form.

Take into consideration that if you customize the form for a SharePoint List, the form doesn't appear as an app in Power Apps Studio or Power Apps Mobile. The Power App form can only be opened from the list for which you created it. Anyone with SharePoint permissions (to manage, design, or edit the associated List) can customize the forms. Any guest users who do not have a plan that includes Power Apps will get an error message if they try to access a list form that has been customized using Power Apps.

Using the Apps

Power Apps provides various ways for users to access and utilize the applications you create, ensuring flexibility and convenience across different platforms. Whether on mobile devices, browsers, SharePoint Online, or within Microsoft Teams, users can easily interact with Power Apps in their preferred environment. Below are the different methods for making Power Apps available to users:

Mobile Access

All Power Apps are mobile-enabled, and Microsoft provides Power Apps applications for Android and iPhone. Users can start the Power Apps phone app and log in with their Microsoft 365 account. A list of accessible apps will appear. By clicking on any of these apps, users can open and start using them immediately.

Browser Access

Users can access Power Apps from any browser supported by Microsoft 365. When a Power Apps app is published, it receives a unique identifier that can be used to direct any browser to the app directly. For example, a URL might look like this: <https://apps.powerapps.com/play/e/default-9e163937-b682-4f9f-95ec-76cbf73d9ea0/a/964f1923-2de1-4afd-8908-95809e5853c0?tenantId=9e163937-b682-4f9f-95ec-76cbf73d9ea0>.

You can retrieve the identifier and URL from the app properties (use the details link from the ellipse button in the apps list). Users can bookmark the URL for quick access.

SharePoint Integration

SharePoint Online offers a web part specifically for embedding and interacting with Power Apps on any modern SharePoint page. To host a Power Apps app on a SharePoint page, add the Power Apps web part, configure the URL or identifier of the app, and then publish the page.

Microsoft Teams Integration

Team owners can add Power Apps as a channel tab in Microsoft Teams. This allows team members to access and use the app directly within the Teams environment.

Moving Power Apps Between Environments

A common task for Power Apps administrators is moving apps from development/test environments to production environments or between different Power Platform environments. This can be achieved using two primary methods: export/import functionality or the building of a Power Apps solution.

Exporting and Importing Canvas Apps

Canvas apps can be moved using the Export package feature under the Apps section. Only the owner and co-owner of an app can export a canvas app package. To import an app, the account must have the Environment Maker permission. Follow the steps below to export a canvas app:

1. From the main window of the Power Apps website, click on the **Apps** menu on the left side to display the list of published apps.
2. Click the vertical ellipsis button next to the app you wish to export.

3. From the contextual menu, select **Export** package.
4. In the export window, use the **Action** button (Figure 21-13) to decide whether the package will create a new app or update an existing app when imported.
5. Click the **Export** button to generate a .zip file, which will be downloaded to your local computer.

Continue with the steps below to import the canvas app into an environment:

1. On the same page with the list of apps, click the **Import** canvas app link at the top of the page.
2. In the new window, click **Upload** and **browse** to the .zip file you wish to import.
3. Once uploaded, another window will display the package details.
4. Click the **Import** button to complete the import process.

Note: If any errors occur (e.g., trying to create an app that already exists), an error message will indicate the problem. If the app uses connectors that are not yet configured, the import menu will prompt you to select or create new connections.

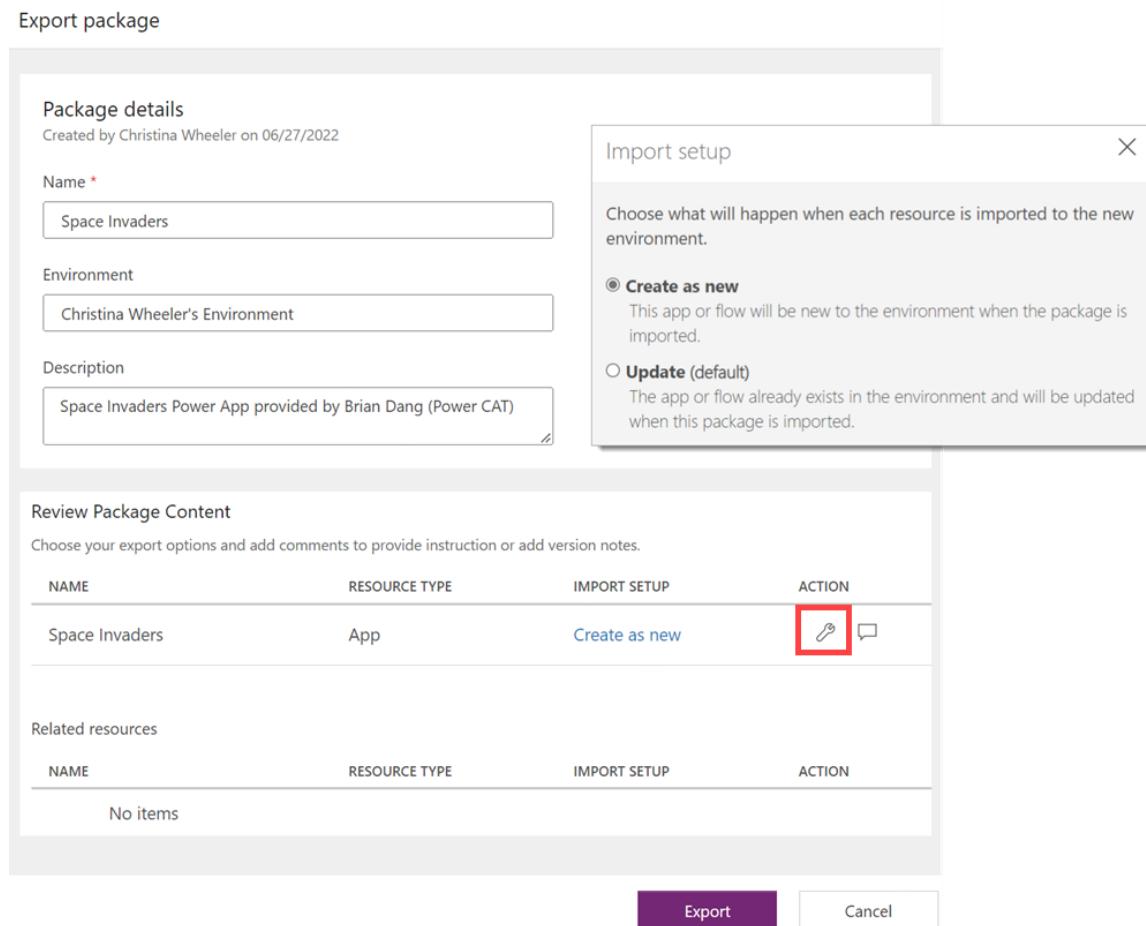


Figure 21-13: Creating an export package for one Power Apps app

GDPR and Power Apps

The European Union GDPR regulations oblige app developers to manage user personal data in an accountable way. GDPR has two consequences for Power Apps: users can request a data controller (usually a company) to retrieve their data at any moment ("right of data portability"), and they can also require the data controller to remove their data ("right to erasure") from the system. Power Apps saves personal information in the Environments, Canvas apps, Gateway, Custom Connectors, and Connections.

In general, users can find their information in the Power Apps Portal or using the [App Creator PowerShell cmdlets](#). A user has the right to find and modify their information only. An administrator with Global Administrator rights can do the same for all users. In some cases, a Power Apps paid license plan is required. Microsoft details the actions necessary to [export](#) or [remove](#) personal user data using the Power Apps Portal and/or the PowerShell cmdlets online.

Power Apps Code Review Tool

In 2021, Microsoft released a solution for conducting code reviews of Canvas apps. This Power Apps Code Review Tool is available for free download from GitHub and can be deployed into your tenant. It uses the Power Apps Language Library to process and extract information about the app. To begin, simply [download and install the solution following the installation instructions](#).

Once installed, you can evaluate existing apps from within your tenant or upload a .msapp file for any canvas app. To download, open the app in Power Apps Studio. Click **File > Save As** and download a copy to your computer using the **This computer** option. Next, from the Power Apps portal, run the **Power Apps Code Review Tool** app and click the **New Review +** link button. When prompted with the dialog, input the app name, upload the .msapp file, fill out any additional optional information, and click **Submit**. The app will then begin to process your canvas app, showing a status of Processing, and will change to a **Review** link once the processing has completed. The **Code Review Checklist** screen will display a score and list of patterns with a pass or fail for each pattern (Figure 21-14). You will see a comment for each failed pattern and a link to view more details. The **App Checker Results** will provide information on issues such as unused variables, delegation issues, and insufficient loading. The App Analysis section lets you see what important app settings are. The **Code Viewer** section displays the screens, controls, and properties used in the app with options to search and filter. The **Statistics** section shows the score, grade, number of passed patterns, and a summary of failed patterns.

Status	Name	Description	Comment
✓	N+1 Database or API requests Performance	N+1 query, which are used often in galleries, can trigger too many requests to servers. This happens when one or more controls within a gallery are bound to a LookUp() or Filter() operation on a data source.	View Details
✓	Nested Search, Filter or LookUp operations in formulas Performance	Consider simplifying nested formulas with Search() and Filter() operations. Avoiding the nesting of these two together leads to a more compact/concise formula and performance improvement.	View Details
✗	Code Readability Maintainability	Avoid expressions or formulas that are very long as they will become hard to read. Examples include, but are not limited to nested If/Then/Else statements and nested operators such as OR and AND.	Code review tool : 1315 characters long code without comments. View Details
✗	Use of Concurrent Function Performance	Consider using the Concurrent() function for parallel independent data requests. Look out for opportunities to use it whenever operations are not dependent on sequential data operations.	Code review tool : This app does not make use of Concurrent function. Please consider use it to ensure external database or API requests are performed in parallel. View Details
✓	Error Handling Coding Standards	Always ensure apps have appropriate error handling methods. It is best to use the IfError() function to manage data validation for Patch() commands and the OnSuccess/OnFail properties when submitting form data.	View Details
✗	App Settings flags Performance	Review app settings to ensure both Delayed Load and Explicit Column Selection is enabled to reduce latency on application load.	Code review tool : Advanced Settings. Please consider turning on the following settings : View Details

Figure 21-14: Power Apps Code Review Tool checklist example

Guest Access to Power Apps

Power Apps is a platform that allows you to create and share apps within your organization. You can grant guest users access to Power Apps by inviting them as Entra ID external users. Guest users are individuals with

email addresses outside your domain. To invite guest users, you need to have the Global Administrator or User Administrator role. You can then use the Entra ID admin center or PowerShell to send invitations to the guest users and assign them the appropriate Power Apps licenses and roles. Guest users can sign into Power Apps using their email addresses and access the apps you shared with them. For guest access prerequisites, visit [Share a canvas app with guest users](#).

Power Apps Preview Program

The Power Apps Preview Program provides a way for you to test upcoming features. This can be useful to validate your current production apps will work with the next upcoming Power Apps updates (vNext). For more information on how to enable, visit [Power Apps preview program](#).

Licensing Power Apps

The licensing for Power Apps is like Power Automate where Microsoft 365 users get a non-premium license allowing them to create Apps for Microsoft 365 using standard connectors. For Power Apps, there are three premium plans which include **Power Apps Premium per-user**, **Power Apps per app**, and **Pay-as-you-go**. Premium licenses are required for Dataverse, model-driven apps as well as canvas apps that use premium or custom connectors. For more information on Power Apps plan pricing, visit [Power Apps pricing](#).

Administrators who need access to admin views in Power Automate, Power Apps, and Dataverse do not need a license. However, a license is required for further administration, such as specific Sales and Marketing modules for Dynamics 365 and the use of custom connectors.

Power Platform Solutions

Solutions in Power Platform provide a structured way to manage and distribute various components such as apps, flows, and custom connectors across different environments. There are two types of solutions that can be deployed:

- **Unmanaged Solutions:** Used during the development phase, these allow full customization and can be transported to other development environments. Unmanaged solutions are considered the source of customization.
- **Managed Solutions:** These are used to distribute solutions to production environments, and these restrict certain customizations to protect the integrity of the solution after deployment.

Key Features and Usage

To create a solution, navigate to the **Solutions** area in the Power Apps maker portal. Here, you can manage and customize components within the solution, aiding in the organization and distribution of customizations.

Managed Properties allow you to control which components within your managed solutions can be customized. By setting these properties, you can prevent modifications that could potentially break the solution when it is imported into another environment. This ensures that the integrity of the solution is maintained and any necessary customizations are controlled and consistent. **Integration with Pipelines** enhances the deployment process for solutions. Pipelines enable the deployment of solutions to test and production environments, allowing makers to initiate deployments directly within their development environments. This feature simplifies the deployment process, ensuring that solutions are consistently and accurately deployed across different environments.

Known Limitations

While solutions provide robust management and deployment capabilities, there are certain limitations to be aware of. For instance, issues can arise with canvas apps that are connected to flows no longer present in the

environment. Reviewing these limitations and addressing potential issues is crucial for ensuring smooth operation and functionality of your solutions.

Additional Features

Solutions in Power Platform offer robust features to enhance the management, customization, and deployment of applications. One key feature is version control, which allows for tracking changes and maintaining different versions of components. This capability is particularly useful for managing updates and ensuring consistency across various environments. By utilizing version control, users can maintain a record of modifications, making it easier to revert to previous versions if necessary, thereby maintaining a stable development process.

Dependency Management ensures that all necessary elements are included and properly configured, preventing issues related to missing or misconfigured components during deployment. This functionality guarantees a smooth and error-free transition of solutions between environments.

In addition, solutions provide robust security and governance features. These features enable effective control over access to components and management of permissions, ensuring that only authorized users can modify or deploy solutions. By implementing these security measures, organizations can safeguard their applications against unauthorized changes and ensure compliance with organizational policies.

Overall, these key features and usage practices enable effective management, customization, and deployment of Power Platform solutions, ensuring they meet organizational needs while maintaining integrity and performance. For more detailed information, you can refer to the [Microsoft Learn documentation](#).

The Power Platform Creator Kit

The Power Platform Creator Kit is a collection of managed solutions that enhance developer productivity by offering a component library, commonly used controls from the Power Apps component framework, templates, and utilities. The kit incorporates the Fluent UI framework to ensure the creation of visually appealing and consistent user experiences for customized business applications. It is delivered as a self-contained solution, encompassing 24 Power Apps components, a reference app for interactive learning (model-driven with custom pages), a canvas page template, a canvas template app, and a theme editor that generates Theme JSON for effortless styling of components. To learn more, visit the [Creator kit](#).

The Power Platform CoE Starter Kit

The Power Platform Center of Excellence (CoE) Starter Kit is a comprehensive set of tools designed to help organizations drive innovation, improvements, and strategies to adopt and support Microsoft Power Platform (including Power Apps, Power Automate, and Copilot Studio). This kit provides tooling and automation through apps, Power BI analytic dashboards, and flows, which aid teams in building the monitoring and automation necessary to support a CoE.

The CoE Starter Kit is an open-source initiative available on GitHub, with detailed installation and configuration instructions provided by Microsoft. To utilize the kit, administrator accounts must have Premium licenses and be granted Microsoft Power Platform service admin, global tenant admin, or Dynamics 365 service admin rights in the Office 365 tenant.

