

Contents

[Microsoft 365 Enterprise documentation and resources](#)

[Microsoft 365 Enterprise overview](#)

[Deploy Microsoft 365 Enterprise](#)

[Deploy foundation infrastructure](#)

[Phase 1: Networking](#)

[Step 1: Prepare your network for Microsoft 365](#)

[Step 2: Configure local Internet connections for each office](#)

[Step 3: Avoid network hairpins](#)

[Step 4: Configure traffic bypass](#)

[Step 5: Optimize client and Office 365 service performance](#)

[Networking exit criteria](#)

[Phase 2: Identity](#)

[Step 1: Plan for users and groups](#)

[Step 2: Secure your privileged identities](#)

[Step 3: Configure hybrid identity](#)

[Step 4: Configure secure user authentication](#)

[Step 5: Simplify access for users](#)

[Step 6: Use groups for easier management](#)

[Identity exit criteria](#)

[Phase 3: Windows 10 Enterprise](#)

[Step 1: Prepare your organization](#)

[Step 2: Deploy as an in-place upgrade](#)

[Step 3: Deploy for new devices](#)

[Step 4: Monitor device health and compliance](#)

[Step 5: Deploy security features](#)

[Windows 10 Enterprise exit criteria](#)

[Phase 4: Office 365 ProPlus](#)

[Office 365 ProPlus exit criteria](#)

[Phase 5: Mobile device management](#)

Mobile device management exit criteria

Phase 6: Information protection

Step 1: Define security and information protection levels

Step 2: Configure classification for your environment

Step 3: Configure increased security for Office 365

Step 4: Configure privileged access management for Office 365

Information protection exit criteria

Deployment strategies

Deploy with existing infrastructure

Deploy workloads and scenarios

Microsoft Teams

Exchange Online

SharePoint Online and OneDrive for Business

Migration

Teams and sites for highly regulated data

Test Lab Guides

Base configuration

Lightweight

Simulated enterprise

Identity

Password hash sync

Pass-through authentication

Azure AD Seamless Single Sign-on

Multi-factor authentication

Protect global administrator accounts

Password reset

Password writeback

Automatic licensing and group membership

Azure AD Identity Protection

Mobile device management

Enroll iOS and Android devices

Device compliance policies

Information protection

Increased Office 365 security

Data classification

Privileged access management

Contoso case study

Overview

Contoso's IT infrastructure and needs

Networking

Identity

Windows 10 Enterprise

Office 365 ProPlus

Mobile device management

Information protection

Security summary

SharePoint Online site for highly regulated data

Modern Desktop Deployment Center

Getting Started: People, Process and Technology Guidance

Step 1: Device and App Readiness

Step 2: Directory and Network Readiness

Step 3: Office and LOB App Delivery

Step 4: User Files and Settings Migration

Step 5: Security and Compliance Considerations

Step 6: OS Deployment and Feature Updates

Step 7: Windows and Office Servicing

Step 8: User Communications and Training

Modern Desktop Deployment and Management Lab Kit

Find help for your deployment

Get your Leadership on Board: Value Discovery and Business Case

Identity and device access configurations

Prerequisite work

Common identity and device access policies

Recommended Exchange Online access policies

[Recommended SharePoint Online access policies](#)

[Compliance solutions](#)

[ISO — Recommended action plan](#)

[NIST — Recommended action plan](#)

[GDPR](#)

[Recommended action plan for GDPR](#)

[Accountability readiness checklists](#)

[Office 365](#)

[Azure](#)

[Dynamics 365](#)

[Microsoft Support and Professional Services](#)

[Information protection](#)

[Data subject requests](#)

[Office 365](#)

[Azure](#)

[Intune](#)

[Dynamics 365](#)

[Visual Studio family](#)

[Azure DevOps Services](#)

[Microsoft Support and Professional Services](#)

[Breach notification](#)

[Office 365](#)

[Azure](#)

[Dynamics 365](#)

[Microsoft Support and Professional Services](#)

[Data protection impact assessments](#)

[Office 365](#)

[Azure](#)

[Dynamics](#)

[Microsoft Support and Professional Services](#)

[Microsoft's data protection officer](#)

Microsoft 365 Enterprise documentation and resources

Learn how to plan, deploy, and use Microsoft Office 365, Windows 10, and Enterprise Mobility + Security together in your organization. These services provide an integrated and secure infrastructure that enables teamwork and unlocks creativity.

Explore

[Overview](#)

[Architecture models](#)

[Microsoft 365 for IT](#)

Deploy

[FastTrack](#)

[Deployment guide](#)

[Modern Desktop deployment](#)

Manage security & compliance

[Compliance solutions](#)

[Office 365 Security & Compliance](#)

[Identity & device access](#)

[Windows Defender ATP](#)

Train your users

[Office 365](#)

[Windows 10](#)

[Intune & Company Portal app](#)

Manage Office 365

[Office 365 Enterprise](#)

[Office 365 Business](#)

[Office 365 ProPlus](#)

Manage Enterprise Mobility + Security

[Microsoft Cloud App Security](#)

[Microsoft Intune](#)

[Azure Active Directory](#)

[Azure Information Protection](#)

[Azure Advanced Threat Protection](#)

Develop for Microsoft 365

[Office 365 Dev Center](#)

[Windows Dev Center](#)

[Microsoft Graph](#)

Other Microsoft 365 products

[Microsoft 365 Business](#)

[Microsoft 365 Education](#)

Need support?

[Azure](#)

[Office 365](#)

[Windows 10](#)

Microsoft 365 Enterprise overview

12/10/2018 • 2 minutes to read • [Edit Online](#)

Microsoft 365 Enterprise is a complete, intelligent solution that empowers everyone to be creative and work together securely.

Although designed for large organizations, Microsoft 365 Enterprise can also be used for medium-sized and small businesses that need the most advanced security and productivity capabilities.

Components

Microsoft 365 Enterprise consists of:

Office 365 Enterprise	Includes both Office 365 ProPlus, the latest Office apps for your PC and Mac (such as Word, Excel, PowerPoint, Outlook, and others), and a full suite of online services for email, file storage and collaboration, meetings, and more.
Windows 10 Enterprise	Addresses the needs of both large and midsize organizations, providing users with the most productive and secure version of Windows and IT professionals with comprehensive deployment, device, and app management.
Enterprise Mobility + Security (EMS)	Includes Microsoft Intune, which is a cloud-based enterprise mobility management (EMM) service that helps enable your workforce to be productive while keeping your corporate data protected.

Plans

Microsoft 365 Enterprise is available in three plans.

E3	Includes Office 365 Enterprise, Windows 10 Enterprise, and Enterprise Mobility + Security (EMS).
E5	Includes all of E3's capabilities plus advanced security, voice, and data analysis tools.
F1	Purpose-built to connect firstline workers to the tools and resources needed to do their best work. Firstline workers are the first in line to engage with your customers and represent your company's brand and value,

For more information, see [Features and capabilities for each plan](#).

At-a-glance

The Microsoft 365 Enterprise poster is a central location for you to view:

- The products and features of Microsoft 365 Enterprise and how they map to its value pillars
- Microsoft 365 Enterprise plans and which components they contain
- The key components of the Modern Workplace, which Microsoft 365 Enterprise enables
- The key business value scenarios of Microsoft 365 Enterprise and which services and products make them happen
- The adoption roadmap that highlights the Microsoft 365 Enterprise [Deployment Guide](#)

Microsoft 365 Enterprise

A complete, intelligent solution that empowers everyone to be creative and work together securely.

Microsoft 365 Enterprise
=
Office 365
&
Windows 10 Enterprise
&
Enterprise Mobility + Security

Unlocks creativity	PowerPoint Designer, Editor, Smart Lookup, Excel Insights	Touch and ink support, 3D	
Built for teamwork	Exchange Online, SharePoint Online, Skype for Business, Microsoft Teams, Yammer, Office 365 ProPlus		
Integrated for simplicity	Office 365 ProPlus deployment	Windows 10 deployment with upgrade in place and Autopilot	Auto-enrollment of Windows PCs and devices
Intelligent security	Office 365 Advanced Threat Protection, Office 365 Multi-Factor Authentication, SharePoint Online and Exchange Online conditional access policies, Office 365 Threat Intelligence, Azure Information Protection (AIP), Data Loss Prevention policies.	Windows Defender Advanced Threat Protection (ATP), Windows Hello for Business, Windows Information Protection (WIP)	Microsoft Intune device-based conditional access policies, Azure AD Privileged Identity Management (PIM), Advanced Threat Analytics, Azure Advanced Threat Protection, Microsoft Cloud App Security, Azure Multi-Factor Authentication, and others
Microsoft 365 Enterprise plans	Operating system Edition, Office Applications, Email & calendar, One-based workspace, Schedule & Task Management, Voice, video, & meetings, Social & Intranet, Threat protection, Identity & access management, Device & app management, Information protection, Advanced compliance, Analytics	Windows 10 Enterprise E3, E5, F1, Microsoft 365 Business Premium, Microsoft 365 Business Standard, Microsoft 365 Business Basic, Microsoft 365 Business Recreational, Microsoft 365 Business All-in, Microsoft 365 Business All-in with Intune, Microsoft 365 Business All-in with Intune and Intune Device Health, Microsoft 365 Business All-in with Intune and Intune Device Health and Intune Device Health	Date
The Modern Workplace	Modern Desktop, Compliance, Security, Teamwork, Firstline Worker	Collaboration, Communication, Leadership connection, Learning & sharing	Foster culture & community, Train & upskill employees, Digitize business process, Deliver real-time expertise
Business Value Scenarios	Collaborate on documents in real time, Harness collective insight, Improve access to business processes, Shape the company culture, Manage projects, tasks, and deadlines, Simplify compliance, Broad set of compliance standards	Office 365 ProPlus, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business Online, Microsoft Teams, Microsoft StaffHub, Project Online, EMS, Windows 10	Provide space for teams to connect and share, Manage and deliver content and video, Moderate firstline tools, articles, and workflows, Close technology gaps and rethink productivity
Roadmap to adoption	Start here, Foundation Infrastructure, Self-guided at aka.ms/m365edeploy , Guided by FastTrack at microsoft.com/fasttrack/microsoft-365	Workloads and scenarios	September 2018 © 2018 Microsoft Corporation. All rights reserved. To send feedback about this documentation, please write to us at M365docs@microsoft.com. Microsoft

To download a copy of the poster, click [here](#).

Deploying

There are two ways to deploy the products, features, and components of Microsoft 365 Enterprise:

1. In partnership with FastTrack

With FastTrack, Microsoft engineers help you move to the cloud at your own pace. See [FastTrack for Microsoft 365](#).

2. Do it yourself

The [Microsoft 365 Enterprise deployment guide](#) takes you step by step through building out the infrastructure and productivity workloads.

For more deployment information, see how:

- **Customers** use Microsoft 365 Enterprise.
- **Microsoft** uses Microsoft 365 Enterprise.
- **The Contoso Corporation** has deployed Microsoft 365 Enterprise.

Identity and device access configurations

Although there is no single best recommendation for all customer environments, the [identity and device access configurations](#) documentation describes how to apply policies and configuration within the Microsoft cloud to ensure that your employees are both secure and productive.

Next step

Start your [Microsoft 365 Enterprise deployment journey](#).

See also

[Microsoft 365 Enterprise product page](#)

Deploy Microsoft 365 Enterprise

12/17/2018 • 6 minutes to read • [Edit Online](#)

Microsoft 365 Enterprise is a combination of Office 365, Enterprise Mobility + Security (EMS), and Windows 10 Enterprise that:

- Has intelligent security.
- Is integrated for simplicity.
- Unlocks creativity.
- Is built for teamwork.

These benefits are not realized just by obtaining the licenses for the three products, but by deploying them and their features in a specific way that includes integration and state-of-the-art security.

There are two main ways to deploy Microsoft 365 Enterprise:

- Do it with Microsoft engineers using FastTrack for Microsoft 365
- Do it yourself with the Microsoft 365 Enterprise deployment guide

FastTrack for Microsoft 365

FastTrack is an ongoing and repeatable benefit—available as part of your subscription—that is delivered by Microsoft engineers to help you move to the cloud at your own pace. FastTrack also gives you access to qualified partners for additional services. With over 40,000 customers enabled to date, FastTrack helps maximize ROI, accelerate deployment, and increase adoption across your organization. See [FastTrack for Microsoft 365](#).

If you want to take advantage of FastTrack to deploy Microsoft 365 Enterprise, you can use the FastTrack [Microsoft 365 deployment advisor](#) for guidance on how to deploy and set up your foundation infrastructure. Note that you must be signed on as a global administrator in an Office 365 or Microsoft 365 tenant in order to access this page.

Get started on your end-to-end deployment journey with FastTrack [here](#).

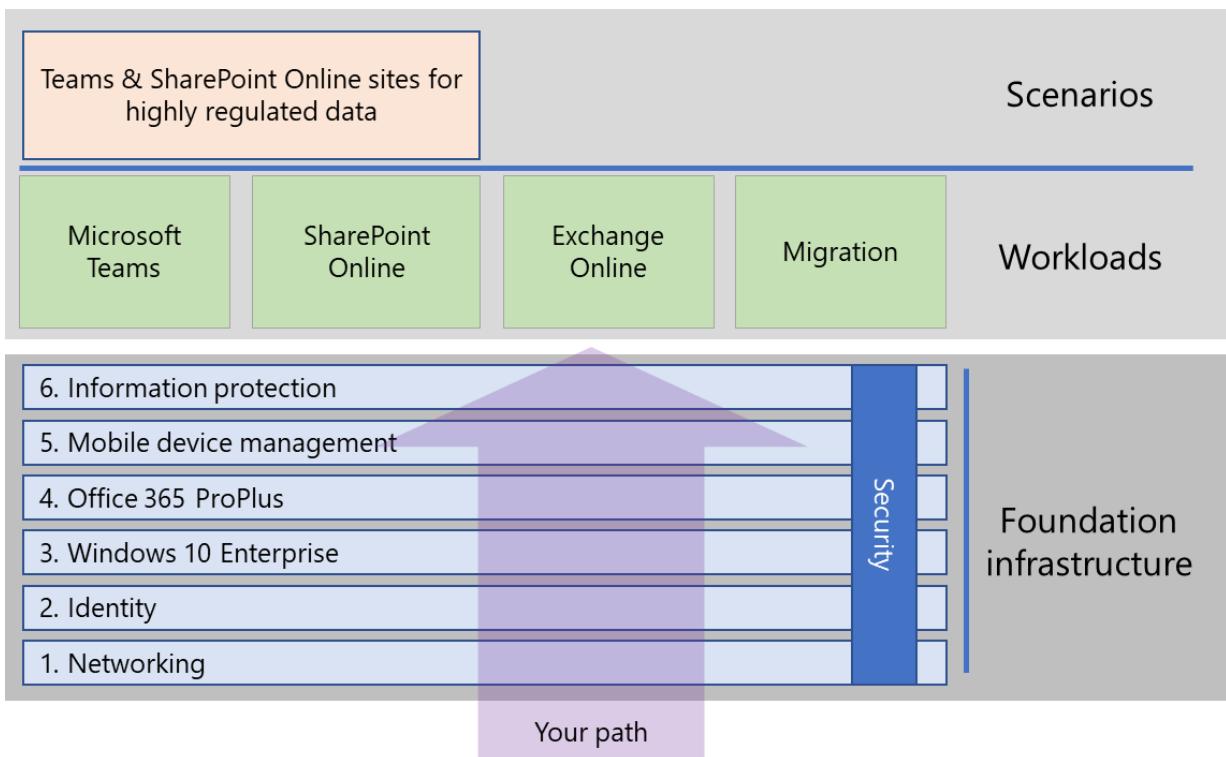
Microsoft 365 Enterprise deployment guide

The Microsoft 365 Enterprise Deployment Guide steps you through the end-to-end deployment so that when you're done, you have the correct and required configuration of Microsoft 365 Enterprise products and features.

To deploy Microsoft 365 Enterprise yourself:

- First, deploy the required [foundation infrastructure](#) for built-in security and integration for simplified management, which makes it easier to ensure your client software is updated with the latest productivity and security enhancements.
- Next, deploy key productivity [workloads and scenarios](#) on top of the foundation infrastructure. These unlock creativity and teamwork in your organization.

Here's the relationship between the foundation infrastructure and the workloads and scenarios and your path through the content.



Get self-started on your end-to-end deployment journey [here](#).

Take a test drive

"For the things we have to learn before we can do them, we learn by doing them." - Aristotle

If you're new to Microsoft 365 Enterprise or to a specific product or feature, one of the best ways to gain understanding is to build it out yourself and see it working.

We've made this easier with Test Lab Guides (TLGs), which step you through the configuration of infrastructure or a feature in a simplified but representative environment using trial or paid subscriptions.