The Core Components of the Starter Kit, one of its four parts, contain assets specifically relevant to administrators. The kit collects extensive information about apps, flows, flow action details, custom connectors, connectors, model-driven apps, shared-with information, chatbots, and logs. This data is displayed in Power BI dashboards, providing administrators with comprehensive insights and analytics.

By leveraging the Power Platform CoE Starter Kit, organizations can enhance governance, drive adoption, and maintain operational efficiency, ensuring successful implementation and management of their Power Platform solutions. To get started, you can download the CoE Starter Kit from its [GitHub repository](#) and follow the setup instructions on the [Microsoft Learn documentation](#).

Updates for the CoE Starter Kit

The CoE Starter Kit is updated monthly to incorporate new features, improvements, and bug fixes. It is recommended that the CoE Starter Kit be upgraded at least every three months to avoid unexpected issues and stay current with the latest capabilities. Among recent updates are:

- **Governance Components:** The updated CoE Starter Kit includes new governance components that help organizations establish audit compliance and streamline archival processes. Enhanced audit capabilities allow administrators to track user activities, monitor environment changes, and ensure compliance with internal and external regulations. New archival processes help manage the lifecycle of Power Platform resources, automating the archiving of unused or outdated apps, flows, and environments.
- **Data Export and Insights:** The CoE Starter Kit now integrates with Data Export capabilities, allowing organizations to export data to Azure Data Lake or other analytics platforms. This enables more advanced analysis and reporting, helping organizations gain deeper insights into Power Platform usage, adoption trends, and performance metrics. Administrators can create customized reports and dashboards using the exported data, providing detailed views of app and flow usage, user activity, environment health, and more.
- **Enhanced Monitoring and Alerts:** Advanced monitoring tools provide real-time visibility into the health and performance of Power Platform environments. Automated alerting capabilities notify administrators of critical events and issues, ensuring proactive management of the Power Platform. Alerts can be configured for various scenarios, such as policy violations, capacity limits, or performance degradation.
- **Nurture Components:** The nurture components, including the Maker Assessment app, help accelerate platform adoption and provide guidance for makers on governance and licensing considerations.

By integrating these updates, the Power Platform CoE Starter Kit significantly enhances its value as a governance and management tool, providing organizations with the capabilities needed to maintain control, ensure compliance, and drive successful adoption of the Power Platform.

ALM for the Power Platform

ALM (Application Lifecycle Management) for the Power Platform refers to the set of practices, processes, and tools used to manage the entire lifecycle of applications built on the Microsoft Power Platform. Key components of ALM for the Power Platform include:

- **Development:** This involves creating and designing applications using Power Platform tools.
- **Version Control:** ALM for the Power Platform involves versioning control mechanisms to track changes made to applications over time. Version control systems like Git are commonly used to manage code changes.
- **Testing and Quality Assurance:** Testing is crucial to ensure that applications built on the Power Platform meet business requirements and function as intended. This includes unit testing, integration testing, and user acceptance testing.
- **Deployment:** Deployment involves moving applications from development environments to testing, staging, and production environments. ALM practices ensure smooth and reliable deployment processes to minimize disruptions.

- **Change Management:** Change management processes are essential for managing changes to applications, including updates, patches, and bug fixes. This includes documenting changes, obtaining approvals, and communicating changes to stakeholders.
- **Monitoring and Maintenance:** Once applications are deployed, ALM practices involve monitoring their performance and health to identify and address issues proactively. This includes monitoring usage metrics, performance metrics, and user feedback.
- **Governance and Compliance:** ALM for the Power Platform includes ensuring compliance with organizational policies, regulatory requirements, and security standards. This involves implementing access controls, data encryption, and auditing mechanisms.

By implementing ALM practices for the Power Platform, organizations can improve the efficiency, reliability, and maintainability of their applications, ultimately delivering better experiences for users and stakeholders.

Build a CI/CD Pipeline for the Power Platform

While solutions can be manually exported and imported between environments, you can also deploy solutions using build tools in Azure DevOps. You can create a [continuous integration/continuous deployment pipeline](#) to manage your Power Platform Application lifecycle using Azure DevOps or through [GitHub actions](#). To learn more about ALM with the Power Platform and the options available to build a CI/CD pipeline, visit Application Lifecycle Management.

Power Platform Pipelines

While Azure DevOps is one way to set up a CI/CD pipeline, there is a new [feature](#) available for Power Platform admins to create pipelines directly within Power Platform environments. This setup uses a managed Host environment and a minimum of one Development and one Production environment. An application called Power Platform Pipelines must be installed in the host environment, which deploys a Deployment Pipeline Configuration app used to configure the pipelines. Once configured, solutions can be deployed to the designated environments configured through the pipeline.

To learn more about setting up the Power Platform Pipelines feature, visit [Set up pipelines in Power Platform](#).

ALM Accelerator Kit

The ALM Accelerator for Power Platform features a canvas app built on Azure Pipelines and Git source control. This app simplifies the creators' process, allowing them to export their Power Platform solutions to source control. It facilitates a review of their work before deploying it to target environments as part of an organization's application lifecycle management (ALM) strategy. You have the flexibility to use the ALM Accelerator as is or customize it to fit your needs. To learn more about the ALM Accelerator Kit, visit [ALM Accelerator for Power Platform](#).

Power BI

Power BI is a powerful business analytics tool from Microsoft designed to help organizations transform raw data into meaningful insights through interactive visualizations and business intelligence capabilities. It enables users to create detailed and dynamic reports and dashboards that can be shared across the organization, fostering data-driven decision-making at all levels.

Power BI is available in several forms, including Power BI Desktop for individual users, Power BI Service for cloud-based collaboration, and Power BI Mobile for on-the-go access to insights. This versatility ensures that users can access and interact with their data anytime, anywhere. Power BI integrates seamlessly with a wide variety of data sources, including databases, cloud services, spreadsheets, and web data. This flexibility allows users to consolidate data from multiple systems into a single, coherent view of their business metrics. The

platform's user-friendly interface, combined with its advanced data modeling and analytical capabilities, makes it accessible to both technical and non-technical users.

Key Features and Components

Key features of Power BI include data import and transformation, data modeling, visualization creation, and collaborative sharing. Users can leverage Power Query to clean and prepare data, use DAX (Data Analysis Expressions) to create complex calculations and build visually appealing charts and graphs to represent their data. Additionally, Power BI's robust security features ensure that sensitive data is protected and accessible only to authorized users.

Main Components

There are three main components to Power BI:

- **Power BI Desktop:** A desktop authoring tool used by report designers to access, transform, and model data, as well as build data visualizations on report pages.
- **Power BI Service:** A cloud-based central hub with workspaces for hosting Power BI reports and dashboards, enabling collaboration and sharing.
- **Power BI Mobile:** An app for mobile devices that allows users to interact with published reports using their smartphones and tablets. This app is available for Windows, iOS, and Android devices.

Additional Elements

In addition to the three main components, Power BI has two additional elements:

- **Power BI Report Builder:** Used for creating [paginated reports](#) in the Power BI Service, allowing for detailed and formatted report layouts.
- **Power BI Report Server:** An [on-premises report server solution](#) with a web portal that hosts Power BI Reports (.pbix), Excel, and paginated reports (.rdl) files without needing the Power BI Service. One limitation of Power BI Report Server is that it does not support creating dashboards, a feature currently only available through the Power BI Service.

Power BI Service

The Microsoft Power BI Service (app.powerbi.com) is the SaaS component of Power BI, often referred to as Power BI Online. This service allows users to view and interact with reports. Report designers use Power BI Desktop to publish reports to the service, and report readers can access these reports through shared workspaces. Every user (both free and licensed) receives a personal workspace called *My Workspace*. Shared workspaces are available for users with Power BI Pro or Power BI Premium licenses.

Workspaces

Power BI workspaces are collaborative environments within the Power BI service where teams can work together on Power BI content such as reports, dashboards, datasets, and dataflows. These workspaces provide a centralized location for users to access, share, and collaborate on business intelligence (BI) assets. Key features and aspects of Power BI workspaces include:

- **Collaboration:** Workspaces enable collaboration among team members by allowing them to share reports, dashboards, and datasets. Multiple users can collaborate on the same content simultaneously.
- **Access Control:** Workspaces come with access control features, allowing workspace admins to manage permissions for members. They can control who can view, edit, or publish content within the workspace.

- **Content Organization:** Workspaces help organize Power BI content into logical units based on projects, teams, departments, or any other relevant grouping. This makes it easier for users to find and access the content they need.
- **Deployment Pipelines:** Power BI workspaces can be used with deployment pipelines to facilitate the deployment of Power BI assets across different environments such as development, test, and production.
- **Integration:** Workspaces seamlessly integrates with other Microsoft services such as SharePoint, Teams, and Azure, providing a unified experience for users who work with various Microsoft tools.
- **API Access:** Power BI provides APIs that allow developers to programmatically manage and interact with workspaces, enabling automation and integration with custom applications and workflows.

Overall, Power BI workspaces play a crucial role in enabling collaboration, organizing content, and facilitating the development and sharing of insights within organizations. They are essential for teams working on business intelligence and data analytics projects.

To learn more about Power BI workspaces, visit [Workspaces in Power BI](#).

Power BI Desktop

Power BI Desktop is a comprehensive and robust desktop application used for authoring, transforming, and modeling data and creating detailed and interactive reports and visualizations. It is the primary tool for report designers to build and publish Power BI reports. Power BI Desktop provides a rich set of features that enable users to connect to various data sources, transform and clean data, create complex data models, and design visually appealing and insightful reports. To [get Power BI Desktop](#), install it as an app from the Microsoft Store or download and install the executable. You do not have to have a Power BI service account to use Power BI Desktop. We recommend signing up for the free version if you don't already have a Power BI Pro or Premium license. Key features of Power BI Desktop include:

- **Data Connectivity:** Power BI Desktop supports a wide range of data connectors, allowing users to connect to various data sources such as databases, cloud services, spreadsheets, and web data. This flexibility enables users to consolidate data from multiple systems into a single report.
- **Data Transformation and Preparation:** Using Power Query, users can clean, transform, and prepare data for analysis. Power Query provides a user-friendly, intuitive interface for performing data transformations such as filtering, merging, and pivoting, ensuring that data is in the correct format for analysis. Users can also apply advanced transformations using the M language.
- **Data Modeling:** Power BI Desktop allows users to create complex data models by defining relationships between different tables, creating calculated columns, and adding measures using DAX (Data Analysis Expressions). This robust modeling capability ensures users can analyze data across multiple dimensions and generate meaningful insights.
- **Interactive Visualizations:** Power BI Desktop offers a wide array of visualization options, including charts, graphs, maps, and custom visuals. Users can drag and drop fields to create interactive and dynamic visualizations that help uncover trends, patterns, and insights within the data.
- **Custom Visuals:** In addition to standard visualizations, Power BI Desktop supports custom visuals. Users can import custom visuals from the Microsoft AppSource marketplace or develop their own, providing endless possibilities for data representation.
- **Advanced Analytics:** Power BI Desktop includes advanced analytics features such as forecasting, clustering, and R and Python scripting integration. These features enable users to perform sophisticated data analysis and gain deeper insights from their data.
- **Report Publishing:** Users can publish a report directly from Power BI Desktop to the Power BI Service once a report is designed and finalized. This seamless integration allows for easy sharing and collaboration, enabling stakeholders to access and interact with the reports online.

- **Page Layout and Formatting:** Power BI Desktop provides extensive options for formatting and customizing the layout of reports. Users can adjust fonts, colors, and themes and configure page settings to ensure that reports are visually appealing and professionally presented.
- **Incremental Refresh:** Power BI Desktop supports incremental data refresh, allowing users to update only the data that has changed since the last refresh. This feature improves performance and reduces the time required to refresh large datasets.
- **Performance Analyzer:** The Performance Analyzer tool in Power BI Desktop helps users optimize their reports by identifying performance bottlenecks and providing recommendations for improving report performance.

Overall, Power BI Desktop is an essential tool for data professionals and business analysts. It provides all the necessary features to transform raw data into actionable insights. Its powerful capabilities make it a cornerstone of the Power BI ecosystem, enabling organizations to leverage data for informed decision-making and strategic planning.

Using Power BI Desktop

Once you have Power BI Desktop installed, you can immediately connect, transform, and build visualizations of your data. In Power BI Desktop, there are several key views that users interact with to create, modify, and visualize their data. These views provide different perspectives and functionalities for building reports and dashboards. The main views in Power BI Desktop are:

- **Report View:** This is the primary workspace where users design and arrange visualizations to create interactive reports. Users can drag and drop visuals onto the canvas, adjust their size and position, and customize their appearance and formatting. Report view also allows users to create drill-through interactions, bookmarks, and tooltips to enhance the interactivity of their reports.
- **Data View:** In Data view, users can see the underlying data tables and fields imported into Power BI Desktop. They can view and edit the data, apply data transformations using the Power Query Editor, and create relationships between tables. This view provides a structured look at the data model, allowing users to define calculated columns and measures.
- **Model View:** The Model view offers a graphical representation of the data model created within Power BI Desktop. Users can see the tables, relationships, and measures in their data model and make modifications as needed. This view is essential for creating and managing relationships between tables and maintaining the structure of the data model.
- **DAX Query View:** Introduced in late 2023, the DAX Query View is a powerful feature that allows users to write, edit, and execute DAX queries directly within Power BI. This addition provides a robust environment for managing DAX queries without needing external tools, enhancing the workflow for BI developers and analysts.

Power BI Desktop regularly receives updates to improve functionality and user experience. Recent updates include introducing on-object interaction support for various visual types, enhancements to the mobile reporting experience, and a new home screen that centralizes all Power BI activities within the desktop application. Users can effectively manage their data preparation and visualization tasks by utilizing these views and staying updated with new features, ensuring their reports and dashboards are informative and engaging.

Query Editor

Power BI Desktop comes with the Power Query Editor, a powerful tool originating from Excel's PowerPivot. It allows users to transform, clean, and shape data before loading it into Power BI for analysis and visualization. Key features of the Query Editor include:

- **Data Source Connectivity:** The Query Editor supports connectivity to various data sources, including databases, files (such as Excel, CSV, JSON), web services, and more. Users can import data from multiple sources and combine them into a single dataset for analysis.

- Data Transformation:** Users can perform various data transformation tasks within the Query Editor to clean and shape their data. This includes filtering rows, removing duplicates, sorting, renaming columns, and changing data types. The Query Editor provides a visual interface for these transformations, making it easy to manipulate data.
- Power Query M Language:** Behind the scenes, the Query Editor generates Power Query M language code to execute data transformation steps. Advanced users can view and edit this code directly, allowing for more complex and customized transformations beyond what the visual interface offers.
- Applied Steps:** Each data transformation action performed in the Query Editor is recorded as an "applied step." Users can see a list of applied steps and easily navigate them to understand the sequence of transformations applied to their data. Applied steps also enable users to modify or remove specific transformations as needed.
- Data Profiling:** The Query Editor provides data profiling capabilities to analyze the structure and quality of the imported data. Users can view summary statistics, distribution histograms, and data quality warnings to identify potential issues or anomalies in the data.
- Data Preview:** Users can preview the transformed data in real-time by applying different transformation steps. This allows users to quickly iterate and refine their data preparation process until they achieve the desired result.