With TLGs, you can self-learn, demonstrate, customize, or build a proof of concept of a complex configuration, workload, or end-to-end scenario.

For more information, see [Microsoft 365 Enterprise Test Lab Guides](#).



How did others do it?

Use these resources to understand how others have deployed and are using Microsoft 365 Enterprise.

How customers use Microsoft 365 Enterprise

Here's how our customers are using Microsoft 365 Enterprise as their complete, intelligent solution that empowers everyone to be creative and work together securely:

- Construction
 - [Search for data security solution unearths collaborative capabilities of Microsoft 365 at general contracting company](#)
 - [EMCOR Group transitions to the cloud, constructs intelligent workplace with Microsoft 365](#)
- Consulting

- ERM contributes to a more sustainable future with Microsoft 365
- Energy services
 - Schlumberger refines global teamwork with Microsoft 365
- Engineering
 - Cadence increases the pace of business with mobile collaboration tools
- Financial services
 - TD Bank empowers employees with assistive technology in Office 365 and Windows 10
 - Family tax preparation startup chooses all-in-one solution to help grow business
- Gaming
 - Gaming company improves productivity and communications with Microsoft 365 and Surface devices
 - Razer plays to win, gains advantage in global gaming industry with Microsoft 365
- Health services
 - Lilly envisions a workplace where internal and external collaboration help enable innovation and accelerate time-to-market for new medicines
 - Healthcare technology innovator accelerates diabetes prevention in the cloud
 - Adventist Health System is enhancing healthcare delivery using Microsoft 365
 - Abrona accelerates GDPR compliance and increases productivity with Microsoft 365
 - Centra embraces transformation, improves patient care with Microsoft 365 intelligent business tools
 - Advocate Aurora Health helps patients live well using Microsoft care coordination solution to enhance collaboration
- Importing
 - Sales, marketing, and import company increases data security and cuts operating costs with Microsoft 365
- Manufacturing
 - Steel company eliminates hardware costs, streamlines IT, and gains mobile productivity in the cloud
 - Embroidery equipment supplier empowers its business with cloud-based services, spreads word to other small businesses
 - Father and son business shows the world what employees with disabilities can achieve
 - Coconut company gains improved mobility, better metrics, and increased productivity by modernizing collaboration tools
 - Thriving Japanese innovator finds future-proof flexibility and enhanced security with Microsoft 365 Business
- Non-profit
 - Move to the cloud saves nonprofit \$500,000 while improving security, mobility, and collaboration
- Professional services
 - Boutique business and real estate law firm supports expansion with comprehensive cloud-based platform
 - Sports technology company helps athletes reach their peak through biofeedback and analytics
 - Digital transformation and the cloud empower business association to serve its members better
- Transportation
 - Qantas empowers employees to do their best work with Microsoft 365, enhancing customer experience
 - Amtrak keeps its mobile enterprise running ahead of schedule with Microsoft 365
 - Amtrak is all aboard with workplace modernization, saving labor costs and improving portfolio transparency using Microsoft 365

How Microsoft uses Microsoft 365 Enterprise

Take a peek inside Microsoft IT and learn how they deployed Microsoft 365 Enterprise and how Microsoft employees use it every day.

Networking

- Optimizing network performance for Microsoft Office 365

Identity

- Managing user identities and secure access at Microsoft
- Using Azure AD Privileged Identity Management for elevated access

Windows 10 Enterprise

- Preparing your organization for a seamless Windows 10 deployment
- Adopting Windows as a service at Microsoft
- Deploying Windows 10 at Microsoft as an in-place upgrade
- Implementing strong user authentication with Windows Hello for Business
- Windows 10 deployment: tips and tricks from Microsoft IT (video)
- Windows Defender ATP helps detect sophisticated threats
- Securing the modern enterprise with Windows Defender and Windows Defender ATP (video)

Office 365 ProPlus

- Deploying and updating Microsoft Office 365 ProPlus
- Automation and update channels help deploy Microsoft Office 365 ProPlus (video)

Mobility and device management

- Managing modern mobile productivity with Enterprise Mobility + Security
- Connecting to work on your Windows 10 device with Microsoft Intune
- Enabling mobile productivity for iOS, OS X, and Android devices at Microsoft

Security and information protection

- Protecting files in the cloud with Azure Information Protection
- Microsoft uses threat intelligence to protect, detect, and respond to threats
- Microsoft thwarts phishing attempts with Office 365

Microsoft Teams

- Deploying Microsoft Teams streamlines collaboration and improves teamwork
- Microsoft Teams increases collaboration in the modern workplace at Microsoft

Data migration

- Microsoft migrates 150,000 mailboxes to Exchange Online
- SharePoint to the cloud: Learn how Microsoft ran its own migration

How the Contoso Corporation deployed Microsoft 365 Enterprise

The Contoso Corporation is a fictional but representative global manufacturing conglomerate with its headquarters in Paris, France. See how [Contoso deployed Microsoft 365 Enterprise](#) and addressed major design decisions and implementation details for networking, identity, Windows 10 Enterprise, Office 365 ProPlus, mobile device management, information protection, and security.

Additional Microsoft 365 solutions

- [Microsoft 365 Business](#)

Bring together the best-in-class productivity and collaboration capabilities of Office 365 with device management and security solutions to safeguard business data for small and midsize businesses (SMB).

- Microsoft 365 Education

Empower educators to unlock creativity, promote teamwork, and provide a simple and safe experience in a single, affordable solution built for education.

Next step

To do it with direct Microsoft assistance, use [FastTrack](#).

To do it yourself, see the [foundation infrastructure](#).

Microsoft 365 Enterprise foundation infrastructure

1/24/2019 • 3 minutes to read • [Edit Online](#)

If you're doing the end-to-end deployment of Microsoft 365 Enterprise yourself, you must first build a firm foundation upon which applications and services can unlock creativity and teamwork in a secure environment. Use these phases to plan for and deploy the foundation infrastructure of Microsoft 365 Enterprise:

	PHASE	RESULTS
	Phase 1: Networking	Your network is optimized for access to Microsoft 365's cloud-based services.
	Phase 2: Identity	Your users and groups are synchronized, your user authentication is strong, and your admin accounts are protected.
	Phase 3: Windows 10 Enterprise	Your existing Windows-based computers can upgrade to Windows 10 Enterprise and new devices are installed with Windows 10 Enterprise.
	Phase 4: Office 365 ProPlus	Your existing users of Microsoft Office can upgrade to Office 365 ProPlus.
	Phase 5: Mobile device management	Your devices can be enrolled and managed.
	Phase 6: Information protection	Your labels are ready to protect documents and Office 365 security features are enabled.

The order of the phases start with the most foundational (networking and identity), and then create layers of infrastructure settings and groups to:

- Install the most current and secure version of Windows on your devices.
- Install the most current version of Office on your devices.
- Manage your organization's devices.
- Protect the information on those devices and in the cloud.

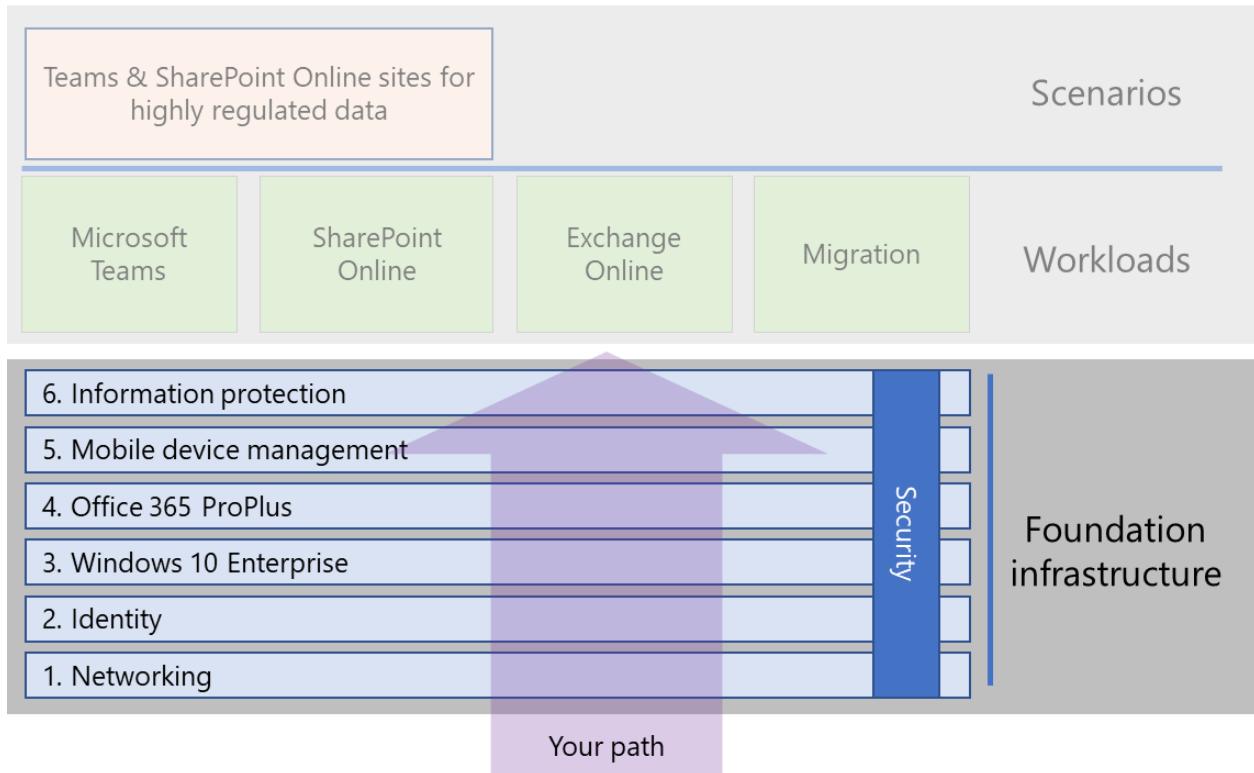
However, you have the flexibility of configuring and rolling out the phases of the foundation infrastructure to fit your business needs.

Before you can exit each phase, you must examine its exit criteria, which include required conditions that you must meet and optional conditions to consider. Exit criteria for each phase ensures that your on-premises and cloud infrastructure and resulting end-to-end configuration meet the requirements for a Microsoft 365

Enterprise deployment.

To see how the content is structured, watch this short video.

Here's the foundation infrastructure in the overall Microsoft 365 Enterprise deployment guide:



Infrastructure configuration vs. user rollout

The foundation infrastructure is a set of configured software and services that, when combined together for a user, allow them to take advantage of the entire spectrum of capabilities and protections that Microsoft 365 Enterprise offers. The ultimate destination of your end-to-end deployment journey is to have this infrastructure apply to all of your users and their Windows-based devices.

However, it is important to note that the Microsoft 365 Enterprise foundation infrastructure is independent of the rollout of software and services to your users. **You can configure the layers of the foundation infrastructure without having to roll out those layers to all of your users.**

Therefore, it is possible to configure, test, and pilot elements of the foundation infrastructure well ahead of the rollout of those elements to the multitude of your users in the offices, regions, or divisions of your organization.

For example, you create the settings for:

PHASE	RESULTS
Identity	Account synchronization and groups for identity-based conditional access policies.
Windows 10 Enterprise	Groups to automatically upgrade computers running Windows 7 or Windows 8.1 to Windows 10 Enterprise in place.
Office 365 ProPlus	Groups to automatically deploy Office 365 ProPlus for users with Office 2010, Office 2013, or Office 2016.

PHASE	RESULTS
Mobile device management	Groups for device enrollment and device-based conditional access policies.
Information protection	Office 365 and Azure Information Protection labels and groups.

When you are ready to rollout elements of this infrastructure to users, you:

PHASE	ROLLOUT ACTION
Identity	Add user accounts to the groups for identity-based conditional access policies.
Windows 10 Enterprise	Add accounts to the groups to automatically deploy Windows 10 Enterprise in place for users with Windows 7 or Windows 8.1.
Office 365 ProPlus	Add user accounts to the groups to automatically deploy Office 365 ProPlus for users with Office 2010, Office 2013, or Office 2016.
Mobile device management	Add accounts to the groups for device enrollment and device-based conditional access policies.
Information protection	Add user accounts to the groups for Information Protection labels.

Once the foundation infrastructure is completed, tested, and piloted, you can roll out installed software, such as Windows 10 Enterprise and Office 365 ProPlus, and cloud-based services and protections, such as device enrollment and conditional access policies, to your users in the manner that best fits your business goals and IT resources.

Deployment and project management strategies

To give you some ideas on how to approach the project management of the different phases of the foundation infrastructure for pilot users and the rest of your organization, see [deployment strategies](#).

Next step

- I have existing infrastructure for Office 365, Enterprise Mobility + Security, or Windows 10 Enterprise:
 - See [Deployment with existing infrastructure](#). This article steps you through the exit criteria for each phase.
- I'm starting from scratch:
 - Begin your end-to-end deployment journey with [Phase 1: Networking](#).

Phase 1: Networking infrastructure for Microsoft 365 Enterprise

2/7/2019 • 2 minutes to read • [Edit Online](#)



Microsoft 365 Enterprise includes Office 365 and Microsoft Intune as part of Enterprise Management + Security (EMS). Both of these cloud-based services rely on the security, performance, and reliability of connections from client devices over the Internet or dedicated circuits. To host these services and make them available to customers all over the world, Microsoft has designed a networking infrastructure that emphasizes performance and integration.

In this phase, you step through the key considerations for creating a performant connection to the cloud services of Microsoft 365 Enterprise. For an overview, see [Office 365 networking principles](#).

NOTE

If you already have a networking infrastructure deployed, please see the [exit criteria](#) for this phase to make sure that it meets the required and optional conditions for Microsoft 365 Enterprise.

Plan and deploy your Microsoft 365 Enterprise networking infrastructure

Use the following steps to build out your networking infrastructure for the requirements and capabilities of Microsoft 365 Enterprise.

1	Prepare your network for Microsoft 365
2	Configure local Internet connections for each office
3	Avoid network hairpins
4	Configure traffic bypass

5

Optimize client and Office 365 service performance

When you've completed these steps, go to the [exit criteria](#) for this phase to ensure that you meet the required and optional conditions for Microsoft 365 Enterprise.

How Microsoft does Microsoft 365 Enterprise

Peek inside Microsoft and learn how the company prepared for and optimized the Microsoft network for the Office 365 cloud services with [Optimizing network performance for Microsoft Office 365](#).

How Contoso did Microsoft 365 Enterprise

See how the Contoso Corporation, a fictional but representative multi-national business, [optimized their network](#) for Microsoft 365 cloud services.



Next step

1

[Prepare your network for Microsoft 365](#)

Step 1: Prepare your network for Microsoft 365

2/13/2019 • 2 minutes to read • [Edit Online](#)

This step is required and applies to both the E3 and E5 versions of Microsoft 365 Enterprise



In Step 1, you must:

- Evaluate and adjust network bandwidth for internal links and Internet connections to account for traffic to Microsoft 365 Enterprise cloud services.
- Align your network with an [Office 365 reference architecture](#).
- Plan the changes, pilot them, and then test whether the changes fit your bandwidth and traffic latency requirements.

For information and recommendations about using ExpressRoute with Office 365 and the other cloud services of Microsoft 365 Enterprise, see [Azure ExpressRoute for Office 365](#).

As an interim checkpoint, you can see the [exit criteria](#) corresponding to this step.

Next step

2

[Configure local Internet connections for each office](#)

Step 2: Configure local Internet connections for each office

12/5/2018 • 2 minutes to read • [Edit Online](#)

This step is required and applies to both the E3 and E5 versions of Microsoft 365 Enterprise



In Step 2, you ensure that each of your offices have local Internet connections and use local DNS servers. Both of these elements are required to reduce connection latency and ensure that on-premises client computers make connections to the nearest point of entry to Microsoft 365 cloud-based services.

In traditional networks for large organizations, Internet traffic travels across the network backbone to a central Internet connection. This does not work well for optimizing performance to a globally distributed Software-as-a-Service (SaaS) infrastructure, which includes the Office 365 and Enterprise Mobility + Security (EMS) products in Microsoft 365.

The Microsoft Global Network includes front end servers to the set of cloud services for Microsoft 365 all over the world. For the best performance, on-premises clients should access a front-end server that is geographically closest to them, rather than sending the traffic over a network backbone and to the front-end server that is closest to the organization's central Internet connection.

To direct a client request to the geographically nearest front-end server, Microsoft's DNS servers use the DNS queries corresponding the client's initial connection request. Therefore, for the lowest network latency:

- All offices of your organization should have local Internet connections for [Optimize](#) category network traffic.
- Each local Internet connection should be using a regionally local DNS server for outbound Internet traffic from that location.

For more information, see [Egress network connections locally](#).

As an interim checkpoint, you can see the [exit criteria](#) for this step.

Next step

3

[Avoid network hairpins](#)

Step 3: Avoid network hairpins

12/5/2018 • 2 minutes to read • [Edit Online](#)

This step is required and applies to both the E3 and E5 versions of Microsoft 365 Enterprise



A [network hairpin](#) happens when traffic bound for a destination is first directed to another intermediate location, such as an on-premises security stack, cloud access broker, or cloud-based web gateway. A network hairpin could also be caused by poor routing on the Internet due to network service providers. A hairpin adds latency and can potentially redirect traffic to a geographically distant location.

To optimize performance for traffic to Microsoft 365 cloud-based services, check whether the ISP providing the local Internet connection has a direct peering relationship with the Microsoft Global Network in close proximity to that location. These connections do not have hairpins.

If you use cloud-based network or security services for your Microsoft 365 traffic, ensure that the hairpinning effect is evaluated and its impact on performance is understood. Examine the following:

- The number and locations of your service providers through which the traffic is forwarded in relationship to your branch offices and Microsoft Global Network peering points
- The quality of the network peering relationship of the service provider with your ISP and Microsoft
- The performance impact of backhauling in the service provider infrastructure

Whenever possible, configure your edge routers to send trusted Microsoft 365 traffic directly, instead of proxying or tunneling through a third-party cloud or cloud-based network security vendor that processes your Internet traffic.

As an interim checkpoint, you can see the [exit criteria](#) for this step.

Next step

4

[Configure traffic bypass](#)

Step 4: Configure traffic bypass

12/5/2018 • 2 minutes to read • [Edit Online](#)

This step is optional and applies to both the E3 and E5 versions of Microsoft 365 Enterprise



Because general Internet traffic can be risky, typical organization networks enforce security with edge devices such as proxy servers, SSL Break and Inspect, and packet inspection devices, and data loss prevention systems. Read about some of the issues with network interception devices at [Using third-party network devices or solutions on Office 365 traffic](#).

However, the DNS domain names and IP addresses used by Microsoft 365 cloud-based services are well known. Additionally, the traffic and services themselves are protected with many security features. Because this security and protection is already in place, your edge devices don't need to duplicate it. Intermediate destinations and duplicate security processing for Microsoft 365 traffic can dramatically decrease performance.

The first step in eliminating intermediate destinations and duplicate security processing is to identify Microsoft 365 traffic. Microsoft has defined the following types of DNS domain names and IP address ranges, known as endpoints:

- **Optimize** - Required for connectivity to every Office 365 service and represent over 75% of Microsoft 365 bandwidth, connections, and volume of data. These endpoints represent Microsoft 365 scenarios that are the most sensitive to network performance, latency and availability.
- **Allow** - Required for connectivity to specific Microsoft 365 services and features but are not as sensitive to network performance and latency as those in the Optimize category.
- **Default** - Represent Microsoft 365 services and dependencies that do not require any optimization. You can treat Default category endpoints as normal Internet traffic.

You can find the DNS domain names and IP address ranges at <https://aka.ms/o365endpoints>.

Microsoft recommends that you:

- Use Proxy Automatic Configuration (PAC) scripts on the Internet browsers of your on-premises computers to bypass your proxy servers for the DNS domain names of Microsoft 365 cloud-based services. For the latest Microsoft 365 PAC script, see the [Get-Pacfile PowerShell script](#).
- Analyze your edge devices to determine the duplicate processing and then configure them to forward traffic to Optimize and Allow endpoints without processing. This is known as traffic bypass.

Edge devices include firewalls, SSL Break and Inspect, and packet inspection devices, and data loss prevention systems. To configure and update the configurations of edge devices, you can use a script or a REST call to consume a structured list of endpoints from the Office 365 Endpoints web service. For more information, see [Office 365 IP Address and URL Web service](#).

Note that you are only bypassing normal proxy and network security processing for traffic to Microsoft 365 Optimize and Allow categories endpoints. All other general Internet traffic will be proxied and be subject to your existing network security processing.

As an interim checkpoint, you can see the [exit criteria](#) for this step.

Next step

5

Optimize client and Office 365 service performance

Step 5: Optimize client and Office 365 service performance

12/5/2018 • 2 minutes to read • [Edit Online](#)

This step is optional and applies to both the E3 and E5 versions of Microsoft 365 Enterprise



You can increase performance by fine tuning the way that the Transmission Control Protocol (TCP) works between client devices and Office 365 services.

For client devices, you can change the following TCP settings on client devices to optimize TCP performance:

- [TCP window scaling](#), so your client device can send more data before requiring an acknowledgement
- [TCP idle time](#), so your client device can handle open connections more efficiently
- [TCP maximum segment size](#), so your client device can send the largest blocks of data in a packet
- [TCP selective acknowledgements](#), so your client device can acknowledge received data more efficiently

For Office 365 services, see these additional resources to optimize performance:

- [Exchange Online](#)
- [Skype for Business Online](#)
- [SharePoint Online](#)
- [Project Online](#)

As an interim checkpoint, you can see the [exit criteria](#) for this step.

Next step

[Networking infrastructure exit criteria](#)

Phase 1: Networking infrastructure exit criteria

12/10/2018 • 2 minutes to read • [Edit Online](#)



If your networking infrastructure meets the following conditions, you're ready to move to Phase 2.

Required: Your network is ready for Microsoft 365 Enterprise

- Your offices have adequate Internet bandwidth for Microsoft 365 traffic, including Office 365, Microsoft Intune, and Windows 10 Enterprise installation and updates
- Your overall network maps to an Office 365 reference architecture
- Your network changes have been piloted and tested and meet with your traffic latency requirements

If needed, [Step 1](#) can help you with this requirement.

Required: Your local offices have local Internet connections and name resolution

You configured each local office with Internet access with a local ISP whose DNS servers use a local public IP address that identifies their location on the Internet. This ensures the best possible performance for users who access Office 365 and Intune.

If you don't use a local ISP for each branch office, performance can suffer because network traffic must traverse an organization's backbone or data requests are serviced by remote front-end servers.

How to test

Use a tool or web site from a device in that office to determine the public IP address that the proxy server is using. For example, use the [What Is My IP Address](#) web page. This public IP address assigned by your ISP should be geographically local. It should not be from a public IP address range for a central office or from a cloud-based network security vendor.

If needed, [Step 2](#) can help you with this requirement.

Optional: Unneeded network hairpins are removed

You examined your network hairpins and determined their impact on performance for all of your offices. You removed network hairpins where possible or worked with your third-party network or security provider to implement optimal Microsoft 365 peering for their network.

If needed, [Step 3](#) can help you with this option.

Optional: You have configured traffic bypass on your Internet browsers and edge devices

You deployed the latest PAC files to your on-premises Internet browsers so that traffic to Microsoft 365 DNS domain names bypass proxy servers.

You configured your network perimeter devices—such as firewalls, and SSL Break and Inspect, and packet

inspection devices—to use traffic bypass or to minimally process traffic to the Optimize and Allow categories of Microsoft 365 endpoints.

How to test

Use the logging tools on your network perimeter devices to ensure that traffic to Microsoft 365 destinations isn't being inspected, decrypted, or otherwise hindered.

If needed, [Step 4](#) can help you with this option.

Optional: Your clients and Office 365 applications are configured for optimal performance

You have optimized the Transmission Control Protocol (TCP) settings on your client devices and for Exchange Online, Skype for Business Online, SharePoint Online, and Project Online services.

If needed, [Step 5](#) can help you with this option.

Next phase



Your next phase in the end-to-end deployment process for Microsoft 365 Enterprise is [identity](#).

Phase 2: Identity

2/26/2019 • 2 minutes to read • [Edit Online](#)



In Microsoft 365 Enterprise, a well-planned and executed identity infrastructure paves the way for stronger security and access to your productivity workloads and their data only by authenticated users and devices.

NOTE

If you've already deployed an identity infrastructure, please see the [identity exit criteria](#) to make sure that you meet the required and optional conditions for Microsoft 365 Enterprise.

Plan and deploy your Microsoft 365 Enterprise identity infrastructure

Use the following steps to plan and deploy your new identity infrastructure in the cloud. You can also use these steps to adapt your existing on-premises or hybrid identity infrastructure to work with Microsoft 365 Enterprise.

1	Plan for users and groups
2	Secure your privileged identities
3	Configure hybrid identity
4	Configure secure user authentication
5	Simplify access for users
6	Use groups for easier management

When you've completed these steps, go to the [exit criteria](#) for this phase to ensure that you meet the required and optional conditions for Microsoft 365 Enterprise.

Identity and device access recommendations

Microsoft provides a set of recommendations for [identity and device access](#) to ensure a secure and productive workforce. For identity, use the recommendations and settings in the following articles along with the steps in this phase:

- [Prerequisites](#)
- [Common identity and device access policies](#)

How Microsoft does Microsoft 365 Enterprise

Learn how IT experts at Microsoft planned for and deployed the identity capabilities of Microsoft 365 Enterprise with these resources:

- [Managing user identities and secure access at Microsoft](#)
- [Using Azure AD Privileged Identity Management for elevated access](#)

How Contoso did Microsoft 365 Enterprise

See how the Contoso Corporation, a fictional but representative multi-national business, [deployed a hybrid identity infrastructure](#) for Microsoft 365 cloud services.



Next step

1	Plan for users and groups
---	---

Step 1: Plan for users and groups

2/26/2019 • 3 minutes to read • [Edit Online](#)

This step is required and applies to both the E3 and E5 versions of Microsoft 365 Enterprise



In this step, you'll create your identity infrastructure that combines users, groups, and group membership with security features in the correct configuration. This allows you to:

- Maintain control over who has access to resources in your environment.
- Secure access with controls that ensure strong assurances of identity (users are who they say they are) and access from safe devices.
- Provision resources in your environment with appropriate permissions to reduce the potential for harm and data leakage.
- Monitor your environment for anomalous user behavior and automatically taking action.

Plan your primary identity provider

To create your identity infrastructure, you'll designate a primary identity provider. This service stores user accounts and their attributes, groups and their memberships, and supports their ongoing administration.

When your organization adopts Microsoft 365 Enterprise, your primary identity provider is either:

- **Active Directory Domain Services (AD DS)**, an intranet identity provider hosted on computers running Windows Server. This is typically used by organizations that have an existing on-premises identity provider.
- **Azure Active Directory (Azure AD)**, a cloud-based Identity as a Service (IDaaS) that provides a broad range of capabilities for managing and protecting your environment. This is typically used by organizations that have no existing on-premises infrastructure.

If your organization has an existing on-premises identity provider, you need to synchronize your user accounts and groups from Windows Server AD to Azure AD to provide more seamless access to the cloud-based services of Microsoft 365 Enterprise. You can also use Azure AD to create and manage groups that exist only in the Microsoft cloud.

After you have your users and groups in Azure AD, you can:

- Manage all the Azure AD accounts for all your cloud applications.
- Use the same set of controls to protect access to applications across your environment.
- Collaborate with external partners.
- Monitor anomalous account behavior, such as suspicious sign-in attempts, and automatically act.

Follow the instructions in the next two sections to plan for and implement your user accounts and groups.

Categorize your users

Users in organizations can be categorized in a number of ways. For example, some are employees and have a permanent status. Some are vendors, contractors, or partners that have a temporary status. Some are external users that have no user accounts but must still be granted access to specific services and resources to support interaction and collaboration. For example:

- Tenant accounts represent users within your organization that you license for cloud services
- Business to Business (B2B) accounts represent users outside your organization that you invite to participate in collaboration

Take stock of the types of users to your organization. What are the groupings? For example, you can group users by high-level function or purpose to your organization.

Additionally, some cloud services can be shared with users outside your organization without any user accounts. You'll need to identify these groups of users as well.

Plan for Windows Server AD and Azure AD groups

You can use groups in Azure AD for several purposes that simplify management of your cloud environment. For example, for Azure AD groups, you can:

- Use group-based licensing to assign licenses for Office 365 and Enterprise Mobility + Security (EMS) to your user accounts automatically as soon as they are added in Azure AD or synchronized from Windows Server AD.
- Add user accounts to specific groups dynamically based on user account attributes, such as department.
- Automatically provision users for Software as a Service (SaaS) applications and to protect access to those applications with multi-factor authentication and other conditional access rules.
- Provision permissions and levels of access for SharePoint Online team sites. Azure AD groups can also be used with scoped Azure Information Protection policies to protect files with encryption and permissions.

Results

When you complete this step, you'll have:

- A list of user accounts in Azure AD that correspond to the employees in your organization and the vendors, contractors, and external partners that work for or with your organization.
- A set of groups and their membership in Azure AD that reflect logical sets of user accounts and other groups for automatic licensing provisioning of security settings for Microsoft cloud services.

As an interim checkpoint, you can see the [exit criteria](#) for this step.

Once your Azure AD users and groups are created, you can start assigning licenses and using Exchange Online. To roll out Exchange Online to your users, see [Deploy Exchange Online for Microsoft 365 Enterprise](#).

Next step

2

[Secure your privileged identities](#)

Step 2: Secure your privileged identities

2/26/2019 • 2 minutes to read • [Edit Online](#)



Protect global administrator accounts

This is required and applies to both the E3 and E5 versions of Microsoft 365 Enterprise

In this section, you'll help prevent digital attacks on your organization by ensuring that your administrator accounts are as secure as possible. To do this, you must:

- Create dedicated global administrator accounts with very [strong passwords](#) and use them only when necessary.
- Perform day-to-day administration by assigning specific administrator roles—such as Exchange administrator or Password administrator—to user accounts of IT staff as needed.

For your dedicated global admin accounts, you must also:

1. Test per-user account or conditional access-based multi-factor authentication (MFA) settings on a test user account to ensure that MFA works correctly and predictably. MFA requires a secondary form of authentication, such as a verification code sent to a smart phone.
2. Configure MFA for each of the dedicated Office 365 global administrator accounts, and use the strongest form of secondary authentication available in your organization. See [Multi-factor authentication](#) for more information.
3. Use a conditional access policy to require MFA for global administrator accounts. See [Protecting administrator accounts](#) for more information.
4. Use an Office 365 Cloud App Security policy to monitor global administrator account activity. See [Configure increased security for Office 365](#) for more information.

See [Protect your Office 365 global administrator accounts](#) for more information about configuration.

NOTE

Organizations should use cloud-only identities to create privileged accounts, such as global administrators, for break-glass scenarios in emergencies, such as a cyberattack. For more information, see [Manage emergency-access administrative accounts in Azure AD](#).

The results of this section are:

- The only user accounts in your subscription that have the global admin role are the new set of dedicated global administrator accounts. Verify this with the following Azure Active Directory PowerShell for Graph command:

```
Get-AzureADDirectoryRole | Where { $_.DisplayName -eq "Company Administrator" } | Get-AzureADDirectoryRoleMember | Ft DisplayName
```

- All other everyday user accounts that manage your subscription have admin roles assigned that are associated with their job responsibilities.

NOTE

See [Connect to Office 365 PowerShell](#) for instructions on installing the Azure Active Directory PowerShell for Graph module and signing in.

**Test Lab Guide: Protect global administrator accounts**

As an interim checkpoint, you can see the [exit criteria](#) for this section.

Set up on-demand global administrators

This is optional and applies only to the E5 version of Microsoft 365 Enterprise

In this section, you'll set up Azure AD Privileged Identity Management (PIM) to reduce the amount of time that your global administrator accounts are vulnerable to attack by malicious users. PIM provides on-demand, just-in-time assignment of the global administrator role when needed.

Instead of your global administrator accounts being a permanent admin, they become eligible admins. The global administrator role is inactive until someone needs it. You'll then complete an activation process to add the global administrator role to the global administrator account for a specific amount of time. When the time expires, PIM removes the global administrator role from the global administrator account.

PIM is available with Azure Active Directory Premium P2, which is included with Microsoft 365 Enterprise E5. Alternately, you can purchase individual Azure Active Directory Premium P2 licenses for your global administrator accounts.

To enable Azure PIM for your Azure AD tenant and global administrator accounts, see the [steps to configure PIM](#).

To develop a comprehensive roadmap to secure privileged access against cyber attackers, see [Securing privileged access for hybrid and cloud deployments in Azure AD](#).

As an interim checkpoint, you can see the [exit criteria](#) for this section.