In summary, the Power BI Desktop Query Editor empowers you to clean, reshape, and enrich your data flexibly and intuitively, ensuring the data is adequately prepared for analysis and visualization in Power BI reports and dashboards. Although you can create reports directly from the Power BI service, it is best to build in Power BI Desktop first and then publish the report to the Power BI service in an individual or shared workspace (Figure 21-15).

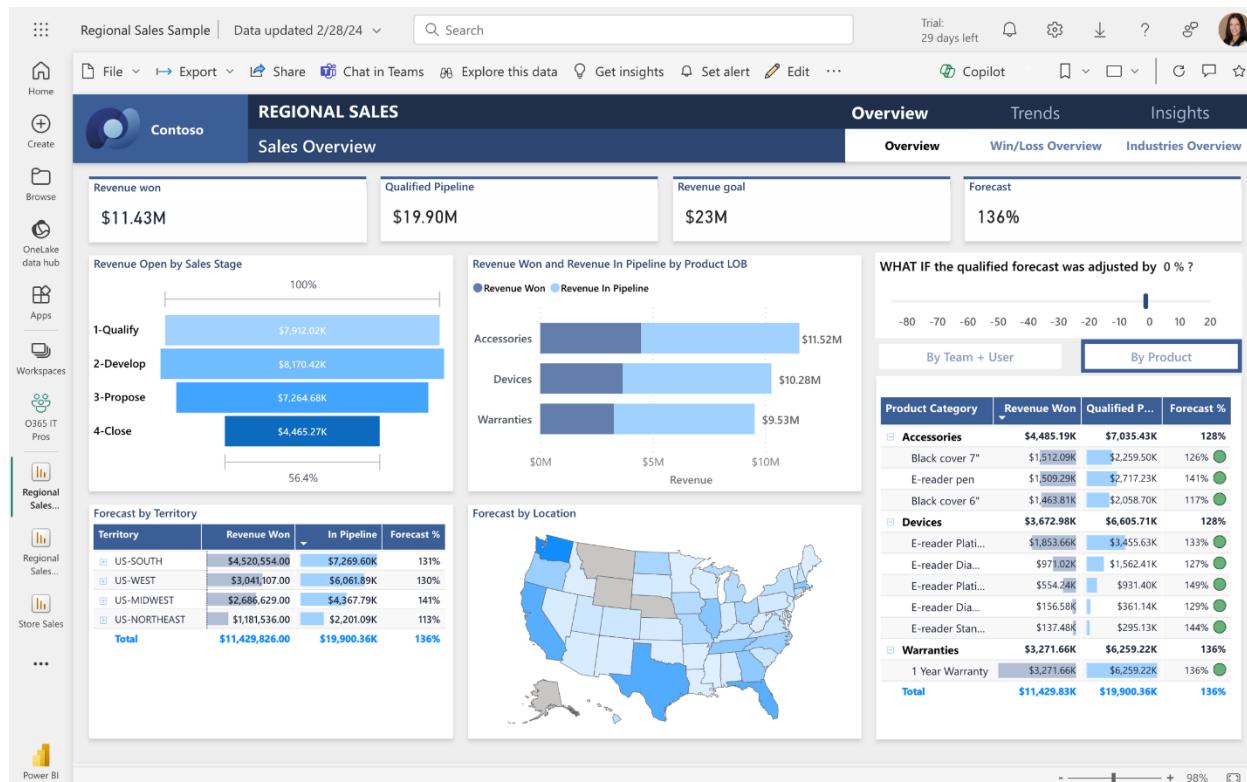


Figure 21-15: Published report displayed in a shared workspace called Office IT Pros

For a getting started guide and tutorials on Power BI Desktop, read [Get started with Power BI Desktop](#) and the [Microsoft Learning path for Power BI](#). To understand the differences between Power BI Desktop and Power BI Service, visit [Comparing Power BI Desktop and the Power BI service](#). To learn more about your sharing and collaboration options in Power BI, visit [Ways to collaborate and share in Power BI](#).

Power BI Desktop OneDrive and SharePoint Integration

Power BI Desktop now integrates with OneDrive and SharePoint. This feature allows you to [connect to files stored in OneDrive for Business or SharePoint Online](#) and get automatic updates when the files change. You can also refresh your datasets in the Power BI service based on the source file changes without republishing them. You can easily access and analyze your Excel, CSV, or Power BI Desktop files from anywhere, using the cloud storage of OneDrive or SharePoint. You can collaborate with others on the same files and see the latest data in Power BI as soon as someone makes a change. You can leverage the security and governance features of OneDrive and SharePoint, such as version history, sharing permissions, and compliance policies.

To use this feature, you need to have a Power BI Pro license, and a OneDrive for Business or SharePoint Online account. You also need to [enable the OneDrive/SharePoint Online refresh option](#) in the dataset settings in the Power BI service.

Dataflows

Power BI Dataflows are a powerful feature that allows you to ingest, transform, integrate, and enrich data from various sources into a centralized, reusable data storage layer. They essentially bring self-service ETL (Extract, Transform, Load) capabilities to Power BI. Key aspects of Power BI Dataflows include:

- **Data Integration:** Dataflows enable users to ingest data from multiple sources, including databases, files, cloud services, and on-premises systems. This integration facilitates the consolidation of diverse datasets within Power BI.
- **Data Transformation:** Like the Power BI Desktop Query Editor, Dataflows provide robust data transformation capabilities. Users can clean, shape, and enrich their data by applying various transformations to standardize it, remove duplicates, perform calculations, and more.
- **Data Enrichment:** Users can further enrich their data by adding calculated columns and aggregations or applying machine learning models directly within Dataflows. This enables deeper insights and prepares the data for advanced analysis.
- **Data Reusability:** Dataflows promote reusability by creating data entities that can be shared and reused across multiple Power BI reports and dashboards. This ensures consistency and reduces redundancy in data preparation efforts.
- **Data Governance:** Power BI Dataflows support organizational data governance by providing features for data lineage, data security, and data refresh scheduling. These capabilities help organizations maintain control over their data assets and ensure compliance with regulatory requirements.
- **Data Refresh:** Dataflows support scheduled data refreshes to keep the data up-to-date with the latest changes from the source systems. Users can define refresh schedules based on their specific requirements to ensure the data remains current for reporting and analysis.
- **Integration with Power BI Desktop:** Data stored in Dataflows can be directly leveraged within Power BI Desktop for building reports and dashboards. This seamless integration streamlines the data preparation and analysis workflow, enabling users to create insightful visualizations efficiently.

Power BI Dataflows empower you to establish a unified and governed data preparation process within the Power BI ecosystem. By centralizing data integration, transformation, and enrichment activities, Dataflows help organizations unlock the full potential of their data assets for analytics and decision-making. To learn more about Power BI dataflows, please visit [Introduction to dataflows and self-service data prep](#).

Using Power Apps and Power Automate with Power BI

Power BI is a read-only tool that allows users to visualize and interact with data. It does not have built-in capabilities to write back data. This has now changed thanks to the integration of Power Apps and Power Automate with Power BI. Using the Power Apps and Power Automate visuals, you can now build Power Apps

and Power Automate solutions to provide users with the ability to write data back to the source from within Power BI.

To learn more, read [Using Power Apps, Power BI, and Power Automate Together](#) and [Power BI data write-back with Power Apps and Power Automate](#).

Power BI Security

Built on Azure, the Power BI Service uses two primary repositories for storing and managing data. Report publishers' data is uploaded to the Power BI Service in Azure Blob Storage, and all metadata and system items are in *Azure SQL Database*.

For more information on the Power BI architecture, read [Power BI Security](#). For more detailed information on Power BI Security, [read the Power BI Security whitepaper](#).

Microsoft Fabric

[Microsoft Fabric](#) is an integrated platform that combines Power BI with various Azure services to offer a comprehensive and unified analytics solution. This innovative platform enables users to seamlessly access, transform, analyze, and visualize data from diverse sources within a single interface. It also incorporates advanced AI features, allowing users to generate insights and reports through natural language queries. The goal of Microsoft Fabric is to streamline and elevate the user experience for all data analytics requirements.

Microsoft Fabric consists of four main layers: the ingestion layer, the storage layer, the compute layer, and the presentation layer. Each layer has its own role and functions, as described below.

- **Ingestion Layer:** The ingestion layer is responsible for receiving data from multiple sources, such as files, databases, web services, or streaming data. This layer leverages Power Query to perform data transformations, validations, and enrichments, ensuring the data is ready for analysis. Additionally, the ingestion layer supports data refresh scheduling and the creation of reusable data pipelines, known as dataflows, which can be shared across different workspaces and datasets.
- **Storage Layer:** The storage layer is designed to store data in various formats and locations depending on the data type and intended use. Azure Data Lake Storage Gen2 is used for large datasets requiring high performance and scalability. This layer also employs Azure Analysis Services for datasets optimized for interactive analysis and Azure SQL Database for other types of data storage, providing a flexible and scalable storage solution.
- **Compute Layer:** The compute layer performs calculations, aggregations, and queries on the stored data. It utilizes Azure Analysis Services to process tabular models supporting complex calculations and measures. Additionally, Azure Synapse Analytics is used to process relational models suitable for simpler calculations and filters. This layer ensures that data processing is efficient and can handle complex analytical tasks.
- **Presentation Layer:** The presentation layer delivers data and reports to Power BI users and applications. Through the Power BI Service, users can access dashboards, reports, and apps that provide data visualizations and insights. This layer also supports embedding Power BI content into custom applications or websites using Power BI Embedded, and it can host and deliver Power BI content securely with Power BI Report Server. This ensures that users can access and interact with data in various ways to meet their needs.

Advanced Features and Capabilities

Microsoft Fabric includes advanced AI-powered features like Copilot, which allows users to generate reports and query data using natural language. This integration helps users quickly create and customize reports with AI assistance, making data analysis more accessible and intuitive. Additionally, Fabric provides comprehensive governance tools, including data lineage, data protection with sensitivity labels, and admin monitoring. These

features help organizations manage compliance and security efficiently, ensuring data is used responsibly and securely.

The platform also supports real-time data ingestion and analytics, enabling users to make timely data-driven decisions. This includes capabilities for handling streaming data and performing real-time analysis, which is crucial for businesses that respond quickly to changing conditions.

Overall, Microsoft Fabric simplifies analytics and data management by integrating various tools and services into a unified platform. This makes it easier for organizations to leverage their data for actionable insights, driving better decision-making and operational efficiency. For more detailed information and updates, you can visit the [Microsoft Fabric Blog](#) and the [Microsoft Learn](#) site.

Latest Power BI Updates and Features

Power BI offers users a range of new features and improvements that make it an even more powerful tool for data visualization and business intelligence. The latest updates focus on improving usability, performance, and functionality, ensuring that users can create and share insightful, interactive reports and dashboards with ease. Below are some of the key enhancements that have been introduced to Power BI:

- **On-Object Interaction Support:** Recent updates include the introduction of on-object interaction support for various visual types. This feature enhances the usability of visualizations by allowing users to interact directly with the objects in their reports, making it easier to modify and adjust visual elements.
- **Mobile Reporting Enhancements:** Enhancements to the mobile reporting experience include improved navigation and interaction capabilities for mobile users. These updates ensure that reports are accessible and user-friendly on mobile devices, providing a better experience for users who need to access data on the go.
- **New Home Screen:** A new home screen in Power BI Desktop centralizes all Power BI activities within the desktop application. This screen provides a streamlined interface where users can easily access their reports, datasets, and workspaces, enhancing the overall user experience.
- **Enhanced Natural Language Query (Q&A):** Power BI's Natural Language Query (Q&A) feature has been enhanced to provide more accurate and relevant results. Users can type questions in natural language, and Power BI will generate visualizations based on the data. The improved Q&A feature includes better understanding of user intents and context, making it easier to explore data and gain insights through conversational queries.
- **Data Connectivity and Preparation:** Power BI has introduced new data connectors and improved data preparation capabilities. These enhancements allow users to connect to a broader range of data sources and prepare their data more effectively for analysis. Improved data preparation features include advanced data transformation options, making it easier to clean and shape data before using it in reports and dashboards.

Licensing Power BI

The licensing options for Power BI include **Power BI (free)**, **Power BI Pro**, **Power BI Premium Capacity-based**, and **Power Premium Per-user (PPU)**. For more information on Power BI pricing, [Power BI pricing](#).

AI Builder for the Power Platform

AI Builder for the Power Platform provides the capability to use AI models to add intelligence to business processes in both Power Apps and Power Automate. AI Builder for Power Automate elevates the realm of automation. It functions as an AI-driven extension, empowering users to harness machine learning for predictive tasks, intricate analyses, form processing, and a wide range of other functions. AI Builder comes

equipped with preconfigured AI models that can be tailored to meet your specific business requirements, or you can create custom models. Some of the key AI capabilities of AI Builder include:

- **Form Processing:** This feature extracts data from forms, invoices, receipts, and other structured documents to automate data entry tasks. It simplifies and accelerates the processing of large volumes of documents.
- **Object Detection:** This capability identifies and locates objects within images, which is useful in applications such as inventory management and quality control. Automating object recognition tasks can significantly streamline operations.
- **Sentiment Analysis:** Analyze text data to determine sentiment, which can be used to assess customer feedback or social media comments. This helps businesses gauge customer satisfaction and identify areas for improvement.
- **Prediction:** Create predictive models based on historical data to forecast future trends and outcomes. This feature enables proactive decision-making by predicting business metrics like sales forecasts and risk assessments.

Integration and Licensing

AI Builder integrates seamlessly with Power Apps and Power Automate, enhancing their capabilities with AI-driven insights. AI Builder credits are included in both Power Apps and Power Automate Premium licenses. For additional capacity, it is available as an add-on license for Power Apps, Power Automate, or Dynamics 365. AI Builder is also available as a 30-day trial, allowing users to explore its capabilities in either a trial or production environment. AI model results are stored in Dataverse, making them easily accessible for use in apps and flows. To learn more, visit the [AI Builder documentation](#).

Advanced Features

AI Builder not only simplifies the integration of AI into Power Apps and Power Automate but also includes advanced features that enhance its usability, security, and functionality. These features are designed to ensure that AI Builder can meet the complex needs of modern businesses while maintaining high standards of governance and user-friendliness. Here are some of the key advanced features:

- **Governance and Security:** AI Builder includes comprehensive governance features, such as capacity management, usage monitoring, and access control, ensuring that AI usage aligns with organizational policies.
- **Generative AI Capabilities:** New features in AI Builder include the ability to build and deploy GPT prompts, enhancing the platform's functionality with the latest generative AI capabilities from Azure's OpenAI service.
- **Copilot Integration:** AI Builder extends Copilot capabilities, making it easier for business users to interact with AI models and extract valuable insights from their data.
- **Advanced Natural Language Processing (NLP):** The natural language processing capabilities of AI Builder have been significantly enhanced. The updated NLP engine provides better understanding and handling of user intents and queries, resulting in more accurate and responsive AI model interactions.
- **Custom AI Models:** Users can now integrate custom AI models into their solutions. This feature allows organizations to leverage their proprietary AI models or third-party models, providing more tailored and sophisticated AI capabilities.
- **Improved Analytics and Reporting:** AI Builder now offers enhanced analytics and reporting tools. These tools provide deeper insights into model performance, user interactions, and overall effectiveness. Administrators can use these insights to continuously refine and improve their AI models.