Next step

3

[Configure hybrid identity](#)

Step 3: Configure hybrid identity

2/26/2019 • 3 minutes to read • [Edit Online](#)

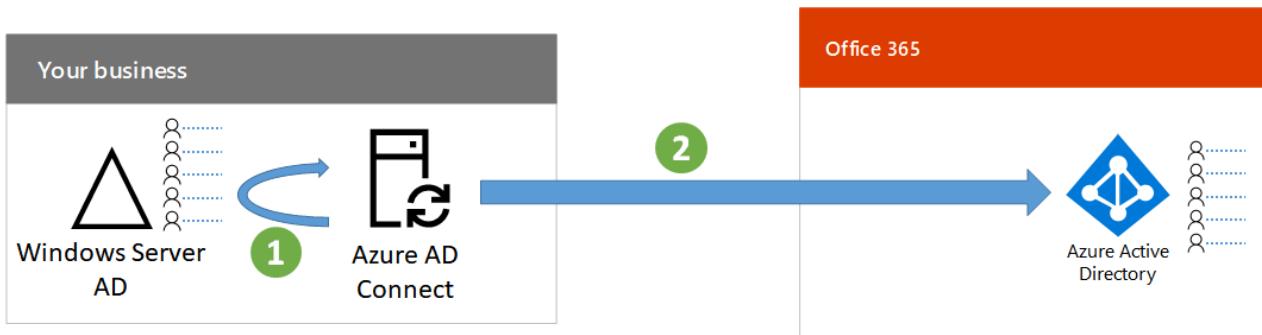


Synchronize identities

This is required for hybrid environments and applies to both the E3 and E5 versions of Microsoft 365 Enterprise

In this section, you'll synchronize your on-premises Active Directory Domain Services (AD DS) with the Azure Active Directory (Azure AD) tenant used by your Office 365 and Enterprise Mobility + Security (EMS) subscriptions.

Azure AD Connect is the supported Microsoft tool that guides you through synchronizing only the identities you really need from single or multi-forest Windows Server AD environments to your Azure AD tenant.



The first decision in your hybrid identity solution is your authentication requirement. The following options are options:

- With **managed authentication**, Azure AD handles the authentication process for user sign-in. There are two methods for managed authentication:
 - Password Hash Sync (PHS)** [Recommended and required for some premium features]. This is the simplest way to enable authentication for on-premises directory objects in Azure AD. Azure AD Connect extracts the hashed password from Windows Server AD, does extra security processing on the password, and saves it in Azure AD. For more information, see [Implement password hash synchronization with Azure AD Connect sync](#).
 - Pass-through Authentication (PTA)** provides a simple password validation solution for Azure AD-based services. PTA uses an agent running on one or more on-premises servers to validate the user authentications directly with your on-premises Windows Server AD. For more information, see [User sign-in with Azure Active Directory Pass-through Authentication](#).
- With **federated authentication**, the authentication process is redirected to another identity provider through an identity federation server, such as Active Directory Federation Services (AD FS), for a user's sign-in. The identity provider can provide additional authentication methods, such as smartcard-based authentication. For more information, see [Choosing the right authentication method for your Azure Active Directory hybrid identity solution](#).

After you've determined your hybrid identity solution, download and run the [IdFix Directory Synchronization Error Remediation Tool](#) to analyze your Windows Server AD for issues.

After resolving all of the issues identified by the IdFix tool, see [Implement password hash synchronization](#) for guidance on installing the Azure AD Connect tool and configuring directory synchronization between your on-premises Windows Server AD and the Azure AD tenant for your Office 365 and EMS subscriptions. After synchronization starts, you'll maintain your user accounts and groups with your on-premises identity provider, such as Windows Server AD.

Microsoft provides a set of recommendations for [identity and device access](#) to ensure a secure and productive workforce.

- For recommended requirements for hybrid environments, see the **Active Directory with password hash sync** column in [prerequisites](#).
- For recommended requirements for cloud only environments, see the **Cloud only** column in [prerequisites](#).

Once your on-premises users and groups are present in Azure AD, you can start assigning licenses and using Exchange Online. To roll out Exchange Online to your users and migrate on-premises mailboxes, see [Deploy Exchange Online for Microsoft 365 Enterprise](#).

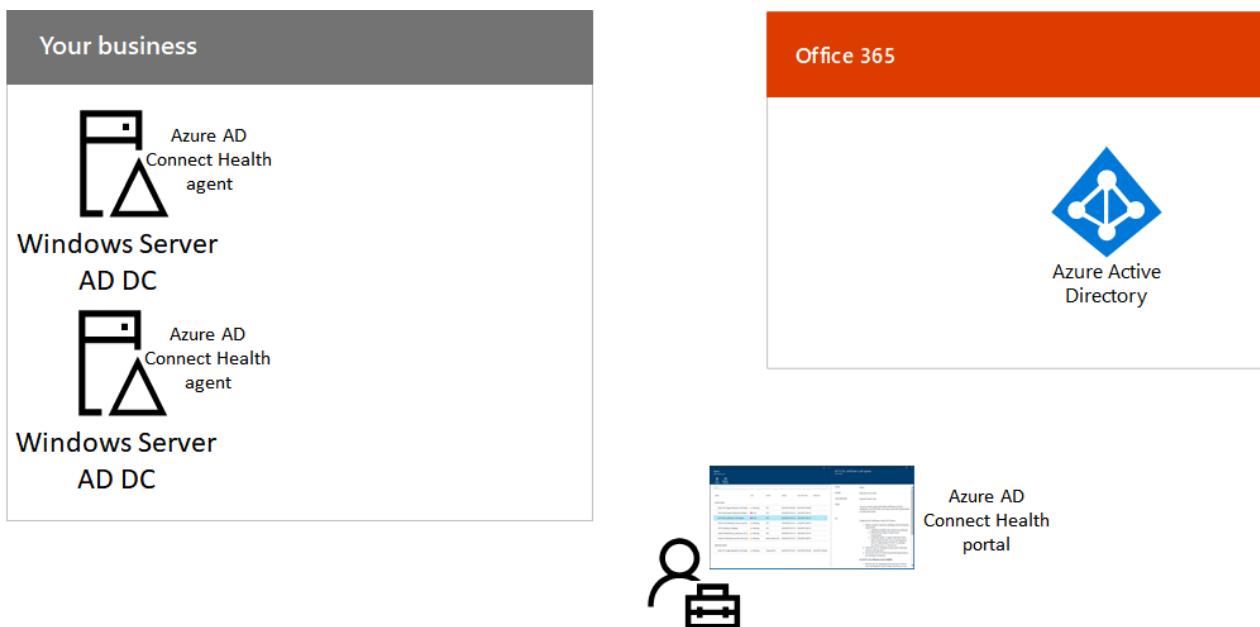
	Test Lab Guide: Password hash synchronization Test Lab Guide: Pass-through authentication
---	--

As an interim checkpoint, you can see the [exit criteria](#) corresponding to this section.

Monitor synchronization health

This is optional and applies to both the E3 and E5 versions of Microsoft 365 Enterprise

In this section, you'll install an Azure AD Connect Health agent on each of your on-premises identity servers to monitor your identity infrastructure and the synchronization services provided by Azure AD Connect. The monitoring information is made available in an Azure AD Connect Health portal, where you can view alerts, performance monitoring, usage analytics, and other information.



The key design decision of how to use Azure AD Connect Health is based on how you are using Azure AD Connect:

- If you're using the **managed authentication** option, start with [Using Azure AD Connect Health with sync to](#)

understand and configure Azure AD Connect Health.

- If you're synchronizing just the names of the accounts and groups using **federated authentication** with Active Directory Federation Services (AD FS), start with [Using Azure AD Connect Health with AD FS](#) to understand and configure Azure AD Connect Health.

When you complete this section, you'll have:

- The Azure AD Connect Health agent installed on your on-premises identity provider servers.
- The Azure AD Connect Health portal displaying the current state of your on-premises infrastructure and synchronization activities with the Azure AD tenant for your Office 365 and EMS subscriptions.

As an interim checkpoint, you can see the [exit criteria](#) for this section.

Next step

4

[Configure secure user authentication](#)

Step 4: Configure secure user authentication

2/26/2019 • 4 minutes to read • [Edit Online](#)



Set up multi-factor authentication

This is optional and applies to both the E3 and E5 versions of Microsoft 365 Enterprise

In this step, you'll set up multi-factor authentication (MFA) to add a second layer of security to user sign-ins and transactions. MFA requires an additional verification method after users have correctly entered their password. Without MFA, the password is the only verification method. The problem with passwords is that many of them are easily guessed by an attacker or unknowingly shared with untrusted parties.

With MFA, the second layer of security can be:

- A personal and trusted device that isn't easily spoofed or duplicated, such as a smart phone.
- A biometric attribute, such as a fingerprint.

You'll enable MFA and configure the secondary authentication method on a per-user account basis. Make sure to let users know that MFA is being enabled so they understand the requirements, such as mandatory use of a smart phone to sign in, and can sign in successfully.

For more information, see [Plan for multi-factor authentication for Office 365 Deployments](#).

To configure multifactor authentication, [Set up multi-factor authentication for Office 365 users](#).

You can require MFA with conditional access policies. For example, you can configure a policy that requires MFA when the authentication is determined to be of medium or high risk. For more information, see [Common identity and device access policies](#).

NOTE

In some applications, such as Microsoft Office 2010 or older and Apple Mail, you can't use MFA. To use these apps, you'll need to use "app passwords" in place of your traditional password. The app password allows the app to bypass MFA and continue working. To learn more about app passwords, see [Create an app password for Office 365](#).



[Test Lab Guide: Multi-factor authentication](#)

As an interim checkpoint, you can see the [exit criteria](#) for this section.

Protect against credential compromise

This is optional and applies only to the E5 version of Microsoft 365 Enterprise

In this section, you'll learn how to configure policies that protect against credential compromise, where an attacker

determines a user's account name and password to gain access to an organization's cloud services and data. Azure AD Identity Protection provides a number of ways to help prevent an attacker from moving laterally through your accounts and groups, and subsequently, to your most valuable data.

With Azure AD Identity Protection, you can:

Determine and address potential vulnerabilities in your organization's identities	Azure AD uses machine learning to detect anomalies and suspicious activity, such as sign-ins and post-sign-in activities. Using this data, Identity Protection generates reports and alerts that help you evaluate the issues and take action.
Detect suspicious actions that are related to your organization's identities and respond to them automatically	You can configure risk-based policies that automatically respond to detected issues when a specified risk level has been reached. These policies, in addition to other conditional access controls provided by Azure Active Directory and Enterprise Mobility + Security (EMS), can either automatically block access or take corrective actions, including password resets and requiring multi-factor authentication for subsequent sign-ins.
Investigate suspicious incidents and resolve them with administrative actions	You can investigate risk events using information about the security incident. Basic workflows are available to track investigations and initiate remediation actions, such as password resets.

See [more information about Azure AD Identity Protection](#).

See the [steps to enable Azure AD Identity Protection](#).

The results of this step are that you've enabled Azure AD Identity protection and you are using it to:

- Address potential identity vulnerabilities.
- Detect possible credential compromise attempts.
- Investigate and address ongoing suspicious identity incidents.

	Test Lab Guide: Azure AD Identity Protection
---	--

As an interim checkpoint, you can see the [exit criteria](#) for this section.

Monitor tenant and sign-in activity

This is optional and applies to both the E3 and E5 versions of Microsoft 365 Enterprise

In this step, you'll review audit logs and sign-in activity using Azure AD reporting. Two types of reports are available.

The **Audit logs activity report** records the history of every task performed in your Azure AD tenant. This report answers questions like:

- Who added someone to an admin group?
- Which users are signing into a specific app?
- How many password resets are happening?

The **Sign-ins activity report** records who performed the tasks reported by the audit logs report. This report answers questions like:

- For a specific user under investigation, what is their sign-in pattern?
- What is my volume of sign-ins over a day, week, or month?
- How many of these sign-in attempts were not successful, and for which accounts?

For more information about the reports and how to access them, see [Azure Active Directory reporting](#).

As a result of this step, you'll gain awareness of these reports and an understanding of how you can use them to gain insights on Azure AD events and activities for planning and security purposes.

Next step

5

[Simplify access for users](#)

Step 5: Simplify access for users

2/26/2019 • 2 minutes to read • [Edit Online](#)



Simplify password resets

This is optional and applies to both the E3 and E5 versions of Microsoft 365 Enterprise

In this section, you'll enable self-service password reset (SSPR) to allow users to reset or unlock their passwords or accounts. To alert you to misuse or abuse, you can use the detailed reporting that tracks when users access the system, along with notifications.

See the [instructions to enable password reset](#).



[Test Lab Guide: Password reset](#)

As an interim checkpoint, you can see the [exit criteria](#) for this section.

Simplify password updates

This is optional for hybrid environments and applies to both the E3 and E5 versions of Microsoft 365 Enterprise

In this section, you'll allow users to reset their passwords through Azure Active Directory (Azure AD), which is then replicated to your local Active Directory Domain Services (AD DS). This process is known as password writeback. With password writeback, users don't need to update their passwords through the on-premises Windows Server AD where user accounts and their attributes are stored. This is valuable to roaming or remote users who do not have a remote access connection to the on-premises network.

Password writeback is required to fully utilize Identity Protection feature capabilities, such as requiring users to change their on-premises passwords when there has been a high risk of account compromise detected.

For additional information and configuration instructions, see [Azure AD SSPR with password writeback](#).

NOTE

Upgrade to the latest version of Azure AD Connect to ensure the best possible experience and new features as they are released. For more information, see [Custom installation of Azure AD Connect](#).



[Test Lab Guide: Password writeback](#)

As an interim checkpoint, you can see the [exit criteria](#) for this section.

Simplify user sign-in

This is optional for hybrid environments and applies to both the E3 and E5 versions of Microsoft 365 Enterprise

In this section, you'll set up Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) to allow your users to sign in to services that use Azure AD user accounts without having to type in their passwords, and in many cases, their usernames. This gives your users easier access to cloud-based applications, such as Office 365, without needing any additional on-premises components such as identity federation servers.

You'll configure Azure AD Seamless SSO with the Azure AD Connect tool.

See the [instructions to configure Azure AD Seamless SSO](#).

	Test Lab Guide: Azure AD Seamless Single Sign-on
---	--

As an interim checkpoint, you can see the [exit criteria](#) for this section.

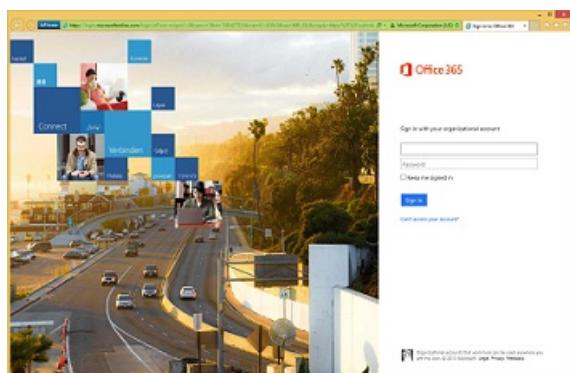
Customize the Office 365 sign-in page

This is optional and for both the E3 and E5 versions of Microsoft 365 Enterprise

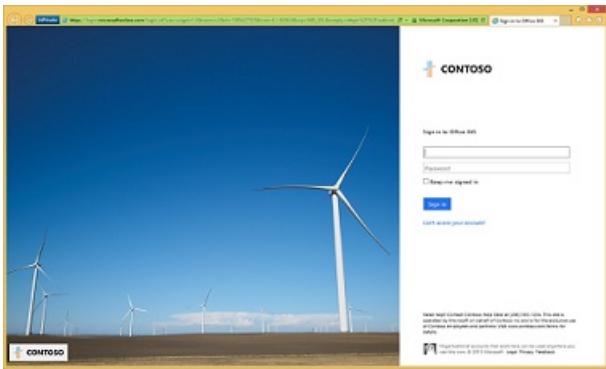
In this section, you'll help users recognize your organization's sign-in page by adding your company name, logo, and other recognizable elements.

With Microsoft 365 Enterprise, you can customize the appearance of the sign-in and Access Panel pages so they include your company logo, color schemes, and custom user information.

When a user attempts to sign in from a device, they see something like the following example on the Office 365 sign-in page *before customization*.



And here is what the same user of the Contoso Corporation would see *after customization*.



For more information, see [Add your company branding to Office 365 Sign In page](#).

For configuration instructions, see [Add company branding to your sign-in and Access Panel pages](#).

As an interim checkpoint, you can see the [exit criteria](#) for this section.

Next step

6

[Use groups for easier management](#)

Step 6: Use groups for easier management

2/26/2019 • 3 minutes to read • [Edit Online](#)

Allow users to create and manage their own groups

This is optional and applies to both the E3 and E5 versions of Microsoft 365 Enterprise

In this section, you'll identify Azure Active Directory (Azure AD) groups that can be managed by group owners instead of IT administrators. Known as *self-service group management*, this feature allows group owners who are not assigned an administrative role to create and manage security groups.

Users can request membership in a security group and that request goes to the group owner, rather than an IT administrator. This allows the day-to-day control of group membership to be delegated to team, project, or business owners who understand the business use for the group and can manage its membership.

NOTE

Self-service group management is available only for Azure AD security and Office 365 groups. It is not available for mail-enabled groups, distribution lists, or any group that has been synchronized from your on-premises Active Directory Domain Services (AD DS).

For more information, see the [instructions to configure an Azure AD group for self-service management](#).

As an interim checkpoint, you can see the [exit criteria](#) for this section.

Set up dynamic group membership

This is optional and applies to both the E3 and E5 versions of Microsoft 365 Enterprise

In this section, you'll create a series of rules that automatically add or remove user accounts as members of an Azure AD group. This is known as *dynamic group membership*. The rules are based on user account attributes, such as Department or Country.

Here's how the rules are applied:

- If a new user account matches all the rules for the group, it becomes a member.
- If a user account isn't a member of the group, but its attributes change so that it matches all the rules for the group, it becomes a member of that group.
- If a user account doesn't match all the rules for the group, it isn't added to the group.
- If a user account is a member of the group, but its attributes change so that it no longer matches all the rules for the group, it is removed as a member of the group.

To use dynamic membership, you must first determine the sets of groups that have a common set of user account attributes. For example, all members of the Sales department should be in the Sales Azure AD group, based on the user account attribute Department set to "Sales".

See the [instructions to create and configure the rules for a dynamic Azure AD group](#).

The results of this section are:

- A set of Azure AD groups that can be configured for dynamic membership
- A set of rules on each dynamic group



As an interim checkpoint, you can see the [exit criteria](#) for this section.

Set up automatic licensing

This is optional and applies to both the E3 and E5 versions of Microsoft 365 Enterprise

In this section, you'll configure security groups in Azure AD to automatically assign licenses from a set of subscriptions to all the members of the group. This is known as *group-based licensing*. If a user account is added to or removed from the group, the licenses for the group's subscriptions will be automatically assigned or removed from the user account.

For Microsoft 365 Enterprise, you'll configure Azure AD security groups to assign both of these licenses:

- Office 365 Enterprise E3 or E5
- Enterprise Mobility + Security (EMS) E3 or E5

Using the groups you identified in Step 2, look for groups that contain a list of accounts where all users in that group must have both Office 365 and EMS licenses. Make sure you have enough licenses for all the group members. If you run out of licenses, new users won't be assigned licenses until licenses become available.

NOTE

You should not configure *group-based licensing* for groups that contain Azure business to business (B2B) accounts.

See additional information on [Group-based licensing basics in Azure Active Directory](#).

See the [steps to configure group-based licensing for an Azure security group](#).

The results of this section are:

- You've identified which security groups are appropriate for group-based licensing.
- You've configured these groups for group-based licensing.



As an interim checkpoint, you can see the [exit criteria](#) for this section.

Next step

[Identity infrastructure exit criteria](#)

Phase 2: Identity infrastructure exit criteria

2/26/2019 • 10 minutes to read • [Edit Online](#)



Before you move on to Phase 3, make sure that your identity infrastructure meets these conditions. Also see [Prerequisites](#) for additional recommendations on identity infrastructure.

Required: All users, groups, and group memberships have been created

You've created user accounts and groups so that:

- Employees in your organization and the vendors, contractors, and partners that work for or with your organization have a corresponding user account in Azure Active Directory (Azure AD).
- Azure AD groups and their members contain user accounts and other groups for various purposes, such as the provisioning of security settings for Microsoft cloud services, automatic licensing, and other uses.

If needed, [Step 1](#) can help you meet this requirement.

Required: Your global administrator accounts are protected

You've [protected your Office 365 global administrator accounts](#) to avoid compromising credentials that can lead to breaches of an Office 365 subscription.

If you skip this requirement, your global administrator accounts can be susceptible to attack and compromise, allowing an attacker to gain system-wide access to your data for harvesting, destruction, or ransom.

If needed, [Step 2](#) can help you meet this requirement.

How to test

Use these steps to verify that you've protected your global administrator accounts:

1. Run the following Azure AD V2 command at the PowerShell command prompt. You should see only the list of dedicated global administrator accounts.

```
Get-AzureADDirectoryRole | where { $_.DisplayName -eq "Company Administrator" } | Get-AzureADDirectoryRoleMember | Ft DisplayName
```

2. Sign in to Office 365 using each of the accounts from step 1. Each sign in must require multi-factor authentication and the strongest form of secondary authentication available in your organization.

NOTE

See [Connect to Office 365 PowerShell](#) for instructions on installing the Azure Active Directory PowerShell for Graph module and signing in to Office 365.

Optional: You have set up Privileged Identity Management to support

on-demand assignment of the global administrator role

You've used the instructions in [Configure Azure AD Privileged Identity Management](#) to enable PIM in your Azure AD tenant and configured your global administrator accounts as eligible admins.

You've also used the recommendations in [Securing privileged access for hybrid and cloud deployments in Azure AD](#) to develop a roadmap that secures privileged access against cyber attackers.

If you skip this option, your global administrator accounts are subject to ongoing online attack and, if compromised, can allow an attacker to harvest, destroy, or hold your sensitive information for ransom.

If needed, [Step 2](#) can help you with this option.

Required: Users and groups are synchronized with Azure AD

If you have an existing on-premises identity provider, such as Active Directory Domain Services (AD DS), you have used Azure AD Connect to synchronize user accounts and groups from your on-premises identity provider to your Azure AD tenant.

With directory synchronization, your users can sign in to Office 365 and other Microsoft cloud services using the same credentials that they use to sign in to their computers and access on-premises resources.

If needed, [Step 3](#) can help you meet this requirement.

If you skip this requirement, you'll have two sets of user accounts and groups:

- User accounts and groups that exist in your on-premises identity provider
- User accounts and groups that exist in your Azure AD tenant

In this state, the two sets of user accounts and groups must be manually maintained by both IT administrators and users. This will inevitably lead to unsynchronized accounts, their passwords, and groups.

How to test

To verify that authentication with on-premises credentials works correctly, sign in to the Office portal with your on-premises credentials.

To verify that directory synchronization is working correctly, do the following:

1. Create a new test group in Windows Server AD.
2. Wait for the synchronization time.
3. Check your Azure AD tenant to verify that the new test group name appears.

Optional: Directory synchronization is monitored

You've used [Azure AD Connect Health with sync](#) (for password synchronization) or [Using Azure AD Connect Health with AD FS](#) (for federated authentication) and have deployed Azure AD Connect Health, which involves:

- Installing the Azure AD Connect Health agent on each of your on-premises identity servers.
- Using the Azure AD Connect Health portal to monitor the state of the ongoing synchronization.

If you skip this option, you can more accurately assess the state of your cloud-based identity infrastructure.

If needed, [Step 3](#) can help you with this option.

How to test

The Azure AD Connect Health portal shows the current and correct state of your on-premises identity servers and the ongoing synchronization.

Optional: Multi-factor authentication is enabled for your users

You used [Plan for multi-factor authentication for Office 365 Deployments](#) and [Set up multi-factor authentication for Office 365 users](#) to enable multifactor authentication (MFA) for your user accounts.

If you skip this option, your user accounts are vulnerable to credential compromise by cyber attackers. If a user account's password is compromised, all the resources and capabilities of the account, such as administrator roles, are available to the attacker. This allows the attacker to copy, destroy, or hold for ransom internal documents and other data.

If needed, [Step 4](#) can help you with this option.

How to test

1. Create a test user account in the Office 365 Admin portal and assign them a license.
2. Configure multi-factor authentication for the test user account with the additional verification method that you are using for actual user accounts, such as sending a message to your phone.
3. Sign in to the Office 365 or Azure portal with the test user account.
4. Verify that MFA prompts you for the additional verification information and results in a successful authentication.
5. Delete the test user account.

Optional: Azure AD Identity Protection is enabled to protect against credential compromise

You've enabled Azure AD Identity Protection to:

- Address potential identity vulnerabilities.
- Detect possible credential compromise attempts.
- Investigate and address ongoing suspicious identity incidents.

If you skip this option, you won't be able to detect or automatically thwart credential compromise attempts or investigate identity-related security incidents. This potentially leaves your organization vulnerable to a successful credential compromise and the resulting threat to your organization's sensitive data.

If needed, [Step 4](#) can help you with this option.

Optional: Users can reset their own passwords

You've used [Azure AD self-service password reset rapid deployment](#) to configure password reset for your users.

If you don't meet this condition, users will be dependent on user account administrators to reset their passwords, resulting in additional IT administration overhead.

If needed, [Step 5](#) can help you with this option.

How to test

1. Create a test user account with an initial password.
2. Use the steps in [Let users reset their own passwords in Office 365](#) to reset the password on the test user account.
3. Sign out and then sign in to the test user account using the reset password.
4. Delete the test user account.

Optional: Password writeback is enabled for your users

You've used the instructions in [Azure AD SSPR with password writeback](#) to enable password writeback for the

Azure AD tenant of your Microsoft 365 Enterprise subscription.

If you skip this option, users who aren't connected to your on-premises network must reset or unlock their Windows Server AD passwords through an IT administrator.

If needed, [Step 5](#) can help you with this option.

NOTE

Password writeback is required to fully utilize Azure AD Identity Protection features, such as requiring users to change their on-premises passwords when Azure AD has detected a high risk of account compromise.

How to test

You test password writeback by changing your password in Office 365. You should be able to use your account and new password to access on-premises Windows Server AD resources.

1. Create a test user account in your on-premises Windows Server AD, allow directory synchronization to occur, and then grant it an Office 365 license in the Office 365 admin portal.
2. From a remote computer that is joined to your on-premises Windows Server AD domain, sign in to the computer and the Office portal using the credentials of the test user account.
3. Select **Settings > Office 365 settings > Password > Change password**.
4. Type the current password, type a new password, and then confirm it.
5. Sign out of the Office portal and the remote computer and then sign in to the computer using the test user account and its new password. This proves that you were able to change the password of an on-premises Windows Server AD user account using the Azure AD tenant.

Optional: Users can sign in using Azure AD Seamless Single Sign-on

You enabled [Azure AD Connect: Seamless Single Sign-On](#) for your organization to simplify how users sign in to cloud-based applications, such as Office 365.

If you skip this option, your users might be prompted to provide credentials when they access additional applications that use Azure AD.

If needed, [Step 5](#) can help you with this option.

Optional: The Office 365 sign-in screen is personalized for your organization

You have used [Add company branding to your sign-in and Access Panel pages](#) to add your organization's branding to the Office 365 sign-in page.

If you skip this option, your users will see a generic Office 365 sign-in screen and might not be confident that they're signing into your organization's site.

If needed, [Step 5](#) can help you with this option.

How to test

Sign in to the Office portal with your user account name and multi-factor authentication. You should see your custom branding elements on the sign-in page.

Optional: Self-service group management is enabled for specific Azure AD security and Office 365 groups

You've determined which groups are appropriate for self-service management, instructed their owners on group

management workflow and responsibilities, and [set up self-service management in Azure AD](#) for those groups.

If you skip this option, all Azure AD group management tasks must be done by IT administrators.

If needed, [Step 6](#) can help you with this option.

How to test

1. Create a test user account in Azure AD with the Azure portal.
2. Sign-in as with the test user account and create a test Azure AD security group.
3. Sign out and then sign-in with your IT administrator account.
4. Configure the test security group for self-service management for the test user account.
5. Sign out and then sign-in with your test user account.
6. Use the Azure portal to add members to the test security group.
7. Delete the test security group and the test user account.

Optional: Dynamic group membership settings automatically add user accounts to groups based on user account attributes

You've determined the set of Azure AD dynamic groups and used the instructions in [Attribute-based dynamic group membership in Azure Active Directory](#) to create the groups and the rules that determine the set of user account attributes and values for group membership.

If you skip this option, group membership must be done manually as new accounts are added or as user account attributes change over time. For example, if someone moves from the Sales department to the Accounting department, you must:

- Update the value of the Department attribute for that user account.
- Manually remove them from the Sales group.
- Manually add them to the Accounting group.

If the Sales and Accounting groups were dynamic, you would only have to change the user account's Department value.

If needed, [Step 6](#) can help you with this option.

How to test

1. Create a test dynamic group in Azure AD with the Azure portal and configure a rule for the Department equals "test1".
2. Create a test user account in Azure AD and set the Department property to "test1".
3. Examine the properties of the user account to ensure that it was made a member of the test dynamic group.
4. Change the value of the Department property for the test user account to "test2".
5. Examine the properties of the user account to ensure that it is no longer a member of the test dynamic group.
6. Delete the test dynamic group and the test user account.

Optional: Group-based licensing to automatically assign and remove licenses to user accounts based on group membership

You [enabled group-based licensing](#) for the appropriate Azure AD security groups so that licenses for both Office 365 and EMS are automatically assigned or removed.

If you skip this option, you must manually:

- Assign licenses to new users whom you intend to have access to Office 365 and EMS.
- Remove licenses from users who are no longer with your organization or do not have access to Office 365 and

EMS.

If needed, [Step 6](#) can help you with this option.

How to test

1. Create a test security group in Azure AD with the Azure portal and configure group-based licensing to assign Office 365 and EMS licenses.
2. Create a test user account in Azure AD and add it to the test security group.
3. Examine the properties of the user account in the Office 365 admin portal to ensure that it was assigned the Office 365 and EMS licenses.
4. Remove the test user account from the test security group.
5. Examine the properties of the user account to ensure that it no longer has the Office 365 and EMS licenses assigned.
6. Delete the test security group and the test user account.

Next phase



Your next phase in the end-to-end deployment process for Microsoft 365 Enterprise is [Windows 10 Enterprise](#).

Phase 3: Windows 10 Enterprise

12/5/2018 • 4 minutes to read • [Edit Online](#)



Microsoft 365 Enterprise includes Windows 10 Enterprise, which gives you the tools to do more and stay secure. Windows 10 Enterprise:

- **Is integrated for simplicity** - Harness the power of the cloud to help reduce the complexity of managing today's modern IT device environment, no matter the size.
- **Has intelligent security** - It's the most secure release of Windows ever, with intelligent security capabilities that are designed to work together to better protect your organization.
- **Enables creativity and teamwork** - Unlocks creativity and teamwork to deliver the most productive experience that both users and IT will love.

You'll need to understand the different ways you can deploy the Windows 10 operating system and choose the right one for your organization. Depending on your Microsoft 365 Enterprise subscription, there are also Windows 10 services and security features that you'll need to configure to get the most out of Windows 10.

Windows 10 enables these strategic business scenarios for Microsoft 365 Enterprise:

- Harness collective knowledge and expertise by empowering people to discover, share, and progress files, information, and ideas across your organization
- Work securely from anywhere, anytime across your device to achieve more while maintaining a flexible workstyle
- Provide peace-of-mind with controls and visibility for industry-verified conformity with global standards in compliance
- Protect your information and reduce the risk of data loss
- Detect and protect against external threats --Monitor, report and analyze activity to react promptly to provide organizational security
- Protect your users and their accounts
- Support your organization with enhanced privacy and compliance to meet the General Data Protection Regulation (GDPR)
- Get current and stay current on your desktop software and devices while reducing security risks and maximizing IT efficiency

For more information, see the [Digital transformation using Microsoft 365](#).

NOTE

To deploy both Windows 10 Enterprise and Office 365 ProPlus together and shift to a [modern desktop](#), see the [Modern Desktop Deployment Center](#).

Windows 10 deployment

There are multiple ways you can deploy Windows 10 Enterprise for your organization. Here, we'll focus on how you can configure and deploy a Windows 10 Enterprise image through these modern deployment scenarios.

DEPLOYMENT SCENARIO	WHEN TO USE IT
Using System Center Configuration Manager as an in-place upgrade	Select this option if you need to upgrade Windows 7 or Windows 8.1 computers to the current version of Windows 10 Enterprise and your computers are currently managed with System Center Configuration Manager (Current branch) .
Using Windows Autopilot	Select this option if you are setting up new Windows computers that have Windows 10 Enterprise, version 1703 or later pre-installed. End users will initiate setup using your desired configuration by entering their work or school account credentials.

If these deployment scenarios do not fit the needs of your organization, you can learn about other scenarios and understand the capabilities and limitations of each in [Windows 10 deployment scenarios](#). You can also [plan for Windows 10 deployment](#) on your own.

You can learn more about Windows 10 with these articles:

- [Microsoft 365 Enterprise product page](#)
- [Windows 10](#)
- [Deploy and update Windows 10](#)

Additional services and features

As part of your deployment of Windows 10 Enterprise, you can add these additional services and features.

Windows Analytics

Windows uses diagnostics data to provide rich, actionable information to help you gain deep insights into operational efficiency and the health of Windows 10 devices in your environment.

- Upgrade Readiness - Upgrade Readiness will help you move to Windows 10 and stay current with new Windows 10 Feature Updates.
- Update Compliance - Update Compliance is targeted to the IT admin who wants to gain a holistic view of all their Windows 10 devices, without any additional infrastructure requirements.
- Device Health - You can use Device Health to proactively detect and remediate end-user impacting issues.