AI Builder empowers users of all skill levels to create intelligent applications and workflows, driving efficiency and innovation across business processes. For more detailed information, you can explore the official AI Builder documentation on [Microsoft Learn](#).

Power Pages

Power Pages is a versatile platform within the Microsoft Power Platform suite that enables users to create, design, and deploy secure, data-driven websites with minimal coding. It is designed to streamline the web development process, making it accessible to both professional developers and business users. Power Pages integrates seamlessly with other Power Platform tools such as Power Apps, Power Automate, and Power BI, allowing for robust data integration and automation capabilities. This platform empowers organizations to deliver interactive and dynamic web experiences, facilitating better customer engagement and data management. Power Pages is available by visiting <https://powerpages.microsoft.com>.

Design Studio for Power Pages

Power Pages Design Studio is a cloud-based WYSIWYG (what-you-see-is-what-you-get) authoring tool tailored for low-code makers to create and style data-centric business sites backed by Dataverse. Upon signing up for a trial, Power Pages auto-provisions a new environment within your tenant. To start building a site, click on **+ Create a site**.

When creating a new site, you can choose from a variety of templates. After selecting a template, you must provide a site name and web address and optionally change the site language. The web address must be unique; if it isn't, the system will prompt you until a unique address is provided. Click **Done** to proceed with site provisioning, which typically takes around 5 minutes. Once provisioned, the site will appear under My sites, where you can preview or edit it. Clicking **Edit** launches the design studio.

The design studio features four key workspaces:

- **Pages Workspace:** Enables users to [create and design webpages](#) using no-code and low-code widgets like lists, forms, text, images, videos, and more.
- **Styling Workspace:** Allows users to [apply global site styles](#). There are 13 preset themes, each customizable with different color palettes, font styles, background colors, section margins, and button styles.
- **Data Workspace:** Facilitates modeling, visualizing, and managing business data for the site. All data and changes made in the [Data workspace](#) is stored in Dataverse.
- **Set up Workspace:** Lets makers and site administrators [configure site settings](#), such as identity providers for authentication and table permissions.

Additionally, Power Pages can be extended using Visual Studio Code and the Power Platform CLI. You can customize your site by editing CSS, applying custom JavaScript, and modifying page content through Visual Studio Code for the Web. To explore these capabilities more, visit the [Microsoft Power Pages documentation](#).

Power Pages Design Studio now includes advanced features such as Copilot integration, enabling natural language site creation and editing, and a new Security workspace for enhanced site protection and management. These additions make Power Pages a robust tool for creating secure, interactive, and dynamic business websites.

New Features in Power Pages Design Studio

- **Copilot Integration:** Power Pages Design Studio now includes advanced features such as Copilot integration. This enables natural language site creation and editing, simplifying the process of building web pages. Users can describe the type of webpage they need, and Copilot will generate the HTML code, complete with text content and images based on the description. The new page is

seamlessly integrated into the main site navigation and can be further customized and edited using Copilot and the user-friendly WYSIWYG editor. To learn more about the Copilot features for Power Pages, visit [Create an AI-generated webpage using Copilot](#).

- **Security Workspace:** A new Security workspace has been introduced for enhanced site protection and management. This feature allows site administrators to configure and manage security settings, ensuring the site remains secure and compliant with organizational policies.

Licensing Power Pages

The licensing options for Power Pages include **Authenticated users per website**, **Anonymous users per website**, and **Pay-as-you-go** plans. For more information on Power Pages pricing, visit [Power Pages pricing](#).

Copilot Studio

Power Virtual Agents are a part of [Copilot Studio](#). Copilot Studio allows you to develop chatbots with no coding or model training requirements. Built on Azure's Bot Framework Service, Copilot Studio provides a guided, no-code graphical interface for creating and integrating bots with prebuilt Power Platform connectors. Bots can trigger Power Automate workflows to perform tasks on behalf of users, enhancing automation capabilities. Continuous background monitoring and AI-driven insights help improve bot performance over time.

Some examples of use cases for Copilot Studio include:

- **Employee Onboarding and HR Assistance:** Use a virtual agent to streamline the employee onboarding process and provide valuable assistance in HR-related tasks. For example, a human resources department can deploy a virtual agent to guide new hires through the onboarding process, help with filling out digital paperwork, provide information on company culture, and answer questions regarding benefits and vacation policies.
- **Sales and Marketing Assistance:** A virtual sales assistant can improve customer engagement and streamline the sales process. An e-commerce company, for instance, could deploy a virtual agent on its website to interact with visitors, recommend products based on their preferences and purchase history, and provide assistance throughout the sales process, including order tracking and returns.
- **IT Helpdesk and Technical Support:** Implementing a virtual agent for IT support can improve the efficiency of resolving technical issues within an organization. An IT department, for instance, could deploy a virtual agent to assist employees with tasks such as resetting passwords, troubleshooting software problems, configuring email clients, and accessing IT resources.
- **Event Management and Registration Assistance:** Developing a virtual agent for event management purposes can streamline the registration process and provide attendees with valuable information. An event management company could deploy a virtual agent to help attendees register for conferences, provide agendas and speaker information, address inquiries about event logistics, and assist with travel arrangements.

Supported Data Sources, Plugins, and Actions in Copilot Studio

Copilot Studio is highly versatile, supporting a wide range of data sources and integrations to enhance the functionality of your virtual agents. When building a Copilot, you can connect to data sources such as SharePoint, Microsoft Dataverse, SQL Server, and external APIs through custom connectors. These connections allow your virtual agents to interact with and retrieve data in real-time, making them more responsive and context aware.

One of the most powerful features of Copilot Studio is its ability to trigger [Power Automate flows directly from within the bot](#). This integration enables you to automate complex workflows, such as approving requests, sending notifications, or updating records, all initiated by user interactions with the bot. Additionally,

Copilot Studio supports the use of Adaptive Cards to present rich, interactive content within conversations, enhancing user engagement with forms, images, or dynamic content. To learn more about Copilot Studio actions, please visit [Use actions with custom copilots \(preview\)](#).

For advanced capabilities, Copilot Studio can be extended with Azure OpenAI. This integration allows virtual agents to handle complex queries, generate natural language responses, and assist with creative tasks, significantly boosting their conversational intelligence.

With these features and the power of Azure OpenAI, you can build highly functional virtual agents tailored to your organization's needs.

Build a Copilot Studio Bot

To create your bot with Copilot Studio, log in to <https://copilotstudio.microsoft.com> using your Microsoft account. It is recommended that you use a personal development environment instead of the default environment.

Note: Copilot Studio is only supported in [specific data locations](#). If you are outside these locations, you must create a custom environment with the Region set to a supported data location before creating your Copilot.

For this example, you will create a simple Q&A bot that uses the public Power Platform Documentation website as the knowledge source. To continue from the home page, click the **+ Create** icon in the left navigation and then click the **New copilot** tile. This will take you to the conversational builder page, which provides the ability to use the conversational creation experience preview feature, where you can describe the bot you want to create. You can skip this step by clicking the **Skip to configure** button to proceed to the **Configuration** page.

1. In the Details section, set the name to **Power Platform Docs Bot**.
2. Click the **+ Add knowledge** button.
3. Select **Public Website** and add this public link: <https://learn.microsoft.com/en-us/power-platform>
4. Click the final **Add** button to return to the Details and ensure the website link is listed in the Knowledge section.
5. Now click the **Create** button to create your bot, which will default to the Overview page.

The overview page confirms that the bot is ready and offers guidance on what to do next, like adding actions, creating topics, or publishing the bot for others to use. The main section shows the bot's name and the option to add knowledge sources, such as the linked Power Platform documentation website, along with setting an optional description and instructions. On the screen's right side is a "Test your copilot" panel, where you can try out the bot and see how it responds to different questions. In this example, the bot successfully answers a query about the latest updates in the Power Platform, showing that it's pulling information from the provided knowledge source. This page is your central hub for refining your bot and ensuring it's ready to go live.

6. Now test your bot in the Test Copilot pane by asking the bot **What is new in the Power Platform?**

After setting up your bot, it's important to configure Topics and Prompts to ensure your bot effectively handles user queries and guides conversations. Topics are the areas of conversation your bot is prepared to handle. In Copilot Studio, you can create Topics to define how your bot should respond to specific types of queries. For example, you might make a Topic for "New Features" where the bot can provide details on the latest updates in the Power Platform. Topics help keep conversations organized and ensure the bot provides relevant information based on the user's input.

The Topics tab in Copilot Studio includes both custom topics you create and System Topics, which are built-in topics provided by the platform. *Custom Topics* in Copilot Studio are user-defined topics that allow you to tailor the bot's conversation capabilities to your specific needs. Unlike System Topics, which handles general

and essential interactions, Custom Topics lets you create specialized dialogues that address your organization's or project's unique requirements.

When creating a Custom Topic, you start by defining trigger phrases—specific words or phrases that, when detected in the user's input, will activate the topic. Once a Custom Topic is triggered, you can configure how the bot should respond. This might involve providing detailed information, asking follow-up questions, or guiding the user through a process. You can also link these topics to actions, such as pulling data from a database or invoking a workflow via Power Automate. The default Custom Topics include:

- **Greeting:** This is triggered when a user first interacts with the bot. It usually handles the initial greeting, introduces the bot, and offers a list of options to get started.
- **Goodbye:** This handles the end of a conversation, providing a polite and clear way to close the interaction.
- **Fallback:** This is triggered when the bot doesn't understand a user's input. It helps manage those situations by asking the user to rephrase their question or redirecting them to a more appropriate topic.
- **Escalation:** In scenarios where the bot can't assist further, this topic can be used to offer additional help, such as connecting the user with a human agent.

System Topics in Copilot Studio are predefined, essential components that help your bot handle fundamental aspects of conversation. These topics ensure your bot can manage common interactions effectively, providing a consistent user experience. Here's an overview of the default System Topics:

- **Conversation Start:** This topic is triggered at the beginning of any interaction with the bot. It typically manages the initial greeting, sets the tone for the conversation, and may present users with options to guide the conversation from the outset.
- **Conversational Boosting:** This is activated when the bot encounters an unknown intent or needs to generate a response without a direct match for the user's input. This topic helps the bot create more contextually appropriate responses, keeping the conversation flowing smoothly even when unsure of the user intent.
- **End of Conversation:** This topic is used when the conversation is about to conclude. It typically handles the closing of the interaction, providing a polite farewell message and ensuring that the user knows the conversation has ended.
- **Escalate:** Triggered when the bot identifies that it can no longer effectively assist the user, this topic facilitates handing off the conversation to a human agent or another support channel. It's essential for managing more complex queries or situations where automated support is insufficient.
- **Fallback:** This topic is triggered when the bot doesn't understand the user's input. It acts as a safety net, prompting the user to rephrase their question or offering suggestions to help guide the conversation back on track.
- **Multiple Topics Matched:** Activated when the bot detects that the user's input could match several different topics, this topic prompts the bot to clarify the user's intent. This ensures the conversation remains focused and relevant to the user's needs.
- **On Error:** Triggered when there's an error in the bot's operations, such as a technical issue or a failure to process a request. This topic manages user expectations by informing them of the error and, when possible, provides steps to resolve the issue or try again.
- **Reset Conversation:** This topic is used when the conversation needs to be restarted, either by the user or the bot. It clears any confusion by effectively resetting the interaction, allowing the conversation to start afresh.
- **Sign In:** This topic handles user authentication, ensuring that users are properly signed in before accessing specific features or personalized information. It maintains security and enables the bot to provide tailored responses based on the user's credentials.

Now let's proceed with changing the starter prompt message.

1. Ensure you are in the **Topics** tab, then select **System** and click on **Conversation Start**.
2. Notice that this topic has a *Trigger* and a *Send a Message* action. To update the action message, place your cursor inside the **Send a Message** action and replace the existing text with your desired wording. For example, you could use: *Welcome to the Power Platform Docs Bot! How can I assist you today?*
3. Click the **Save** button to save your changes. If the Save button is disabled, click on the white area outside of the Send a Message action to enable the button.
4. To test, click on the restart conversation icon and notice your bot now prompts with your updated verbiage as highlighted in 245.

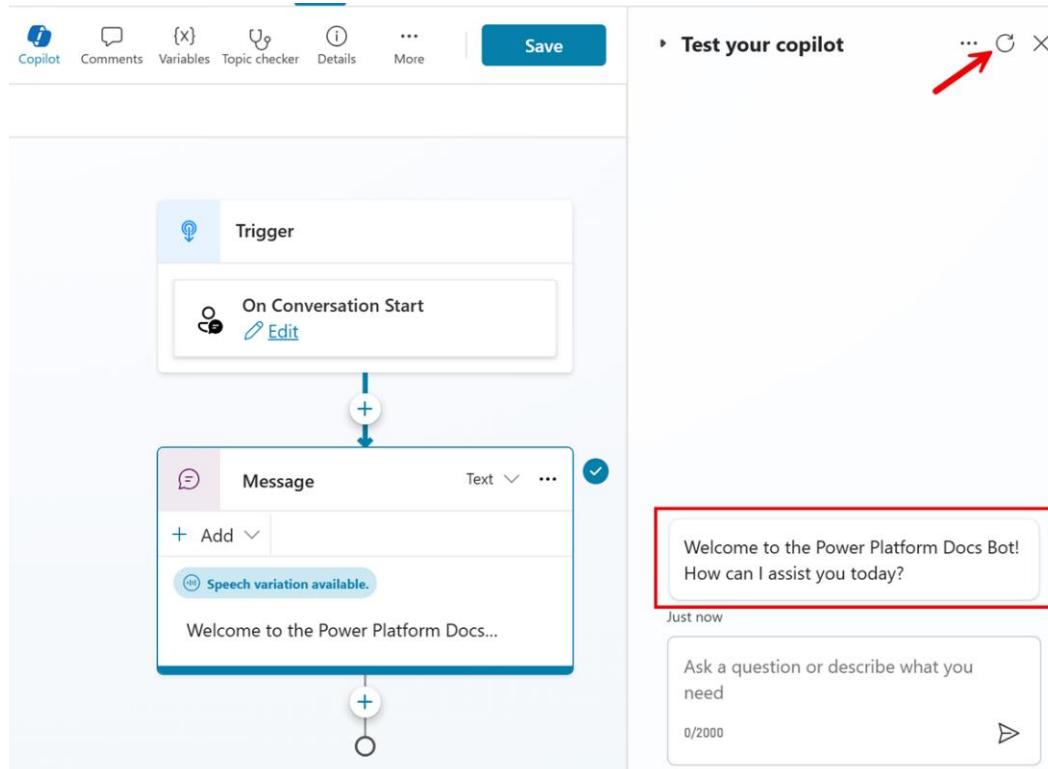


Figure 21-245: Restarting the conversation to test the updated Conversation Start prompt message

Now ask your bot some questions about the Power Platform to test the results you get.