See [Windows Analytics Overview](#) for more information.

Windows security

Windows 10 provides features to help protect against threats, help you secure your devices, and help with access control. With Windows 10, you get critical security features that protect your device right from the start. Microsoft 365 E3 adds security features such as Windows Hello for Business, Windows Defender Application Control, and Windows Information Protection. With Microsoft 365 E5, you get all the protection from Microsoft 365 E3 security plus cloud-based security features and Windows Defender Advanced Threat Protection.

To learn more about the security features that you get with Windows 10 Enterprise and get guidance on how you can deploy, manage, configure, and troubleshoot three key security features, see [Step 5: Deploy Windows 10 Enterprise security features](#).

How Microsoft does Microsoft 365 Enterprise

To peek inside Microsoft and learn how the company planned for, deployed, and is managing updates for

Windows 10, see:

- [Preparing your organization for a seamless Windows 10 deployment](#)
- [Adopting Windows as a service at Microsoft](#)
- [Deploying Windows 10 at Microsoft as an in-place upgrade](#)
- [Implementing strong user authentication with Windows Hello for Business](#)
- [Windows 10 deployment: tips and tricks from Microsoft IT \(video\)](#)
- [Windows Defender ATP helps detect sophisticated threats](#)
- [Securing the modern enterprise with Windows Defender and Windows Defender ATP \(video\)](#)

How Contoso did Microsoft 365 Enterprise

See how the Contoso Corporation, a fictional but representative multi-national business, [deployed Windows 10 Enterprise](#).



Next step

1

[Prepare your organization for Windows 10 Enterprise](#)

Step 1: Prepare your organization for Windows 10 Enterprise

2/26/2019 • 4 minutes to read • [Edit Online](#)

This article applies to both the E3 and E5 versions of Microsoft 365 Enterprise



Before upgrading your devices to Windows 10 Enterprise, consider the following:

- **Your domains must be added and verified**

With a Microsoft 365 subscription, you get a default domain name that ends in onmicrosoft.com (for example, contoso.onmicrosoft.com). Most organizations prefer to use one or more of the domains they own so their email addresses end in their own domain name (like username@contoso.com). To use your own domain, you need to add it to Microsoft 365 and verify that you own it. We recommend that you add and verify your domains now so they're ready to go whenever you set up Microsoft 365 services, like email and Skype for Business.

- **You don't need to add users at this time**

To use Microsoft 365 services or install Microsoft 365 products, users need accounts in Microsoft 365 and they need product licenses. How you add users to Microsoft 365 depends on the number of users and whether you currently have Active Directory on-premises. If you don't have Active Directory (or you have Active Directory but don't want to synchronize it to Microsoft 365), you can add users directly to Microsoft 365 and assign licenses, either individually or in bulk.

If you have Active Directory on-premises, you can [sync it with Microsoft 365](#) to create user accounts in Azure AD, the cloud directory used by Microsoft 365. With this method, you can create accounts for users and for security groups you use to manage permissions to resources (like SharePoint Online site collections or documents). Synchronizing your Active Directory with Microsoft 365 won't assign licenses to the users.

- **You don't need to license users at this time**

Before users can use Microsoft 365 services or install software from the Microsoft 365 portal, they need product licenses. As a global or user management admin, you can directly assign products licenses in Microsoft 365 either individually or in bulk. You can also use [group-based licensing](#) to automatically assign licenses when users are added to a particular group.

- **You install Office 365 ProPlus separately**

Obtaining a Microsoft 365 license does not automatically install Office 365 ProPlus on your client computers. See [Phase 4: Office 365 ProPlus](#) for more information.

Set Windows diagnostics data level

Microsoft uses diagnostic data to help keep Windows devices secure by identifying malware trends and other threats and to help us improve the quality of Windows and Microsoft services. You must ensure that the diagnostics service is enabled at a minimum level of Basic on all endpoints in your organization. *By default, this service is enabled and set to the Enhanced level.* However, it's good practice to check and ensure that they are receiving sensor data. Setting levels through policies overrides device-level settings.

Windows 10 operating system diagnostic data levels

You can configure your operating system diagnostic data settings using the management tools you're already

using, such as Group Policy, MDM, or Windows Provisioning. You can also manually change your settings using Registry Editor. Setting your diagnostic data levels through a management policy overrides any device level settings.

Use the appropriate value in the table below when you configure the management policy.

LEVEL	DATA GATHERED	VALUE
Security	Security data only.	0
Basic	Security data, and basic system and quality data.	1
Enhanced	Security data, basic system and quality data, and enhanced insights and advanced reliability data.	2
Full	Security data, basic system and quality data, enhanced insights and advanced reliability data, and full diagnostics data.	3

You can enable diagnostics data through any of these methods:

- **Microsoft Intune** - If you plan to use Intune to manage your devices, you can create a configuration policy to enable diagnostic data by configuring the [SystemAllowTelemetry](#) system policy. For more info on setting up configuration policies, see [Manage settings and features on your devices with Microsoft Intune policies](#).
- **Registry Editor** - You can use the Registry Editor to manually enable diagnostic data on each device in your organization. Alternately, you can write a script to edit the registry. If a management policy already exists, such as Group Policy or MDM, it will override this registry setting.
- **Group Policy** - If you do not plan to enroll devices in Intune, you can use a Group Policy object to set your organization's diagnostic data level.
- **Command prompt** - You can set Windows 10 diagnostics data and service to automatically start with the command prompt. This method is best if you are testing the service on only a few devices. Enabling the service to start automatically with this command will not configure the diagnostic data level. If you have not configured a diagnostic data level using management tools, the service will operate with the default Enhanced level.

See [Configure Windows diagnostic data in your organization](#) to learn more about Windows diagnostic data and how you can enable it based on the method that you choose.

As an interim checkpoint, you can see the [exit criteria](#) corresponding to this step.

Next step

2

[Deploy Windows 10 Enterprise for existing devices as an in-place upgrade](#)

Step 2: Deploy Windows 10 Enterprise for existing devices as an in-place upgrade

12/5/2018 • 25 minutes to read • [Edit Online](#)

This article applies to both the E3 and E5 versions of Microsoft 365 Enterprise



The simplest path to upgrade PCs currently running Windows 7 or Windows 8.1 to Windows 10 is through an in-place upgrade. You can use a System Center Configuration Manager (Configuration Manager) task sequence to completely automate the process.

If you have existing computers running Windows 7 or Windows 8.1, we recommend this path if your organization is deploying Windows 10. This leverages the Windows installation program (Setup.exe) to perform an in-place upgrade, which automatically preserves all data, settings, applications, and drivers from the existing operating system version. This requires the least IT effort, because there is no need for any complex deployment infrastructure.

Follow these steps to configure and deploy a Windows 10 Enterprise image using Configuration Manager as an in-place upgrade.

Part 1: Verify readiness to upgrade Windows

First, use the Upgrade Readiness capability of Windows Analytics to provide powerful insights and recommendations about the computers, applications, and drivers in your organization, at no extra cost and without additional infrastructure requirements. This new service guides you through upgrade and feature update projects using a workflow based on Microsoft recommended practices. Up-to-date inventory data allows you to balance cost and risk in your upgrade projects.

See [Manage Windows upgrades with Upgrade Readiness](#) to learn more, get started, use, and troubleshoot Upgrade Readiness.

Next, follow the guide to use System Center Configuration Manager (Current Branch) to upgrade Windows 7 or later operating system to Windows 10. As with any high-risk deployment, we recommend backing up user data before proceeding. OneDrive cloud storage is ready to use for licensed Microsoft 365 users and can be used to securely store their files. For more info, see [OneDrive quick start guide](#). To access this page, you must sign in as a tenant admin or global admin in an Office 365 or Microsoft 365 tenant.

For a list of Configuration Manager versions and the corresponding Windows 10 client versions that are supported, see [Support for Windows 10 for System Center Configuration Manager](#).

To verify readiness to upgrade Windows

Review these requirements before starting your Windows 10 deployment:

- **Windows editions eligible for upgrade** - Your devices must be running editions of Windows 7 or Windows 8.1 that are eligible for upgrade to Windows 10 Enterprise. For a list of supported editions, see [Windows 10 upgrade paths](#).
- **Supported devices** - Most computers that are compatible with Windows 8.1 will be compatible with Windows 10. You may need to install updated drivers in Windows 10 for your devices to properly function. See

[Windows 10 specifications](#) for more info.

- **Deployment preparation** - Make sure you have the following before you start configuring the deployment:
 - Windows 10 installation media - The installation media must be located on a separate drive, with the ISO already mounted. You can obtain the ISO from [MSDN Subscriber Downloads](#) or from the [Volume Licensing Service Center](#).
 - Backups of user data - Although user data will be migrated in the upgrade, best practice is to configure a backup scenario. For example, export all user data to a OneDrive account, BitLocker To Go-encrypted USB flash drive, or network file server. For more information, see [Back up or transfer data in Windows](#).
- **Environment preparation** - You will use an existing Configuration Manager server structure to prepare for operating system deployment. In addition to the base setup, the following configurations should be made in the Configuration Manager environment:
 1. [Extend the Active Directory Schema](#) and [create a System Management container](#).
 2. Enable Active Directory Forest Discovery and Active Directory System Discovery. For more info, see [Configure discovery methods for System Center Configuration Manager](#).
 3. Create IP range boundaries and boundary group for content and site assignment. For more info, see [Define site boundaries and boundary groups for System Center Configuration Manager](#).
 4. Add and configure the Configuration Manager reporting services point role. For more info, see [Configuring Reporting in Configuration Manager](#).
 5. Create a file system folder structure for packages.
 6. Create a Configuration Manager console folder structure for packages.
 7. Install System Center Configuration Manager (Current Branch) updates and any additional Windows 10 prerequisites.

Part 2: Add a Windows 10 OS image using Configuration Manager

Now you'll need to create an operating system upgrade package that contains the full Windows 10 installation media. In the following steps, you'll use Configuration Manager to create an upgrade package for Windows 10 Enterprise x64.

To add a Windows 10 OS image using Configuration Manager

1. Using the Configuration Manager console, in the **Software Library** workspace, right-click the **Operating System Upgrade Packages** node, and then select **Add Operating System Upgrade Package**.
2. On the **Data Source** page, specify the UNC path to the Windows 10 Enterprise x64 media, and then select **Next**.
3. On the **General** page, specify **Windows 10 Enterprise x64 Upgrade**, and then select **Next**.
4. On the **Summary** page, select **Next**, and then select **Close**.
5. Right-click the created **Windows 10 Enterprise x64 Update** package, and then select **Distribute Content**.
6. Choose your distribution point.

Part 3: Configure deployment settings

In this step, you'll configure an upgrade task sequence that contains the settings for the Windows 10 upgrade. You'll then identify the devices to upgrade, and then deploy the task sequence to those devices.

Create a task sequence

To create an upgrade task sequence, perform the following steps:

1. In the Configuration Manager console, in the **Software Library** workspace, expand **Operating Systems**.
2. Right-click the **Task Sequences** node, and then select **Create Task Sequence**.
3. On the **Create a new task sequence** page, select **Upgrade an operating system from upgrade package**, and then select **Next**.

4. On the **Task Sequence Information** page, specify **Windows 10 Enterprise x64 Upgrade**, and then select **Next**.
5. On the **Upgrade the Windows operating system** page, select **Browse** and choose the **Windows 10 Enterprise x64 Upgrade operating system upgrade package**, select **OK**, and then select **Next**.
6. Continue through the remaining wizard pages, and then select **Close**.

Create a device collection

After you create the upgrade task sequence, you'll need to create a collection that contains the devices you will upgrade.

NOTE

Use the following settings to test the deployment on a single device. You can use different membership rules to include groups of devices when you are ready. For more info, see [How to create collections in System Center Configuration Manager](#).

1. In the Configuration Manager console, in the **Assets and Compliance** workspace, right-click **Device Collections**, and then select **Create Device Collection**.
2. In the Create Device Collection wizard, on the **General** page, enter the following settings and then select **Next**:
 - Name: Windows 10 Enterprise x64 Upgrade
 - Limiting Collection: All Systems
3. On the **Membership Rules** page, select **Add Rule > Direct rule** to launch the Create Direct Membership Rule Wizard.
4. On the **Welcome** page of the Create Direct Membership Rule Wizard, select **Next**.
5. On the **Search for Resources** page, enter the following settings, replacing the placeholder **Value** text with the name of the device you are upgrading:
 - Resource Class: System Resource
 - Attribute Name: Name
 - Value: *PC0003*
6. On the **Select Resources** page, select your device, and select **Next**.
7. Complete the Create Direct Membership Rule wizard and the Create Device Collection Wizard.
8. Review the Windows 10 Enterprise x64 Upgrade collection. Do not continue until you see the machines you added in the collection.

Create an operating system deployment

Follow these steps to create a deployment for the task sequence.

1. In the Configuration Manager console, in the **Software Library** workspace, right-click the task sequence you created in a previous step, and then select **Deploy**.
2. On the **General** page, select the **Windows 10 Enterprise x64 Upgrade** collection, and then select **Next**.
3. On the **Content** page, select **Next**.
4. On the **Deployment Settings** page, select the following settings, and then select **Next**:
 - Action: Install

NOTE

For this test deployment, you'll set the purpose to **Available**, which requires user intervention to start the deployment. In a production environment, you may wish to automate the deployment using the Required purpose, which involves configuring additional options such as scheduling when the deployment is run.

- Purpose: Available
5. On the **Scheduling** page, accept the default settings, and then select **Next**.
 6. On the **User Experience** page, accept the default settings, and then select **Next**.
 7. On the **Alerts** page, accept the default settings, and then select **Next**.
 8. On the **Summary** page, select **Next**, and then select **Close**.

Part 5: Start the Windows 10 upgrade task sequence

Follow these steps to start the Windows 10 Upgrade task sequence on the device that you are upgrading.

1. Log on to the Windows computer and start **Software Center**.
2. Select the task sequence that you created in a previous step, and then select **Install**.
3. When the task sequence begins, it automatically initiates the in-place upgrade process by invoking the Windows setup program (Setup.exe) with the necessary command-line parameters to perform an automated upgrade, which preserves all data, settings, apps, and drivers.
4. After the task sequence completes successfully, the computer will be fully upgraded to Windows 10.

If you experience issues when using Windows 10 in an enterprise environment, you can consult [top Microsoft Support solutions for the most common issues](#). These resources include KB articles, updates, and library articles.

During the rollout of updates across your organization, use the Update Compliance capability of Windows Analytics to provide a holistic view of OS update compliance, update deployment progress, and failure troubleshooting for Windows 10 devices. This new service uses diagnostic data including installation progress, Windows Update configuration and other information to provide such insights, at no extra cost and without additional infrastructure requirements. Whether it's used with Windows Update for Business or other management tools, you can be assured that your devices are properly updated.

See [Monitor Windows Updates and Windows Defender Antivirus with Update Compliance](#) to learn more, get started, and use Update Compliance.

As an interim checkpoint, you can see the [exit criteria](#) corresponding to this step.

Next step

3

[Deploy Windows 10 Enterprise for new devices with Windows Autopilot](#)

Step 3: Deploy Windows 10 Enterprise for new devices with Windows Autopilot

12/5/2018 • 19 minutes to read • [Edit Online](#)

This article applies to both the E3 and E5 versions of Microsoft 365 Enterprise



If you have new Windows 10 PCs, you can use Windows Autopilot to customize the out-of-box-experience (OOBE) for your organization and deploy a new system with apps and settings already configured. There are no images to deploy, no drivers to inject, and no infrastructure to manage. Users can go through the deployment process independently, without the need to consult their IT administrator.

You can set up and pre-configure new Windows 10 devices and get them ready for productive use using Windows Autopilot. To learn more about Windows Autopilot, including benefits and Windows Autopilot scenarios, see [Overview of Windows Autopilot](#). When ready, follow these parts to start setting up new devices.

Part 1: Start Windows Autopilot deployment

See [Overview of Windows Autopilot](#) to:

1. Learn about and complete the prerequisites for Windows Autopilot deployment. The prerequisites include:

- **Device registration and OOBE customization**

To register devices, you need to acquire their hardware ID and register it. We are actively working with various hardware vendors to enable them to provide the required information to you, or upload it on your behalf. You also have the option to capture this information by yourself using a PowerShell script that generates a .csv file with the device's hardware ID.

Once devices are registered, there are OOBE customization options that you can configure including skipping privacy settings and EULA.

- **Company branding for OOBE**

This allows you to add branding to appear during device OOBE.

- **MDM auto-enrollment in Microsoft Intune**

Automatic enrollment lets users enroll their Windows 10 devices in Intune for device management when they connect their devices to Azure AD. To enroll, users add their work account to their personally-owned devices or join corporate-owned devices to Azure AD. In the background, the device is also enrolled for management with Intune.