Copilot Studio Security Authentication

When you're ready to deploy a bot you've built in Copilot Studio, you can set up authentication requirements that align with your organization's security standards. Security authentication in Copilot Studio is key to making sure only the right people can access and interact with your bots. It's all about protecting sensitive data and keeping your bot interactions secure and trustworthy.

To access the authentication settings for your bot, go to Settings > Security > Authentication. You'll see three options to configure: No authentication, Authenticate with Microsoft, and Authenticate manually. Since the bot you just created uses a public-facing website as the knowledge source, set your bot's authentication to No authentication and click the **Save** button.

You also can configure your bot to respond using Generative AI. To update the settings, follow the steps below:

1. Click on Generative AI in the left navigation of the Settings page.
2. If the How should your copilot interact with people? setting is set to Classic, change it to Generative.

3. Notice that How strict should the content moderation be? is set to High by default. You can leave this setting as is, but for public-facing websites, you might want to lower the moderation to Medium for more balanced results. You can change this setting anytime.
4. Click Save.
5. To exit the settings page, click the X located to the right of the Settings header.

For more information on user authentication in Copilot Studio, visit [Configure user authentication - Microsoft Copilot Studio](#).

Publish your Copilot Studio bot and Test a Channel

The next step is to publish your bot and configure it for the desired channel.

1. To publish your bot, click the **Publish** button.
2. Next, click on the **Channels** tab and select the channel you want to test.

For more information on publishing and deploying your bot through channels, visit [Key concepts - Publish and deploy your copilot](#).

New Features and Enhancements in Copilot Studio

Copilot Studio continues to evolve, offering a range of new features and enhancements designed to improve the chatbot development experience and expand its capabilities. These updates ensure that Copilot Studio remains a powerful and versatile tool for creating intelligent, responsive, and secure chatbots. To learn more about the latest features and release plan, please visit [New and planned features for Microsoft Copilot Studio, 2024 release wave 1](#).

Licensing Copilot Studio

To create and manage bots with Copilot Studio, you will need to be licensed. For more information on Copilot Studio pricing, [Copilot Studio Pricing](#). Copilot Studio capacity is pooled at the tenant level. To learn more, visit [Quotas, limits, and configuration values for Copilot Studio](#).

Teams and the Power Platform

Many organizations worldwide use Microsoft Teams as their central hub for corporate collaboration. The integration of the Power Platform into Teams has enhanced its capabilities. This integration allows users to embed canvas or model-driven apps as tabs within a team or as personal apps, providing easy access to essential tools and data. Users can also create Power Apps directly in Teams, backed by Dataverse for Teams, simplifying app development and deployment. Power Automate flows can also be created within Teams, streamlining workflows and automating processes. The Power Platform and Teams synergy creates a more integrated and efficient digital workplace.

To embed a Power App as a tab in Teams, you click on the + in a team next to the tabs in the channel of the team you want to add it to. Choose Power Apps, then select the Power App you want to embed as a tab in a team. For this example, an app called Salesforce Demo is selected to be added as a tab in a team channel. The Salesforce Demo app appears as a tab in a channel (Figure 21-246). This example app was created outside Teams using Power Apps Studio as a canvas app and with SharePoint lists as the backend data. You can add any canvas app or model-driven app in Teams, or you can create new Power Apps directly inside Teams using the Power Apps Teams app.

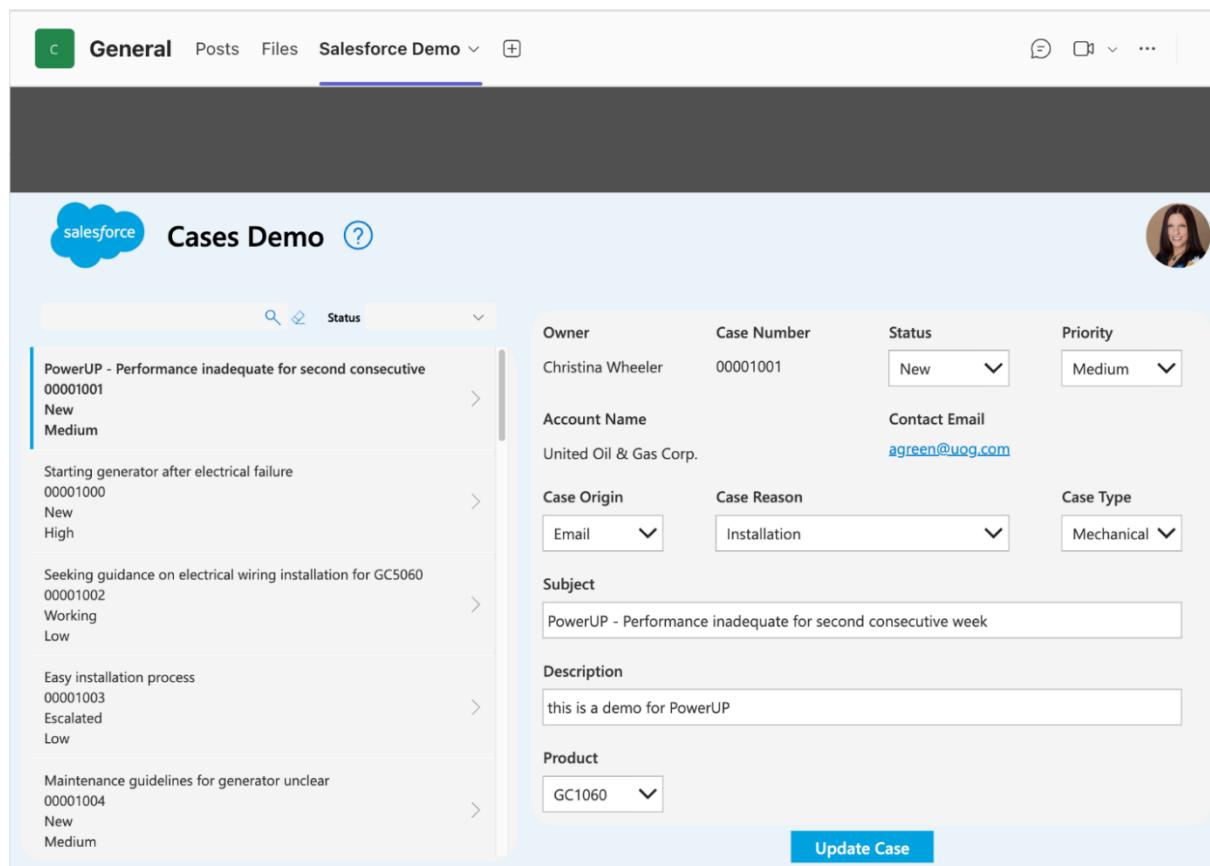


Figure 21-246: Power App embedded as a tab in a team example

For more details on using Power Automate and to see an example of the Request a team Power Platform app template, see the article [Teams + Power Automate: Practical Examples to Automate Tasks](#).

Dataverse for Teams

When you create a Power App directly in Teams, the backend used is Dataverse. Introduced in September 2020, Dataverse for Teams allows you to build custom apps, bots and flows within Teams using Power Apps, Power Automate, and Power Virtual Agents. The Dataverse for Teams environment is automatically created when you create a bot or app in Teams or install the Power Apps app in Teams for the first time. Each team gets one Dataverse for Teams environment and the capacity is measured with relational, file, and image data. Table 21-56 shows the differences between Dataverse for Teams and Dataverse and Table 21-57 shows Dataverse for Teams service limitations.

Environment lifecycle	Dataverse for Teams	Dataverse
Environments	1 per Team	Unlimited
Maximum size	1 million rows or 2 GB	4 TB or more
Upgrade to Dataverse	Yes	N/A

Table 21-56: Environment lifecycle differences between Dataverse for Teams & Dataverse

Unit	Service limit
Dataverse for Teams environments	5 environments + 1 additional environment for every 20 eligible Microsoft 365 user licenses.
Max storage per tenant (Dataverse for Teams environments)	10 GB + Dataverse for Teams environments × 2 GB (up to a maximum of 19.5 TB). The 2 GB storage limit can't be extended. If more storage is needed, you can upgrade the environments to Dataverse.

Table 21-57: Environment lifecycle differences between Dataverse for Teams & Dataverse

Data Storage Comparison

Now that you understand the Power Platform, let's review some of the storage options that are natively integrated within it. SharePoint lists are popular as they are simple to create and share. They are perfect for single-table data models with lower volumes. However, what if you want your application to be scalable. This is where Dataverse is a good fit. While SharePoint lists are great, SharePoint is not a true relationship database, and the only way to create relationships between lists is by using lookup columns (see Table 21-58 for relationship capabilities comparison).

SharePoint Lists	Dataverse for Teams	Dataverse
SharePoint lists are limited to 12 lookups per list. Lookups include one-to-one or one-to-many lookups. There are limited query operations supported by XML-based CAML queries.	Dataverse for Teams supports one-to-many and many-to-many relationships. There's no support for advanced data types (customer, multiple transaction currencies) and no support for non-relational storage logs.	Dataverse supports one-to-many and many-to-many relationships. It supports simple to complex relationships, including polymorphic relations. Powerful query operations using T-SQL statements or FetchXML. Dataverse implements a Common Data Model.

Table 21-58: Data model comparison between SharePoint lists, Dataverse for Teams, and Dataverse

Chapter 22: Prepare Microsoft 365 Business for Copilot

Author: [Ivan Fioravanti](#), CoreView CTO and cofounder

Your step-by-step guide to adopting Microsoft 365 Copilot with confidence

Since its release in November 2023, organizations have responded to Microsoft 365 Copilot with a mix of anticipation and trepidation.

On one hand, Microsoft's research indicates that Copilot adoption could mean a revolution in user productivity. According to their research, 70% of Copilot users were more productive with 68% reporting it also improved the quality of their work.

However, many Microsoft 365 customers are concerned about Copilot's level of access to sensitive files. Organizations that previously relied on 'security by obscurity' now need to rethink their approach.

Microsoft 365 is already a hub of security risks. Fast-paced collaboration means organizations are sharing documents, creating new collaboration spaces, and sharing sensitive information via Teams, OneDrive and SharePoint faster than IT teams can reasonably control. This leads to many challenges, many of which were highlighted in Gartner's recent study titled "[The Top 10 "Gotchas" of Microsoft 365 Copilot](#)":

- Risky configuration settings enabled by default
- Reporting tools lack granularity
- Confusing options from Copilot for extending licenses and managing costs
- Increased risks of oversharing
- Introduction of new attack surfaces to monitor and protect
- No ability to prioritize content sources
- Increased content and app sprawl
- New retention and compliance challenges
- Inconsistent capabilities across applications and languages
- Higher than expected change management effort

These challenges are a major headache for security and governance teams on any day of the week. Now, with Copilot adoption firmly on the agenda for Microsoft 365 teams, excessive and sensitive sharing must be identified fast, new governance processes must be put in place, and risky settings must be reconfigured post-haste to ensure users collaborate safely and securely.

Did you know? According to AIIM, [58% of sensitive cloud data lives in Teams](#) and Office 365 documents, making security and governance of Microsoft a #1 priority for CIOs and CISOs.

Adopt Microsoft Copilot with Confidence

The key to successful Copilot adoption is to ensure that your underlying Microsoft 365 infrastructure is properly governed. But where do you even start?

Your first priority is to make sure that only appropriate users can access the objects and spaces they need to do their job. But it doesn't stop there. Default configurations that introduce new security risks will need to be rebuilt from scratch. You'll also need to set up a thorough approval process to ensure that new users are granted access to sensitive data on an as-needed basis only. Plus, the entire organization will need to be re-educated on best practices for sharing and managing data without introducing security risks.

In this whitepaper, we'll provide you with a step-by-step guide on resolving common Copilot challenges for Microsoft 365. We'll show you how CoreView's suite of [end-to-end Microsoft 365 governance](#), security, and administration tools can help you address each of these challenges.

CoreView's unique 7-step approach

Microsoft 365 is a foundational tool for enterprise collaboration and productivity. Copilot is a game changer for Microsoft 365 users. But it's impossible to adopt new innovations when you spend all your time dealing with routine management and juggling dozens of different interfaces just to keep your tenant safe and secure.

AI like Copilot isn't creating new vulnerabilities and efficiencies. It's highlighting the problems that are already there. Wherever you are on your AI journey, CoreView can help you find and fix configuration problems, automate management, and streamline how you work.

Our approach is built around seven key steps:

1. **Implement and enforce multi-factor authentication (MFA):** MFA isn't a luxury, it's a necessity. It adds a critical layer of defense, ensuring that compromised credentials alone can't grant access to your systems.
2. **Regularly review and update access permissions:** Roles and responsibilities evolve, and access permissions should do the same. Conduct periodic audits to ensure that only the right people have the right access at the right time.
3. **Eliminate legacy accounts and reduce attack surfaces:** Old, unused accounts are open invitations to cybercriminals. Identify and decommission such accounts to minimize vulnerabilities.
4. **Educate and empower your workforce:** Humans are your first line of defense. Regular training on cybersecurity best practices can transform your workforce from a potential liability into a formidable barrier against threats.
5. **Leverage advanced threat protection tools:** Use sophisticated tools that offer real-time threat detection, automated alerts, and actionable insights to stay ahead of potential threats.
6. **Embrace a zero-trust security model:** Adopt a 'never trust, always verify' stance. Zero trust embeds identity verification for anyone trying to access resources in your network, regardless of where they're accessing from.
7. **Ensure compliance through continuous monitoring:** Regulatory landscapes are dynamic. Implement continuous monitoring mechanisms to ensure ongoing compliance and swiftly adapt to new regulations.

At CoreView, we ensure that best practices are more than just understood — they're effectively implemented, uniformly applied across all Microsoft applications, continuously monitored, and highly automated. For IT teams tasked with managing Microsoft 365, it's more than a solution — it's a strategic advantage that frees your time to adopt new technology ahead of your competitors.

10 unique Copilot challenges (+ solutions)

Based on Gartner's 2024 report, there are 10 key challenges to adopting Copilot for your organization. They include everything from risky configurations to oversharing risks to poor license optimization.

CoreView can help you mitigate these issues with [powerful automation tools](#) that simplify the way you perform common security and compliance tasks. It can also provide more in-depth reports, offer recommendations to reduce licensing costs, and much more. Here's a look at how the platform addresses these common challenges with Microsoft Copilot.

Risky configuration settings enabled by default

One of the key challenges when adopting Microsoft 365 Copilot is that many of the default configuration settings can introduce security risks if not properly managed. Out of the box, Copilot may have access to sensitive data and systems without appropriate safeguards in place.

For example, Copilot could be enabled by default for all users, allowing it to access a wide range of company information across Microsoft 365 apps like Outlook, Teams, and SharePoint. If data governance policies and access controls aren't established upfront, there is a risk of Copilot surfacing private data inappropriately or enabling data leaks.

Additionally, default Copilot settings may allow it to interact with external plugins and access web content when generating responses. Without proper vetting and restrictions, this could introduce new attack surfaces and allow Copilot to pull in data from untrusted external sources.

CoreView's Configuration Manager, Simeon Cloud, provides [Security Baselines for Microsoft 365](#) to help mitigate these risks by providing a predefined set of best practice configurations for Microsoft and Copilot. Rather than relying on the default settings, administrators can use CoreView to deploy a curated Microsoft 365 baseline that applies appropriate access controls, data governance policies, and security hardening from day one.

When installing a new tenant, simply activate the "Use Simeon Baseline" toggle in CoreView's Simeon Cloud dashboard (Figure 22-1). This ensures that as your organization rolls out Copilot, it is set up according to industry best practices and aligned to common security and compliance requirements. These Baselines provide an automated way to enforce secure configurations across the Microsoft 365 environment to reduce risk as Copilot is adopted.

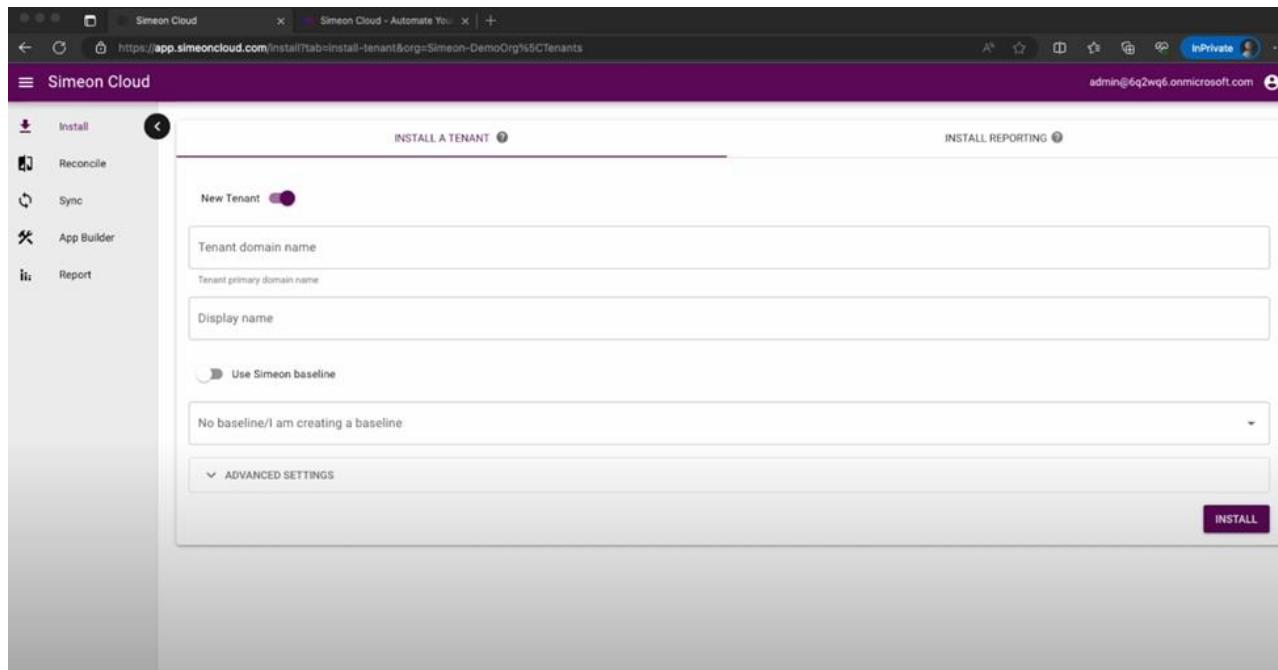


Figure 22-1: Coreview's Configuration Manager, Simeon Cloud

Reporting tools lack granularity

Another challenge organizations face when adopting Microsoft 365 Copilot is the lack of granularity in native reporting tools. Out of the box, Microsoft 365 provides high-level usage and adoption metrics, but these reports often lack the detail needed to effectively govern Copilot usage and mitigate risks.

Microsoft 365 reports can show overall Copilot usage across the tenant, but they may not provide insights into which specific users or departments are most leveraging Copilot. This makes it difficult for IT to identify potential areas of concern, such as users accessing sensitive data or generating content that doesn't align with corporate policies through Copilot.

Also, Microsoft 365 reports typically don't allow administrators to drill down into the specifics of how Copilot is being used. They may show that a user interacted with Copilot, but not what queries were made, what type of content was generated, or how that content was then shared or utilized. Without detailed reporting and [analytics around Copilot usage](#), you lack visibility into potential security, compliance, and productivity risks.

CoreView addresses these reporting limitations through advanced governance capabilities that provide deep visibility into Copilot usage. CoreView's reporting tools enable you to slice and dice Copilot analytics across multiple dimensions, such as user, department, location, device, and more.

For example, CoreView's Copilot Usage report (Figure 22-2) provides detailed information on how employees use Copilot licenses across different platforms on Microsoft 365. Similarly, the Copilot Eligible Users report (Figure 22-3) highlights users who should be given a Copilot license based on their 30-day activity stream.

With CoreView's governance features, IT teams can implement granular permissions and access controls around Copilot. Specify which users or groups have access to Copilot, and even apply feature-level permissions to restrict access to sensitive capabilities. As your organization rolls out Copilot, you can proactively mitigate risks by ensuring only authorized users can leverage the tool to access and generate corporate data.

Licenses	User principal name	Full name	Copilot last action	Recipient type details	Company
Microsoft 365 E5 Microsoft Stream Microsoft Power Automate Free	admin@cvlabmultiforest.onmicrosoft.com	Admin	Never used	UserMailbox	Coreview
Office 365 E3	Christiano.lorimanyuk@cvlabmultiforest.com	Romanyuk	Never used	UserMailbox	
Exchange Online (Plan 2) Microsoft Stream	jlinkoperator2@cvlabmultiforest.onmicrosoft.com	jlink operator 2	Never used	UserMailbox	
Microsoft 365 E5	luig@3112@cvlabmultiforest.com	luig@3112	Never used	SharedMailbox	CoreView
Office 365 E3	Romano.jfranc@cvlabmultiforest.com	JFranc	Never used	UserMailbox	
Office 365 E3	Romanoa.liliana@cvlabmultiforest.com	Liliana	Never used	UserMailbox	

Figure 22-2: CoreView's Copilot Usage report

The screenshot shows a CoreView report titled "Copilot eligible users". The interface includes a sidebar with "ENTRA ID APPLICATIONS" sections for "Service principals..." and "Application permis...". The main area displays a table with columns: "User principal name", "Teams total actions 30", "Exchange total actions 30", and "SharePoint total actions 30". The table lists 142 users, each with a checkbox, a pencil icon, and a copy icon. The first few rows show user names like "elisabetta@contoso.com" and "johndoe@contoso.com" with their respective action counts.

User principal name	Teams total actions 30	Exchange total actions 30	SharePoint total actions 30
elisabetta@contoso.com	504	343	3
johndoe@contoso.com	1312	106	2
janedoe@contoso.com	3311	1585	36
stevedoe@contoso.com	761	94	2
michelle@contoso.com	1811	809	20
anne@contoso.com	670	747	5
mark@contoso.com	2447	7132	55
linda@contoso.com	2448	1404	33
richard@contoso.com	1097	3453	101
charles@contoso.com	981	692	15

Figure 22-3: CoreView's Copilot Eligible Users report

Confusing options from Copilot for extending licenses and managing costs

As organizations adopt Microsoft 365 Copilot, they may face challenges around understanding the various licensing options and managing those costs effectively. Microsoft offers multiple paths for extending Copilot capabilities, but the range of choices can be confusing, leading to suboptimal decisions.

The screenshot shows a CoreView report titled "Active users". The interface includes a sidebar with "Custom reports" and other icons. The main area displays a table with columns: "User principal name", "Copilot last action", "Copilot inactive SKUs", "Copilot plan", and "Account type". A green box highlights the "Copilot last action" column, which shows "Never used" for all listed users. The table lists 3142 users, each with a checkbox, a pencil icon, and a copy icon. The first few rows show user names like "elisabetta@contoso.com" and "johndoe@contoso.com" with their respective account types.

User principal name	Copilot last action	Copilot inactive SKUs	Copilot plan	Account type
elisabetta@contoso.com	Never used			ONCLOUD
johndoe@contoso.com	Never used			ONCLOUD
janedoe@contoso.com	Never used			SYNCHRONIZED
stevedoe@contoso.com	Never used			ONCLOUD
michelle@contoso.com	Never used			ONCLOUD
anne@contoso.com	Never used			SYNCHRONIZED
mark@contoso.com	Never used			ONCLOUD

Figure 22-4: CoreView's License Optimization Report

For example, Copilot requires an add-on license on top of eligible Microsoft 365 plans like E3, E5, Business Premium, and more. However, the specific Copilot features available can vary based on the underlying Microsoft 365 license. This makes it difficult for IT to determine which combination of licenses will deliver the right Copilot capabilities for their users' needs.

With a per-user monthly cost of \$30, Copilot licensing can quickly become expensive if not governed properly. IT teams need to carefully assess which users will benefit most from Copilot and avoid the temptation to simply roll it out broadly.

There are also multiple ways to extend Copilot, such as using plugins, Microsoft Graph connectors, or Power Platform connectors. Each path comes with its own licensing implications and capacity limits that IT must navigate. Without clear guidance and insights, organizations risk making licensing missteps that drive up costs unnecessarily.

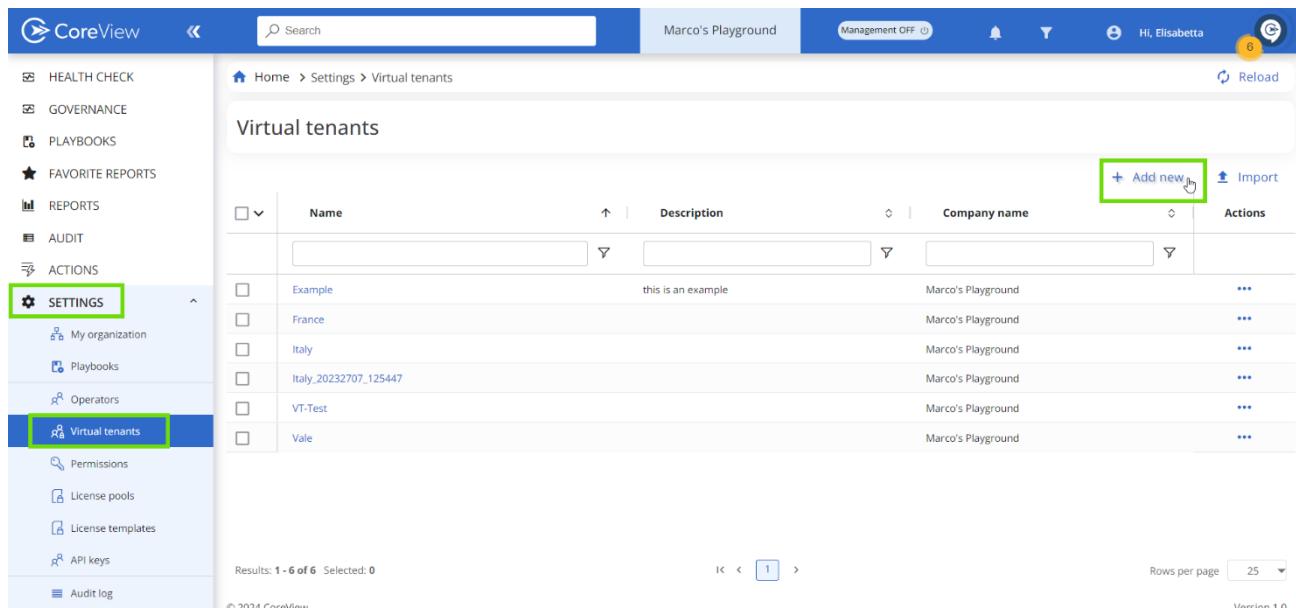
Address these Copilot licensing challenges head on with [CoreView's actionable licensing insights](#). The new Copilot actions featured in CoreView's License Optimization Center (Figure 22-4) enables IT to know how frequently each user interacts with Copilot.

This allows organizations to reclaim licenses from users who aren't getting value from Copilot and reallocate them to those who will benefit more. By proactively managing license assignments based on actual usage insights from CoreView, organizations can control Copilot licensing costs and maximize the return on their investment.

Increased risks of oversharing

[Reports show](#) that on average, 13% of an organization's critical data is overshared, equating to over 598,000 files at risk. While it doesn't itself change data access permissions, Copilot can inadvertently expose existing security gaps, making it easier for users to discover and share information they shouldn't have access to. That's why proper data governance is essential for organizations to realize the full potential of Copilot while protecting sensitive information.

If a user has been granted excessive permissions to confidential files, Copilot's powerful natural language search capabilities could allow them to easily surface and share that sensitive data. Copilot essentially digitizes all the information a user has access to, making it searchable and shareable with simple queries.



The screenshot shows the CoreView interface for managing virtual tenants. The left sidebar has a 'SETTINGS' section with several options: My organization, Playbooks, Operators, Virtual tenants (which is highlighted with a green box), Permissions, License pools, License templates, API keys, and Audit log. The main content area is titled 'Virtual tenants' and displays a table with columns: Name, Description, Company name, and Actions. There are 6 rows listed, each with a checkbox and three dots. At the top right of the table, there are 'Add new' and 'Import' buttons, with 'Add new' being highlighted with a green box. The bottom of the screen shows pagination (Results: 1 - 6 of 6 Selected: 0), row count (Rows per page: 25), and a copyright notice (© 2024 CoreView). The top bar includes a search bar, user info (Marco's Playground, Hi, Elisabetta), and a notification icon (8).

	Name	Description	Company name	Actions
<input type="checkbox"/>	Example	this is an example	Marco's Playground	...
<input type="checkbox"/>	France		Marco's Playground	...
<input type="checkbox"/>	Italy		Marco's Playground	...
<input type="checkbox"/>	Italy_20232707_125447		Marco's Playground	...
<input type="checkbox"/>	VT-Test		Marco's Playground	...
<input type="checkbox"/>	Vale		Marco's Playground	...

Figure 22-5: CoreView's Virtual Tenants™

As users leverage Copilot to generate documents, presentations, and other content, there is also a risk that sensitive data could be included without appropriate labeling or access restrictions. This could lead to confidential information being stored in unprotected locations or shared too broadly.

CoreView addresses these challenges through advanced capabilities that allow granular control over permissions and access policies. For instance, CoreView's Virtual Tenants™ (Figure 22-5) allow administrators to segment visibility and control based on attributes like department or location. This ensures that even if a user has Copilot access, they are only able to surface information from the appropriate data sources based on their virtual tenant restrictions.

With CoreView, access deep analytics and reporting to identify potential oversharing risks. Administrators can easily see which users have access to sensitive data through Copilot, track usage patterns, and detect anomalous behavior that may indicate improper data access.