- **Network connectivity to cloud services used by Windows Autopilot**

The Windows Autopilot Deployment Program uses a number of cloud services to get your devices to a productive state and these services must be accessible from devices registered as Windows Autopilot devices.

- **Devices must be pre-installed with Windows 10, version 1703 or later**

2. Learn about and select the Windows Autopilot Deployment Program for your organization. You can select from these deployment programs:

- **Microsoft Store for Business**
- **Microsoft Intune**
- **Partner Center**

Part 2: Set up a Windows 10 device for Microsoft 365

Before you can set up Windows devices for Microsoft 365 users, make sure all the Windows devices are running Windows 10, version 1703 (Creators Update) or later.

After all Windows devices in your organization have either been upgraded to Windows 10 Creators Update or are already running Windows 10 Creators Update, you can join these devices to your organization's Azure Active Directory.

Set up a brand new or newly-upgraded Windows 10 device

Follow these steps to set up a device using the Windows 10 OOB on a brand new device running Windows 10 Creators Update (or later) or on a device that was upgrade to Windows 10 Creators Update (or later) but has not gone through out-of-box setup.

1. If you don't have a wireless network configured, make sure you connect the device to the internet through a wired or Ethernet connection.
2. Go through the Windows device setup experience. On a new or reset device, the setup experience starts with the **Let's start with region. Is this right?** screen.
3. Go through Windows 10 device setup until you get to the **How would you like to set up?** page. Here, select **Set up for an organization**.
4. Sign in using the Microsoft 365 user's account and password. Depending on the user password setting, you may be prompted to update the password.
5. Finish Windows 10 device setup.

After you're done, the device will be connected to your organization's Azure AD.

Set up a device that has already completed out-of-box setup

If your device has Windows 10 Creators Update (or later) and has already gone through the out-of-box setup, follow these steps.

1. On your user's Windows PC that is running Windows 10, version 1703 (Creators Update), select the **Windows** logo, and then select the **Settings** icon.
2. In **Settings**, go to **Accounts**.
3. On the **Your info** page, select **Access work or school > Connect**.
4. On the **Set up a work or school account** dialog, under **Alternate actions**, select **Join this device to Azure Active Directory**.
5. On the **Let's get you signed in** page, enter your work or school account, and select **Next**.
6. On the **Enter password** page, enter your password, and select **Sign in**.
7. On the **Make sure this is your organization** page, verify that the information is correct, and select **Join**.
8. On the **You're all set!** page, select **Done**.

After you're done, the user will be connected to your organization's Azure AD.

Verify the device is connected to Azure AD

Follow these steps to verify the device's sync status with Azure AD, and then start using your Microsoft 365 account on the device.

1. Open **Settings**.
2. On the **Access work or school** page, select the **Connected to** area to expose the buttons **Info** and **Disconnect**.
3. Select **Info** to get your synchronization status.
4. On the **Sync status** page, select **Sync** to get the latest mobile device management policies onto the PC.
5. To start using the Microsoft 365 account, go to the Windows **Start** button, right-click your current account picture and then select **Switch** account.
6. Sign in by using your organization email and password.

If you experience issues when using Windows 10 in an enterprise environment, you can consult [top Microsoft Support solutions for the most common issues](#). These resources include KB articles, updates, and library articles.

As an interim checkpoint, you can see the [exit criteria](#) corresponding to this step.

Next step

4

[Monitor device health and compliance](#)

Step 4: Monitor device health and compliance

12/5/2018 • 2 minutes to read • [Edit Online](#)



Windows Analytics uses diagnostic data to provide rich, actionable information to help you gain deep insights into the operational efficiency and health of Windows 10 devices in your environment.

The Device Health capability of Windows Analytics provides proactive insights to help detect and remediate issues affecting end users. This new service uses diagnostic data to provide such insights without additional infrastructure requirements. Proactively remediating end-user issues enables you to reduce support costs and improve efficiency. Look for additional features to be released soon, which will enhance the capabilities and value of this new service.

See [Monitor the health of devices with Device Health](#) to learn more, get started, and use Device Health.

As an interim checkpoint, you can see the [exit criteria](#) corresponding to this step.

Next step

5

[Deploy Windows 10 Enterprise security features](#)

Step 5: Deploy Windows 10 Enterprise security features

1/23/2019 • 4 minutes to read • [Edit Online](#)



Windows 10 provides security features to protect enterprise users, stop cyberthreats, and prevent data loss.

To learn more about these technologies, see:

- [Identity protection](#) - Learn about Windows Hello for Business, Credential Guard, and access control.
- [Threat protection](#) - Learn about Windows Defender Advanced Threat Protection, a unified platform for preventative protection, post-breach detection, automated investigation, and response.
- [Information protection](#) - Learn about BitLocker, Windows Information Protection, and other ways that Windows 10 helps protect enterprise data.

This step shows you how you can deploy, manage, configure, and troubleshoot using these security features:

- [Windows Defender Antivirus](#)
- [Windows Defender Exploit Guard](#)
- [Windows Defender Advanced Threat Protection](#)

Windows Defender Antivirus

Windows Defender Antivirus (AV) is an antimalware solution that's built into Windows 10. It provides security and antimalware management for desktops, portable computers, and servers. For more info about Windows Defender AV, the minimum requirements, and how you can manage this feature, see [Windows Defender Antivirus in Windows 10 and Windows Server 2016](#).

If you are not using Windows Defender AV as your primary antivirus client, or if you are also using Windows Defender ATP, there are some considerations you need to take into account. To learn more, see [Windows Defender AV compatibility](#).

Deployment and management

To deploy and manage Windows Defender AV, follow the guidance here:

- [Deploy, manage, and report on Windows Defender AV](#)
- [Reference topics for management and configuration tools](#)

Configuration

Users can configure a number of features. For more info, see these resources:

- [Configure Windows Defender AV features](#)
- [Reference topics for management and configuration tools](#)

To help understand configuration options, refer to this list of all settings (as defined by their Group Policy configuration): [Use Group Policy settings to configure and manage Windows Defender AV](#)

You can use the [Windows Defender AV protection Evaluation Guide](#) to help evaluate the protection level and impact of Windows Defender AV on your network. This can also be useful in creating an initial configuration or as

a 'quick start guide' and is regularly updated to provide the most useful recommendations for configuring and enabling features to ensure maximum protection.

Reporting

You can obtain reporting by using a configuration tool, such as System Center Configuration Manager or Microsoft Intune. You can also obtain reporting from Update Compliance (OMS) or by consuming Windows event logs in your SIEM. If you have a license for Windows Defender ATP, you can also obtain reporting into Windows Defender AV detections and perform basic remediation. For more info, see these resources:

- [Deploy, manage, and report on Windows Defender AV](#)
- [Report on Windows Defender AV protection](#)
- [Windows Defender ATP portal overview](#)

Troubleshooting

For info on basic troubleshooting of error and event codes, see [Review event logs and error codes to troubleshoot issues with Windows Defender AV](#).

You can also submit issues (such as false positives) by using the Windows Defender Security Intelligence submission system. To learn how, see [Submit issues to Microsoft](#).

Windows Defender Exploit Guard

Windows Defender Exploit Guard is a new set of host intrusion prevention capabilities for Windows 10. For more info about Windows Defender Exploit Guard, the minimum requirements, and how you can manage this feature, see [Windows Defender Exploit Guard](#).

Deployment, management, and configuration

To deploy, manage, and configure Windows Defender Exploit Guard, follow the guidance here:

- [Exploit protection](#)
- [Attack surface protection](#)
- [Network protection](#)
- [Controlled folder access](#)

You can use a series of evaluation topics to help evaluate the protection level and impact of Windows Defender Exploit Guard on your network. This can also be useful in creating an initial configuration or as a 'quick start guide' and the topics and guidance are regularly updated to provide the most useful recommendations for configuring and enabling features to ensure maximum protection. For more info, [Evaluate Windows Defender Exploit Guard](#).

Reporting

You can obtain reporting by using a configuration tool, such as System Center Configuration Manager or Intune. You can also obtain reporting by consuming Windows event logs in your SIEM. If you have a license for Windows Defender ATP, you can also obtain reporting into Windows Defender AV detections and perform basic remediation. For more info, see these resources:

- [View Windows Defender Exploit Guard events](#)
- [Windows Defender ATP portal overview](#)

Troubleshooting

You can perform basic troubleshooting or optionally provide Microsoft with .cab files and submit issues (such as false positives) by using the Windows Defender Security Intelligence submission system. To learn how, see [Submit issues to Microsoft](#).

Windows Defender Advanced Threat Protection

Windows Defender ATP, only available with the Microsoft 365 Enterprise E5 plan, is a security service that enables enterprise customers to detect, investigate, and respond to advanced threats on their networks. For more info about Windows Defender ATP, the minimum requirements, and how you can manage this feature, see:

- [Windows Defender ATP](#)
- [Minimum requirements](#)

Deployment, management, and configuration

To deploy Windows Defender ATP, you'll need to ensure you have the right Windows license. After verifying that you have the right license, you'll need to decide the geolocation for where your data will be stored. After that, you can start onboarding endpoints to the service.

For more details on these steps, see these main topics:

- [Validate licensing provisioning and complete set up](#)
- [Data storage and privacy](#)
- [Onboard endpoints and setup access](#)

Detect, investigate, respond

After successfully onboarding endpoints to the service, you can start investigating alerts from the various dashboards. Once you've investigated alerts, you can take response actions on alerts.

For more info on how to do these, see:

- [Windows Defender ATP portal overview](#)
- [Use the Windows Defender ATP portal](#)
- [Take response actions](#)

Integrate with other products and tools

Windows Defender ATP integrates and supports various other products and tools to expand its security capabilities.

For more info on the tools and other products, see:

- [SIEM tools](#)
- [Create custom alerts](#)
- [Use APIs](#)
- [Build Power BI reports](#)

Troubleshooting

You might encounter issues while onboarding or while using the product. For more info on how to address issues, see:

- [Troubleshooting onboarding issues](#)
- [Troubleshooting Windows Defender ATP](#)

Next step

[Windows 10 Enterprise infrastructure exit criteria](#)

Phase 3: Windows 10 Enterprise infrastructure exit criteria

1/15/2019 • 4 minutes to read • [Edit Online](#)



If your Windows 10 Enterprise infrastructure meets the following conditions, you're ready to move to Phase 4.

Required: Your Microsoft 365 domains are added and verified

The Azure AD tenant for your Office 365 and Intune subscriptions are configured with your Internet domain names (such as contoso.com), rather than just a domain name that includes "onmicrosoft.com".

If you do not do so, you will be limited in the authentication methods that you can configure. For example, pass-through and federated authentication cannot use the "onmicrosoft.com" domain name.

If needed, [Step 1](#) can help you with this requirement.

Optional: Your users are added and licensed

The accounts corresponding to your users are added, either directly to your Azure AD tenant for your Office 365 and Intune subscriptions, or from directory synchronization from your on-premises Windows Server AD.

Once the users are added, you can assign them Microsoft 365 Enterprise licenses, either directly as a global or user administrator, or automatically through group membership.

If needed, [Step 1](#) can help you with this option.

Optional: Diagnostics are enabled

You have enabled diagnostic data settings using Group Policy, Microsoft Intune, the Registry Editor, or at the command prompt.

If needed, [Step 1](#) can help you with this option.

Required for in-place upgrade: Created a Configuration Manager task sequence for an operating system deployment

To start a Configuration Manager task sequence to do an in-place upgrade on a device running Windows 7 or Windows 8.1, you must have:

- Set the proper Windows diagnostics data level
- Verified the readiness to upgrade Windows
- Created a Configuration Manager task sequence that includes a device collection and an operating system deployment with a Windows 10 OS image

Once this is in place, you can perform in-place upgrades on devices that are ready to upgrade Windows. To get the maximum benefit out of Microsoft 365 Enterprise, upgrade as many devices running Windows 7 and Windows 8.1 as you can.

Each device running Windows 10 Enterprise can participate in the benefits of the integrated solution of Microsoft 365 Enterprise. The remaining devices running Windows 7 or Windows 8.1 cannot use the cloud-connected technologies and advanced security features of Windows 10 Enterprise.

If needed, [Step 2](#) can help you with this requirement.

Required for new devices: Configured Windows Autopilot

To use Windows Autopilot to deploy and customize Windows 10 Enterprise on a new device, you must have:

- Configured the proper Windows diagnostics data level
- Configured the prerequisites for Windows Autopilot, which include:
 - Device registration and OOBE customization
 - Company branding for OOBE
 - MDM auto-enrollment in Microsoft Intune
 - Network connectivity to cloud services used by Windows Autopilot
- Devices that are pre-installed with Windows 10, version 1703 or later
- Selected the Windows Autopilot Deployment Program for your organization

Once the Windows Autopilot configuration is in place, you can use it to configure and customize Windows 10 Enterprise for the out-of-the-box experience (OOBE) for:

- New devices
- Devices that have already completed an out-of-box setup in your organization.

Windows Autopilot configures the device and connects it to Azure AD.

Without Windows Autopilot, you must manually configure new devices, including the connection to Azure AD.

If needed, [Step 3](#) can help you with this requirement.

Optional: You are using Windows Analytics Device Health to monitor your Windows 10 Enterprise-based devices

You used the information in Monitor the health of devices with Device Health to detect and remediate issues affecting end users. Quickly addressing end-user issues can reduce your support costs and demonstrate to your users the IT commitment to Windows 10 Enterprise, which can help drive adoption across your organization.

If needed, [Step 4](#) can help you with this option.

Required: You are using Windows Defender Antivirus or your own antimalware solution

You deployed Windows Defender Antivirus or your own antivirus solution to protect your devices running Windows 10 Enterprise from malicious software. If you deployed Windows Defender Antivirus, you have implemented a reporting method, such as System Center Configuration Manager or Microsoft Intune, to monitor antivirus events and activity.

If needed, [Step 5](#) can help you with this requirement.

Required: You are using Windows Defender Exploit Guard

You deployed Windows Defender Exploit Guard to protect your devices running Windows 10 Enterprise from intrusion and have implemented a reporting method, such as System Center Configuration Manager or Microsoft Intune, to monitor intrusion events and activity.

If needed, [Step 5](#) can help you with this requirement.

Required: You are using Windows Defender Advanced Threat Protection (Microsoft 365 Enterprise E5 only)

You deployed Windows Defender Advanced Threat Protection (ATP) to detect, investigate, and respond to advanced threats against your network and devices running Windows 10 Enterprise.

Optionally, you have integrated Windows Defender ATP with other tools to expand its capabilities.

If needed, [Step 5](#) can help you with this requirement.

Updates for Windows 10 Enterprise

Next phase



Your next phase in the end-to-end deployment process for Microsoft 365 Enterprise is [Office 365 ProPlus](#).

Phase 4: Office 365 ProPlus

12/5/2018 • 4 minutes to read • [Edit Online](#)



This applies to both the E3 and E5 versions of Microsoft 365 Enterprise and Microsoft 365 Education

Microsoft 365 Enterprise includes Office 365 ProPlus, the subscription version of Office. Like Office 2016, Office 365 ProPlus includes all the Office applications, and those applications are installed directly on your client devices. Unlike Office 2016, Office 365 ProPlus is updated with new features on a regular basis and has a user-based licensing model that allows people to install Office on up to 5 devices. For more details, see [About Office 365 ProPlus in the enterprise](#).

In this phase, you deploy Office 365 ProPlus to client devices as part of Microsoft 365 Enterprise. In addition to this guidance, we recommend you use [Microsoft Fastrack](#) to help with your deployment.

Office 365 ProPlus enables these strategic business scenarios for Microsoft 365 Enterprise:

- Collaborate on documents in real time or on your own time to simplify the cocreation process
- Harness collective knowledge and expertise by empowering people to discover, share, and progress files, information, and ideas across your organization
- Empower users to transform business processes and increase efficiency
- Manage projects, tasks, and deadlines to meet your business objectives
- Use intelligent assistance for design, writing, content discovery, and more to help your work shine
- Discover insights, analyze your data, and share your findings to help everyone make informed decisions
- Communicate with your team to stay informed, solicit input, and build cohesion and consensus
- Communicate with partners, colleagues, and customers around the world for scheduled and ad hoc calls and online meetings with groups of all sizes
- Store and share files inside and outside your organization to work seamlessly across organizational boundaries
- Work securely from anywhere, anytime across your device to achieve more while maintaining a flexible workstyle
- Provide peace-of-mind with controls and visibility for industry-verified conformity with global standards in compliance
- Protect your information and reduce the risk of data loss
- Get current and stay current on your desktop software and devices while reducing security risks and maximizing IT efficiency

For more information, see the [Digital transformation using Microsoft 365](#).