CoreView's no-code workflow builder (Figure 22-6) allows IT to automatically take corrective actions when oversharing is detected, such as revoking permissions or triggering additional approval processes. Real-time alerts notify administrators of high-risk Copilot interactions so they can swiftly investigate and remediate leaks.

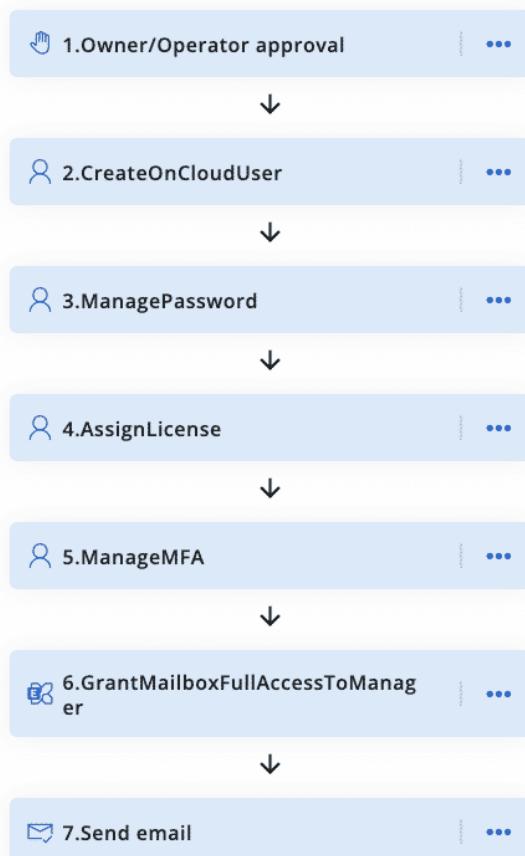


Figure 22-6: CoreView's Workflow Builder

Introduction of new attack surfaces to monitor and protect

As a generative AI system, Copilot has broad access to data across Microsoft 365 applications, along with the ability to generate new content based on that data. The expanded access creates additional security risks that must be managed.

Copilot essentially inherits the access rights of the user interacting with it. If a user has permissions to view sensitive data in SharePoint, Teams, or other Microsoft 365 apps, Copilot will be able to access that same data to generate responses. This means that if a user's account is compromised, an attacker could potentially leverage Copilot to extract confidential information via carefully crafted prompts.

Copilot's natural language interface also opens up new social engineering risks. Attackers may attempt to trick users into entering malicious prompts that cause Copilot to reveal sensitive data or generate harmful content. Since Copilot can access data across Microsoft 365, a single compromised prompt could expose information from multiple sources.

Figure 22-7: CoreView's Copilot Management Playbook

The AI models powering Copilot present another potential attack surface. Techniques like model inversion attacks could allow malicious actors to manipulate Copilot's behavior or extract information from the underlying models. As Copilot integrates with various Microsoft 365 services, any vulnerabilities in those integrations could also be exploited.

CoreView helps organizations address these challenges through integration with leading SIEM solutions. By feeding Copilot usage data into SIEM tools through the Data Connector, CoreView enables security teams to detect unusual Copilot activity, such as attempts to extract sensitive data through targeted prompts. This allows swift response to potential threats.

Additionally, CoreView provides an out-of-the-box Copilot Management Playbook (Figure 22-7) that centralizes Copilot-related access policies and controls. This automated workflow simplifies the task of enforcing a secure Copilot deployment by ensuring that permissions are properly scoped and suspicious activities trigger alerts.

No ability to prioritize content sources

As organizations adopt Copilot, they may face challenges around effectively prioritizing the various Microsoft 365 content sources that Copilot can access and utilize. Out of the box, Copilot has the ability to surface information from a wide range of Microsoft 365 data, including emails, documents, presentations, and more. However, not all content sources are equally relevant or valuable for every user or use case.

Without the ability to prioritize content sources, Copilot may struggle to surface the most pertinent information for a given query. It could pull in data from less relevant sources, potentially leading to suboptimal or even misleading responses.

To drive effective Copilot adoption, IT teams need more granular control over content source prioritization. You require the ability to specify which data sources are most relevant for different user groups or business scenarios. CoreView's dedicated [security and compliance audits](#) can help you decide which content libraries

and data repositories should be indexed and made available to Copilot based on relevance and security considerations.

For example, administrators can choose to prioritize certain SharePoint sites or OneDrive folders that contain the most up-to-date and authoritative information for a given department or project. This ensures that when users prompt Copilot, it is drawing from the most relevant and reliable data sources to generate insights for that specific user.

With CoreView, IT can deprioritize or exclude content sources that contain sensitive information, such as legal documents or financial data. By keeping these sources out of Copilot's reach, organizations can mitigate the risk of inadvertent data exposure and maintain tight control over information access.

Increased content and app sprawl

As organizations adopt Microsoft 365 Copilot, they face an increased risk of content and app sprawl across their environment. Copilot makes it easier than ever for users to generate new content, from documents and presentations to emails and chat messages. While this boost in productivity is valuable, it can also lead to a proliferation of unmanaged and duplicative data if proper governance isn't in place.

Users may struggle to find the information they need among a sea of duplicative and poorly organized content. IT may lack visibility into all the apps being used, making it difficult to govern data access and ensure security. And the organization as a whole may face increased storage costs and compliance risks.

To address these challenges, CoreView provides powerful tools for governing content and apps in Microsoft 365 (Figure 22-8). The platform's real-time health checks proactively identify sprawl risks, such as inactive Teams or OneDrive accounts with large amounts of data. This gives IT visibility into potential problem areas before they get out of control.

CoreView also provides automated playbooks that help enforce governance policies at scale. With CoreView, IT can automatically detect when a new Team is created and ensure it adheres to naming conventions. It can also apply retention labels and sensitivity labels to Copilot-generated content based on predefined rules. These playbooks help ensure that data is properly classified and managed throughout its lifecycle.

The screenshot shows the CoreView Governance Center. At the top, there are navigation links for Home, Governance, and Governance center. Below that, a sub-navigation bar includes Overview, Security & identity management (which is selected and highlighted in green), License management, and SharePoint & OneDrive management. On the left, a sidebar titled 'Filter assistant' contains a 'Status' section with checkboxes for 'Enable policy: ON' (checked), 'Enable remediation: ON' (checked), 'Enable remediation: OFF' (unchecked), 'Set as public: ON' (checked), 'Set as public: OFF' (checked), and 'Enable policy: OFF' (unchecked). The main area displays four audit findings in cards:

- Admin on cloud without strong password** (CoreView policy)
0 Matched items | Remediation is scheduled
- Admin with password not changed in the last 90 days** (CoreView policy)
0 Matched items | Remediation is scheduled
- Admin without MFA** (CoreView policy)
7 Matched items | 2 Exceptions | Remediation is scheduled
- External user in Microsoft 365 group** (CoreView policy)
0 Matched items

At the bottom left, it says "© 2024 CoreView." and at the bottom right, "Version 1.0".

Figure 22-8: CoreView's Governance Center

In addition, CoreView provides detailed insights into which apps are being used across the environment, including any third-party services connected to Copilot. IT can easily see usage metrics, data access

permissions, and other key details to assess risk and compliance. Once again, playbooks make it simple to revoke access or adjust permissions as needed to maintain a secure and streamlined app ecosystem.

New retention and compliance challenges

As users interact with Copilot to generate content and surface insights from across Microsoft 365, it becomes critical to properly retain and manage this data for legal, regulatory, and business requirements. However, the dynamic and conversational nature of Copilot interactions can make traditional Microsoft 365 compliance approaches difficult to apply.

With CoreView, organizations can address these retention and compliance challenges with a comprehensive set of governance tools specifically designed for Microsoft 365 and Copilot. The platform provides granular authentication and access controls to ensure only authorized users can interact with Copilot, so that generated content remains properly secured.

[CoreView's automated playbooks](#) enable organizations to enforce consistent retention policies for Copilot data. Administrators can define rules to automatically apply retention labels to Copilot-generated content based on criteria like sensitivity, user attributes, or business context. This ensures that data is retained for the appropriate duration and can be efficiently discovered when needed.

Real-time security alerts from CoreView notify administrators of potential compliance risks, such as sensitive data being shared via Copilot. Proactive monitoring allows organizations to swiftly investigate and remediate issues before they result in regulatory violations or data breaches.

CoreView also simplifies eDiscovery by providing a centralized interface to search and retrieve Copilot data. Administrators can quickly locate relevant Copilot prompts and generated content, then export this data in a compliant format. Our auditing capabilities maintain a detailed record of all Copilot interactions for forensic analysis and reporting.

Inconsistent capabilities across applications and languages

As organizations adopt Microsoft 365 Copilot, they may encounter inconsistencies in the AI assistant's capabilities across different Microsoft applications and languages. While Copilot is designed to work seamlessly within the Microsoft 365 suite, the depth and breadth of its functionality can vary depending on the specific app and the user's language settings.

Copilot may offer more advanced features and better performance in widely-used apps like Word and Outlook, compared to less popular tools like Visio or Viva Engage. This can lead to a fragmented user experience, where employees have to adjust their expectations and workflows based on the app they are using with Copilot.

Language inconsistencies can also hinder Copilot adoption, particularly for global organizations with a presence across multiple regions. These inconsistencies can create confusion and frustration among employees, leading to reduced trust and usage of Copilot. To address this challenge, organizations need granular insights into how Copilot is being used across different Microsoft 365 apps and by users with various language settings. CoreView's advanced analytics capabilities provide this visibility.

[CoreView's audit logs](#) (Figure 22-9) drill down into specific Copilot activities within each Microsoft 365 application, revealing which apps are seeing the highest engagement and which ones may be lagging behind due to limitations. This data allows IT teams to identify opportunities for targeted user training, app-specific configuration optimizations, and feedback to Microsoft on areas for Copilot improvement.

The screenshot shows the CoreView dashboard with the 'Audit' and 'Copilot' sections highlighted. The 'Copilot activities' section is selected, displaying a table of audit logs. The table has columns for Workload, Operation, Record type, User Id, User type, and Creation date. The data shows various Copilot operations like 'Modify', 'Visit', and 'Delete' across platforms like Yammer, Sway, AzureActiveDirectoryStsLogon, SharePointSearch, etc., performed by users like 'elisabetta@contoso.com' and 'doadmin@contoso.com'. The interface includes filters, a search bar, and navigation controls.

Workload	Operation	Record type	User Id	User type	Creation
Copilot	Modify	Yammer	elisabetta@contoso.com	Application	Jan 26, 2024
Copilot		Sway	elisabetta@contoso.com	Application	Jan 26, 2024
Copilot	Visit	AzureActiveDirectoryStsLogon	elisabetta@contoso.com	Application	Jan 26, 2024
Copilot	Delete	SharePointSearch	doadmin@contoso.com	Application	Jan 26, 2024
Copilot	Wait	SharePointFileOperation	elisabetta@contoso.com	DcAdmin	Jan 26, 2024
Copilot		MicrosoftTeamsAddOns	elisabetta@contoso.com	Application	Jan 26, 2024
Copilot	PasswordLogonInitialAuthUsingPassword	AzureActiveDirectory	elisabetta@contoso.com	Regular	Jan 26, 2024
Copilot	Visit	PowerApps	elisabetta@contoso.com	DcAdmin	Jan 26, 2024
Copilot	Wait	SkypeForBusiness	elisabetta@contoso.com	DcAdmin	Jan 26, 2024

Figure 22-9: Coreview's Copilot Audit Logs

To access all Copilot logs, click on "Audit" in the side panel menu on the CoreView dashboard, then navigate to "Copilot" > "Copilot Activities". It will provide you with a detailed breakdown of Copilot operations from different users across various Microsoft 365 apps like SharePoint, PowerApps, and Viva Engage.

Higher than expected change management effort

Copilot introduces a new way of interacting with Microsoft 365 applications. Underestimating the change management needs can lead to slow adoption, user resistance, and suboptimal return on investment. Effective change management for Copilot involves more than just technical deployment. It requires a comprehensive approach that addresses user awareness, training, support, and ongoing reinforcement.

Organizations need to clearly communicate the benefits of Copilot and how it will enhance productivity and efficiency. Users must be equipped with the knowledge and skills to confidently interact with the AI assistant and understand its capabilities and limitations.

However, delivering this level of change management at scale can be challenging, particularly for large and distributed organizations. IT teams may struggle to provide personalized training and support to meet the diverse needs of different user groups, departments, and regions. Generic, one-size-fits-all approaches to change management often fall short in driving meaningful adoption.

Once again, CoreView's audit logs can prove particularly useful here, enabling IT teams to identify departments, user groups, or regions that are underutilizing Copilot — pinpointing areas where targeted change management interventions are needed.

With this visibility, organizations can develop personalized communication, training, and support strategies tailored to the specific needs of each user segment. For example, if CoreView reveals that the finance department has low Copilot adoption, IT can work with finance leaders to understand the unique challenges and requirements of their team.

By monitoring Copilot usage trends, IT can also identify which interventions are having the greatest impact and adjust their strategies accordingly. For example, if usage across the HR department has doubled after a recent Copilot training session, that could indicate that the resources shared were particularly effective.

Five more advanced tips for Copilot adoption

Adopting Microsoft 365 Copilot is an exciting step for organizations looking to leverage AI to boost productivity and innovation. While tools like CoreView provide valuable analytics and governance capabilities to support the rollout, there are additional strategies you can employ to ensure a smooth and successful adoption.

An effective Copilot implementation goes beyond just deploying the technology. It requires a comprehensive approach that addresses user readiness, training, support, and ongoing optimization. By taking proactive steps to prepare users, establish best practices, and continuously refine the user experience, IT teams can greatly maximize the value of the AI assistant.

Here are five advanced tips to help IT teams successfully adopt Microsoft 365 Copilot, using resources, tools, and strategies recommended directly by Microsoft:

Break down adoption into cohorts for a phased rollout

Deploying the Copilot machine across your entire Microsoft 365 organization at once can be challenging. Instead, consider breaking your company-wide adoption into cohorts, such as by department or region.

For example, [Microsoft](#) divided their internal adoption along two vectors: organizations like Legal or Sales and regions like North America or Europe. Different cohorts will have different focuses, but the overall strategy can be similar. This phased approach allows you to run Copilot through early adopters, gather feedback, optimize your processes, and then progressively roll it out to the rest of the organization. Communicate the phased plan clearly so employees know when to expect access.

With CoreView, you can easily create a Virtual Tenant™ that matches the criteria of your defined cohorts. This enables you to delegate reporting on Copilot adoption and allocate licenses to active Microsoft 365 users (or reallocate licenses from inactive ones).

Prepare teams for the unique Copilot support model

Supporting Copilot requires a different approach than traditional IT tools. Give your support teams early access to Copilot along with your initial pilot groups. Establish a collaborative space where support can share knowledge. Have them build out an internal knowledge base as they learn. Conduct shadowing and role-playing sessions so the team gains practical experience. Push support resources live before the broad deployment and track common issues that arise.

The fact that Copilot spans many Microsoft 365 apps adds complexity, so ensure your support staff represents different app specialties and service tiers.

Drive adoption through Copilot Lab's prompt library

Prompts are how you ask Copilot to perform tasks. [Copilot Lab](#) provides a library of example prompts to help users get started and build their skills. Have your training and adoption teams leverage these prompts in their materials and sessions.

Encourage users to explore the prompt library to find inspiration for their own workflows. Gather the most effective prompts used in your organization and share them internally. Consider building a company-specific prompt library in SharePoint or Teams. Promote a culture of sharing successful prompts across the organization to accelerate productivity.

Implement a tiered security and governance approach

Applying zero trust principles is crucial for secure Copilot usage. Require MFA, manage app behaviors, use least-privilege access, and protect data with sensitivity labels and data loss prevention policies.

Configure tenant-level policies in the Microsoft 365 admin center to control how Copilot accesses data.

For more advanced scenarios, use Copilot Studio to customize Copilot's interactions with other systems and data sources. Educate users that Copilot inherits the same security and compliance boundaries they already have in place for Microsoft 365. Implement a tiered governance model aligned to different data sensitivity levels.

Use the Copilot Scenario Library to identify use cases

[The Copilot Scenario Library](#) provides guidance on how Copilot can be applied to different business functions like sales, marketing, finance, and HR. Have your teams review these scenarios to identify high-impact use cases to prioritize in your rollout.

The library includes example outcomes, success measures, and individual scenarios for each department. Use this to create targeted adoption campaigns and training for each function. Encourage business leaders to explore the scenarios for their own departments to generate excitement and buy-in. Track your organization's Copilot usage across scenarios to measure success.

CoreView's Free Tools for Microsoft 365 Management

With over 25 million managed licenses across 40+ partners using Microsoft 365, CoreView has been helping organizations like yours adopt new Microsoft technologies for over a decade. We also offer a suite of free tools to help organizations better secure, govern, and manage their Microsoft 365 environments.

By leveraging [CoreView's free tools](#), your team can proactively mitigate security risks, optimize configurations, and ensure a smooth transition to Microsoft Copilot. Here are some of CoreView's top free tools for Microsoft 365 management:

Entra Security Scanner for App Registrations

At CoreView, we're dedicated to helping businesses improve their Microsoft 365 environment and make best practice effortless. With our free tool, [Entra Security Scanner for App Registrations](#), you can secure Microsoft 365 as you continue to prepare for and adopt Copilot.

These PowerShell scripts, developed by Office 365 for IT Pros editor and Microsoft MVP Vasil Michev, give you:

- **Comprehensive Permissions Audits:** Understand the scope of permissions granted to each in-house developed app, identifying any that may be unnecessarily broad or risky.
- **Credentials Management Analysis:** Evaluate how your internal apps manage credentials, highlighting any that may be expired or non-compliant.
- **Actionable, Tailored Recommendations:** Get advice for mitigating the identified risks, tightening your security posture, and ensure your internal apps adhere to best practices for security and compliance.

Please note that the time it takes to run these scripts depends on the number of site collections you have. We strongly suggest reading the instructions before using the scripts.

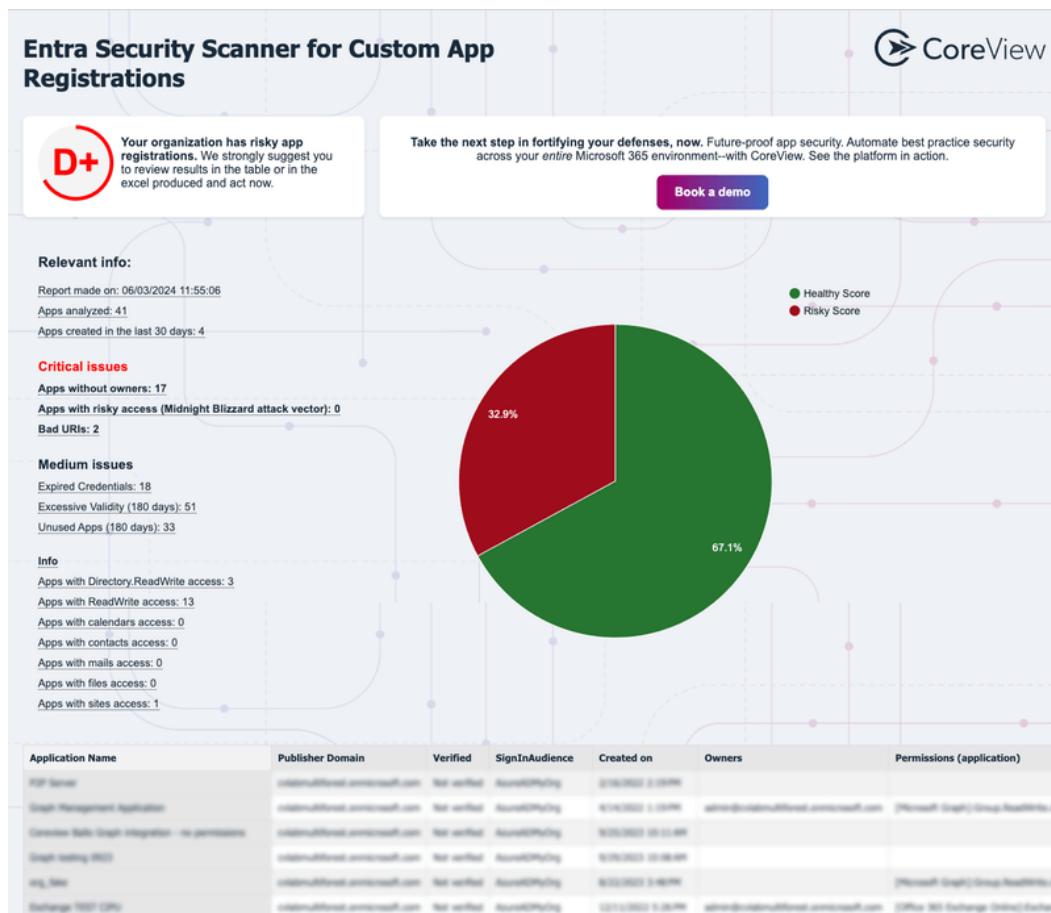


Figure 22-10: Entra Security Scanner

Free Microsoft 365 Governance Starter Kit

The [Free Microsoft 365 Governance Starter Kit](#) from CoreView helps organizations kickstart their governance initiatives.

Designed to integrate seamlessly into your busy schedule, use these templates and checklists to:

- Quickly pinpoint **critical governance gaps** with the Assessment Checklist
- Jumpstart your action plan with **customizable plan templates**
- Implement **powerful collaboration governance**, balancing security and teamwork

By leveraging this starter kit, IT teams can begin to establish a solid foundation for Microsoft 365 governance. The included resources help identify governance gaps, prioritize remediation efforts, and formulate strategies for maintaining a secure and compliant environment.

Checklist for Planning Automations in Power Automate

CoreView recognizes the immense value that automation brings to Microsoft 365 administration. Power Automate is Microsoft's powerful workflow automation tool that enables streamlining of repetitive tasks.

To help organizations succeed with Power Automate, CoreView offers a free [Checklist for Planning Automations](#). This checklist covers key considerations such as:

- Identifying suitable processes for automation based on frequency, complexity, and impact
- Mapping out required inputs, outputs, and data transformations for each automation
- Determining appropriate triggers and actions within Power Automate
- Establishing testing and deployment plans to ensure automations function as intended

By systematically working through this planning checklist, IT teams can ensure their Power Automate initiatives are well-designed and aligned with business objectives. The checklist helps avoid common pitfalls and wasted effort by enforcing a structured approach to automation projects.

About CoreView

CoreView is the Global Leader in effortless Microsoft 365 Security, Governance, and Administration. Our end-to-end solution stretches across the whole Microsoft 365 ecosystem; from your tenant level configurations, right up to your most critical workloads.

Created by Microsoft 365 experts, for Microsoft 365 experts, CoreView makes best practice effortless by simplifying, unifying, and enhancing the Microsoft 365 admin experience. CoreView empowers 1,500 Microsoft 365 organizations globally to turn the tide on endless tasks, deliver best practice security, and drive ROI. Learn more here: <https://www.coreview.com>

Appendix

This appendix holds interesting information about Microsoft 365 that fits better here rather than interrupting the flow of text in a chapter.

Annualized Run Rate for the Microsoft Cloud

Table: A-1 lists the annualized run rate for the Microsoft Cloud business segment as reported in Microsoft quarterly results. The big leap from FY19 is accounted for [Microsoft's September 2018 announcement](#) that they would include results for LinkedIn from that point.

Quarter results	Reported annualized revenue run rate (ARR) for the Microsoft Cloud
FY15 Q3 (April 2015)	\$6.3 billion
FY15 Q4 (July 2015)	\$8.0 billion
FY16 Q4 (July 2016)	\$12.1 billion
FY17 Q1 (October 2016)	Over \$13 billion
FY17 Q2 (January 2017)	Over \$14 billion
FY17 Q3 (April 2017)	\$15.2 billion
FY17 Q4 (July 2017)	\$18.9 billion
FY18 Q1 (October 2017)	\$20.4 billion
FY18 Q2 (January 2018)	\$21.2 billion (based on \$5.3B revenue reported for the quarter)
FY18 Q3 (April 2018)	\$24 billion (\$6B revenue)
FY18 Q4 (July 2018)	\$27.6 billion (\$6.9B revenue)
FY19 Q1 (October 2018)	\$39 billion (\$9.77B revenue)
FY19 Q2 (January 2019)	\$40.4 billion (\$10.1B revenue)
FY19 Q3 (April 2019)	\$40.96 billion (\$10.24B revenue)
FY19 Q4 (July 2019)	\$44 billion (\$11B revenue)
FY20 Q1 (October 2019)	\$46.4 billion (\$11.6B revenue)
FY20 Q2 (January 2020)	\$50 billion (\$12.5B revenue)
FY20 Q3 (April 2020)	\$53.2 billion (\$13.3B revenue)
FY20 Q4 (July 2020)	\$57.2 billion (\$14.4B revenue)
FY21 Q1 (October 2020)	\$60.8 billion (\$15.2B revenue)
FY21 Q2 (January 2021)	\$66.8 billion (\$16.7B revenue)
FY21 Q3 (April 2021)	\$70.8 billion (\$17.7B revenue)
FY21 Q4 (July 2021)	\$78 billion (\$19.5B revenue)
FY22 Q1 (October 2021)	\$82.8 billion (\$20.7B revenue)
FY22 Q2 (January 2022)	\$88.4 billion (\$22.1B revenue)
FY22 Q3 (April 2022)	\$93.6 billion (\$23.4B revenue)
FY22 Q4 (July 2022)	\$100 billion (\$25 B revenue)
FY23 Q1 (October 2022)	\$102.8 billion (\$25.7B revenue)
FY23 Q2 (January 2023)	\$108.4 billion (\$27.1B revenue)
FY23 Q3 (April 2023)	\$114 billion (\$28.5B revenue)
FY23 Q4 (July 2023)	\$121.2 billion (\$30.3B revenue)
FY24 Q1 (October 2023)	\$127.2 billion (\$31.8B revenue)
FY24 Q2 (January 2024)	\$134.8 billion (\$33.7B revenue)
FY24 Q3 (April 2024)	\$140.4 billion (\$35.1B revenue)
FY24 Q4 (July 2024)	\$147.2 billion (\$36.8B revenue)

Table: A-1: Annualized revenue run rate for the Microsoft Cloud

Growth in Office 365 User Numbers

Table A-2 details the growth in Office 365 user numbers since November 2015. For several years Microsoft reported the number of monthly active users every six months during their April and October earnings. In April 2020, Microsoft switched to reporting the number of paid seats instead, claiming that Office 365 then had 258 million. You could assume that a paid seat is an active seat, but that isn't always the case. In their April 2023 earnings call, Microsoft said that the number of paid commercial Office 365 seats grew 11% year-over-year (the number cited in October 2021 was 17%). Table A-2 documents the growth in Office 365 usage since 2015. The bolded figures for paid seats are those given by Microsoft in quarterly briefings.

Date	Microsoft number for monthly active Office 365 users	Microsoft number for paid seats
November 2015	60 million	
April 2016	70 million	
October 2016	85 million	
April 2017	Over 100 million	
October 2017	120 million	
April 2018	135 million	
October 2018	155 million	
April 2019	180 million	
October 2019	200 million	
April 2020	230 million (estimate)	258 million
October 2020	245 million (estimate)	278 million (estimate)
April 2021	264.5 million (estimate)	299 million
July 2021	280 million (estimated)	315 million (estimate)
October 2021	290 million (estimated)	325 million (estimate)
April 2022	321 million (estimate)	345 million
July 2022	330 million (estimated)	360 million (estimate)
October 2022	345 million (estimated)	366 million (estimate)
January 2023	365 million (estimated)	375 million (estimate)
April 2023	370 million (estimate)	382 million
July 2023	380 million (estimate)	388 million (estimate)
October 2023	390 million (estimate)	400 million (estimate)
January 2024	400 million (estimate)	"over 400 million"
April 2024	403 million (estimate)	410 million
July 2024	406 million (7% increase YoY)	413 million

Table A-2: Growth in Office 365 user numbers over time

Note: Numbers shown since April 2020 are based on data reported by Microsoft in quarterly results. Because Microsoft doesn't give precise numbers for active users or paid seats, the data listed here is our best interpretation of the figures given by Microsoft, including percentage growth since a prior quarter. Take the numbers as an estimate and use them as a guideline.

Office 365 Quarterly Performance Against SLA

Table A-3 details the performance against SLA since Microsoft first started to publish figures SLA performance details in 2013. The highlighted figure is the most recent quarterly result. The data applies to the commercial cloud and not to GCC, DoD, or other Microsoft 365 cloud services.

Q1 2013	Q2 2013	Q3 2013	Q4 2013	Q1 2014	Q2 2014	Q3 2014	Q4 2014
99.94%	99.97%	99.96%	99.98%	99.99%	99.95%	99.98%	99.99%
Q1 2015	Q2 2015	Q3 2015	Q4 2015	Q1 2016	Q2 2016	Q3 2016	Q4 2016
99.99%	99.95%	99.98%	99.98%	99.98%	99.98%	99.99%	99.99%
Q1 2017	Q2 2017	Q3 2017	Q4 2017	Q1 2018	Q2 2018	Q3 2018	Q4 2018
99.99%	99.97%	99.985%	99.988%	99.993%	99.98%	99.97%	99.98%
Q1 2019	Q2 2019	Q3 2019	Q4 2019	Q1 2020	Q2 2020	Q3 2020	Q4 2020
99.97%	99.97%	99.98%	99.98%	99.98%	99.99%	99.97%	99.97%
Q1 2021	Q2 2021	Q3 2021	Q4 2021	Q1 2022	Q2 2022	Q3 2022	Q4 2022
99.97%	99.98%	99.985%	99.976%	99.98%	99.98%	99.99%	99.99%
Q1 2023	Q2 2023	Q3 2023	Q4 2023	Q1 2024	Q2 2024		
99.98%	99.99%	99.99%	99.996%	99.97%	99.99%		

Table A-3: Office 365 SLA performance since 2013