If you already have Office 365 ProPlus deployed, please see the [exit criteria](#) for this phase to make sure that it meets the required conditions for Microsoft 365 Enterprise.

NOTE

To deploy both Windows 10 Enterprise and Office 365 ProPlus together and shift to a [modern desktop](#), see the [Modern Desktop Deployment Center](#).

Step 1: Assess your environment

Before deploying Office 365 ProPlus, follow the guidance in [Assess your environment and requirements for deploying Office 365 ProPlus](#). This assessment includes system requirements, details of your client devices (such as architectures and required languages), licensing requirements, network capability, and application compatibility. Completing the assessment will help you make key decisions as part of planning your deployment.

Step 2: Plan your deployment

After assessing your environment, follow the guidance in [Plan your deployment of Office 365 ProPlus](#) to create a deployment plan. This plan includes the following decisions:

- How to deploy Office, including what tool to use (such as System Center Configuration Manager or the Office Deployment Tool [ODT]) and where to install Office from
- How to manage updates to Office
- Which update channels to use (update channels for Office control how frequently your users receive feature updates to their Office applications)
- The Office installation packages and deployment groups you want to use, including which Office applications and languages should be installed for which users

The [planning article](#) includes best practices for all these options, including managing your deployment, managing your updates, defining installation packages, and creating deployment groups.

Step 3: Deploy

Based on your deployment plan from step 2, choose how you want to deploy:

- **Deploy Office 365 ProPlus with System Center Configuration Manager:** Manage your deployment with Configuration Manager, and download and deploy Office from distribution points on your network
- **Deploy Office 365 ProPlus with the ODT from the cloud:** Manage your deployment with the ODT, and install Office on client devices directly from the Office CDN
- **Deploy Office 365 ProPlus with the ODT from a local source:** Manage your deployment with the ODT, and download and deploy Office from a local source on your network
- **Self-install Office 365 ProPlus from the Office portal:** Manage your deployment from the Office portal and have your users install Office on their client devices directly from the portal

Many organizations will use a combination of these options for different users. For example, an organization might use Configuration Manager to deploy Office to most of their users, but enable self-install for a small group of workers who are not frequently connected to the internal network.

If your organization uses Configuration Manager, we recommend upgrading to the Current Branch and updating to the current release. For more details, see [Which branch of Configuration Manager should I use?](#)

How Microsoft does Microsoft 365 Enterprise

Learn how the experts at Microsoft planned for and deployed Office 365 ProPlus in Microsoft 365 Enterprise with these resources:

- Deploying and updating Microsoft Office 365 ProPlus
- Automation and update channels help deploy Microsoft Office 365 ProPlus (video)

How Contoso did Microsoft 365 Enterprise

See how the Contoso Corporation, a fictional but representative multi-national business, [deployed Office 365 ProPlus](#).



Next step

[Office 365 ProPlus infrastructure exit criteria](#)

Office 365 ProPlus deployment exit criteria

2/13/2019 • 2 minutes to read • [Edit Online](#)



This applies to both the E3 and E5 versions of Microsoft 365 Enterprise and Microsoft 365 Education

Before you move on to the next phase in the deployment process, ensure that your configuration meets the following required criteria for Office 365 ProPlus infrastructure.

- Assessment of infrastructure and environment is complete, including:
 - Client device details
 - Deployment tools
 - Office 365 licensing and accounts
 - Network capability
 - Application compatibility
- Deployment plan is complete, including:
 - How to deploy Office 365 ProPlus
 - How to manage updates to Office 365 ProPlus
 - Whether to deploy and install from a local source on your network or from the cloud
 - Which client devices get which update channels
 - Installation packages defined
 - All client devices assigned to deployment groups
 - Which Office applications, architectures, and languages go to which client devices
- Deployment of Office 365 ProPlus is complete, including:
 - All client devices have Office 365 ProPlus installed
 - All client devices are in the appropriate update channel and are receiving updates
 - All client devices have the appropriate languages installed or available

Next phase



Your next phase in the end-to-end deployment process for Microsoft 365 Enterprise is [mobile device management](#).

Phase 5: Mobile device management for Microsoft 365 Enterprise

2/13/2019 • 9 minutes to read • [Edit Online](#)



This feature applies to the E3 and E5 versions of Microsoft 365 Enterprise

Microsoft 365 Enterprise includes features to help manage devices, and their apps, within your organization. Using Microsoft Intune, you can manage iOS, Android, macOS, and Windows devices to protect access to your organization's resources, including your data. Intune integrates with Azure Active Directory (Azure AD), and enables the following business scenarios for Microsoft 365:

- Store and share files inside and outside your organization to work seamlessly across organizational boundaries
- Work securely from anywhere, anytime across your device to achieve more while maintaining a flexible workstyle
- Provide peace-of-mind with controls and visibility for industry-verified conformity with global standards in compliance
- Protect your information and reduce the risk of data loss
- Detect and protect against external threats
- Monitor, report, and analyze activity to react promptly to provide organizational security
- Protect your users and their accounts

For more information, see the [Digital transformation using Microsoft 365](#).

In this phase, you enroll your devices in Intune, and create and enforce policies to help keep your data secure and protected. The entire library of Intune documentation is [available online](#). It's also good practice to review the [Intune deployment planning, design and implementation guide](#) before you get started.

Step 1: Plan for your scenario

One of the main reasons to manage mobile devices is to secure and protect your organization's resources.

[Common ways to use Microsoft Intune](#) lists some real-world examples, including securing Office 365 email and data.

Intune gives you options to manage access to your organization using [Mobile Device Management \(MDM\)](#) or [Mobile Application Management \(MAM\)](#). MDM is when users "enroll" their devices in Intune. Once enrolled, they are managed devices, and can receive any policies, rules, and settings used by your organization. For example, you can install specific apps, create a password policy, install a VPN connection, and more.

Users with their own personal devices may not want to enroll their devices, or be managed by Intune and your policies. But, you still need to protect your organization's resources and data. In this scenario, you can protect your apps using MAM. For example, you can use a MAM policy that requires a user to enter a PIN when accessing SharePoint on the device.

You'll also determine how you're going to manage personal or organization-owned devices. You may want to treat devices differently, depending on their use. For example, you may want different plans for users in Human Resources (HR) or users in Sales. [Identify mobile device management use-case scenarios](#) can get you started, and includes some guidance on these different scenarios.

Step 2: Get your prerequisites

Next, get your prerequisites based on your requirements and your scenarios created in the previous step. [Implement your plan](#) lists all the requirements. Here are the significant items you need for Intune with Microsoft 365:

- **Intune subscription:** Included with Microsoft 365, and gives you access to Microsoft Intune in the [Azure portal](#)
- **Office 365 subscription:** Included with Microsoft 365, and is used for Office apps, including email
- **Azure Active Directory (Azure AD) premium:** Included with Microsoft 365, and is used to create user or security groups. These groups receive Intune policies that you create, such as forcing a password length to unlock a device. The groups you create in [Phase 2: Identity](#) can be used.

There may be some additional requirements, depending on your organization's needs. For example, if you'll be managing iOS devices, you'll need an Apple MDM Push certificate. If you're using on-premises Exchange, then you'll need the on-premises Exchange connector. These additional requirements are outlined when you get to those steps.

Step 3: Set up Intune

Intune uses many features in Azure AD, including your domain, your users, and your groups. You can also create new users and new groups to fit your company needs. For example, you can create a group called **iOS devices**, or **All HR users**. Take advantage of [Dynamic Groups](#) that lets you build either user or device groups based around simple or advanced rules.

This step focuses on setting up Intune, and getting it ready for you to manage your devices.

1. **Confirm your devices are supported.** Confirm your iOS, macOS, Android, Galaxy, and Windows devices are supported by Intune. If your organization includes devices that aren't supported, then the policies aren't applied to those devices.
2. **Customize your domain name.** By default, a domain named something like **your-domain.onmicrosoft.com** is automatically created in Azure AD. **onmicrosoft.com** can be customized for your organization. When you customize, it also gives users a familiar domain when connecting to Intune and using resources.
3. **Sign in to Intune.** When you sign in, you may be prompted to enter information about your organization. Intune is included with Microsoft 365, and can be opened directly from the [Office 365 Admin portal](#). You can also open Intune directly from the [Azure portal](#).
4. **Choose your mobile device management configuration.** The first time you use Intune, you must enable device management. Intune can be used as a cloud-only service, a hybrid with Intune and System Center Configuration Manager, or using Mobile Device Management for Office 365. You can choose which setup works best for your organization.
5. **Add users and add groups.**

You can manually add users, or connect to Azure AD to sync users with Intune. You can also give Admin roles to specific users. Users are required unless your devices are "userless" devices, such as kiosk devices.

Azure AD groups are used to simplify how you manage devices and users in Intune. Using groups, you can

do many different tasks. For example, your organization wants to require a specific app on Android devices. You can create an Android devices group, and deploy a policy with this app to the group.

In Intune, you can add users or groups that you create in [Phase 2: Identity](#)

6. **Assign licenses.** For users or devices to enroll in Intune, they need a license on the device. Each user or userless device requires an Intune license to access the Intune service. These licenses are included with Microsoft 365, and must be assigned in Intune.

Step 4: Enroll devices

To manage devices, the devices must be enrolled in Intune. As an administrator, you'll set up enrollment restrictions and policies for your users and devices. Each device platform (iOS, Android, macOS, and Windows) has a variety of options. You can have your users enroll themselves. Or, you can automate enrollment so users simply sign in to the device.

Enrollment is a key step when using Intune. [Enroll devices](#) lists the steps for the different devices.

	Test Lab Guide: iOS and Android device enrollment

Step 5: Add and deploy apps

Apps on mobile devices are often the quickest way users get access to your corporate resources.

There are challenges when using apps, as there are different devices, including personal devices and corporate devices. And, you want to protect your organization's resources and its data while also making sure users are productive.

Intune can manage apps, including add apps, assign them to different users or groups, and review other key details. For example, you can see which apps fail to install, check the version of an app, and more.

When users get a mobile device, one of the first tasks is to access organizational email and documents. Using Intune, you can [create and deploy email settings](#) using email apps that are pre-installed on the devices.

[Add apps](#) lists the steps to add, deploy, monitor, configure, and protect apps on devices within your org.

	Test Lab Guide: Device compliance policies

Step 6: Turn on compliance and conditional access

In the previous steps, you set up your environment, and enabled Intune. Now, you're ready to create some policies using compliance and conditional access.

Compliance and conditional access are important to managing devices. **Compliance policies** are created to help protect your organization's resources. When you create a compliance policy, you're defining the standard or the "baseline" of what a device must have. For example, you can choose an acceptable (or unacceptable) threat level, block jailbroken devices, require a password length, and more. If these devices don't meet your rules, meaning they aren't compliant, then you can block access to your resources.

This "blocking" introduces **Conditional access**. If a device is considered not-compliant, then you can block access to email, SharePoint, and more.

Intune in the [Azure portal](#) lets you create these policies, and apply them to your users and devices. As a best practice, start small, and use a staged approach. For example, create an iOS policy that blocks jailbroken devices. Apply (called "assign" in Intune) the policy to a pilot or test group. After initial testing, add more users to the pilot group. Using a staged approach, you can get feedback from a wide range of user types.

[Get started with device compliance policies](#) and [What's conditional access?](#) can help you get started.

Step 7: Apply features and settings

These features and settings are often considered the "cool" part of Intune, and are very powerful. Once you've successfully enforced some compliance policies using conditional access, you're ready to create **Device profiles**.

Intune in the [Azure portal](#) lets you create different profiles based on your device platform - iOS, macOS, Android, and Windows. For example, you can:

- Use Endpoint protection on Windows 10 devices to enable different BitLocker options, including encryption.
- Use the Restricted apps feature on iOS devices to create a list of approved apps that can be installed. Or, create a list of prohibited apps.
- Use the Kiosk settings to choose which apps can be used on Android devices running in kiosk mode.
- Apply a Wi-Fi connection and its settings, including the security type, on devices running macOS.
- And more

[What are Microsoft Intune device profiles?](#) is a great place to read about profiles, see how to create a profile, and more.

Remember, start small, and use a staged approach. Assign the profile to a pilot or test group. Then, assign the profile to more pilot groups.

Step 8: Get to know the other features

Intune is a powerful service, and includes many features. Here are some other tasks you can do using Intune:

- Manage software and updates on Windows [devices & PCs](#), and [iOS](#) devices
- Turn on [Windows Defender Advanced Threat Protection \(ATP\)](#) on your Windows 10 devices, and use compliance and conditional access to protect access to corporate resources, such as SharePoint or Exchange Online
- Use [Lookout](#), [Symantec](#), and other mobile defense threat partners
- Add a [partner certificate authority \(CA\)](#) to issue and renew certificates
- [Provide guidance to your end users](#) on the Company Portal app, getting apps, and more
- Monitor [apps](#), monitor [device compliance](#), monitor [configuration profiles](#), and more telemetry using the audit logs. You can also connect to the [Intune Data Warehouse](#) and use Power BI for even more reporting needs.

Identity and device access recommendations

Microsoft provides a set of recommendations for [identity and device access](#) to ensure a secure and productive workforce. For device access, use the recommendations and settings in the following articles along with the steps in this phase:

- [Prerequisites](#)
- [Common identity and device access policies](#)

How Microsoft does Microsoft 365 Enterprise

Learn how IT experts at Microsoft planned for and deployed EMS and device management with these resources:

- [Managing modern mobile productivity with Enterprise Mobility + Security](#)
- [Connecting to work on your Windows 10 device with Microsoft Intune](#)
- [Enabling mobile productivity for iOS, OS X, and Android devices at Microsoft](#)

How Contoso did Microsoft 365 Enterprise

See how the Contoso Corporation, a fictional but representative multi-national business, [deployed their mobile device management infrastructure](#) with Microsoft 365 cloud services.



Next step

[Mobile device management infrastructure exit criteria](#)

Mobile device management infrastructure exit criteria

12/5/2018 • 2 minutes to read • [Edit Online](#)



This applies to the E3 and E5 versions of Microsoft 365 Enterprise

Before you move on to the next phase in the deployment process, ensure that your configuration meets the following requirements for mobile device management infrastructure.

- Intune is set up, including the creation of Azure AD users and groups to apply your organization's rules for devices.
- You have enrolled devices in Intune so that the devices can receive the policies you create.
- Apps are added to devices so your users get access to your organization's Microsoft 365 cloud services, such as Exchange Online and SharePoint Online.
- Features and settings are configured and applied to your devices using the Azure AD users and groups you create, which might include enabling anti-virus and restricting specific apps.
- Compliance policies are in place to require a firewall or a password length on a device. If devices aren't compliant, conditional access blocks access to your organization's data.

Next phase



Your next phase in the end-to-end deployment process for Microsoft 365 Enterprise is [information protection](#).

Phase 6: Information protection

12/5/2018 • 2 minutes to read • [Edit Online](#)



Information protection is a set of policies and technologies that define how you transmit, store, and process sensitive information. In Phase 6, you step through information protection settings and features of Microsoft 365 Enterprise that help you secure data for your cloud-based workloads and scenarios.

NOTE

If you already have already deployed information protection, please see the [exit criteria](#) for this phase to make sure that it meets the required and optional conditions for Microsoft 365 Enterprise.

Plan and deploy your Microsoft 365 Enterprise information protection infrastructure

It's important to work with your legal and compliance teams to determine if your organization needs to meet compliance standards such as HIPPA, CJIS, or GDPR. You should also work with your security group to determine the objectives for information protection for your organization and for departments or groups that require additional security.

Next, use the following steps to build out information protection for Microsoft 365 Enterprise.

1	Define security and information protection levels
2	Configure classification for your environment
3	Configure increased security for Office 365
4	Configure privileged access management for Office 365

When you've completed these steps, go to the [exit criteria](#) for this phase to ensure that you meet the required and optional conditions for Microsoft 365 Enterprise.

How Microsoft does Microsoft 365 Enterprise

Learn how IT experts at Microsoft use the information protection capabilities of Microsoft 365 Enterprise to protect information and defend against cyber attacks:

- Protecting files in the cloud with Azure Information Protection
- Microsoft uses threat intelligence to protect, detect, and respond to threats
- Microsoft thwarts phishing attempts with Office 365

How Contoso did Microsoft 365 Enterprise

See how the Contoso Corporation, a fictional but representative multi-national business, [implemented information protection](#) with Microsoft 365 cloud services.



Next step

1

Define security and information protection levels

Step 1: Define security and information protection levels

12/5/2018 • 2 minutes to read • [Edit Online](#)

This step is required and applies to both the E3 and E5 versions of Microsoft 365 Enterprise



In this step, you'll define the levels of security and protection for your organization. For example, your sales department might only require a low security level. However, your research department and its highly valuable intellectual property might require a high security level that encrypts files and limits access to only research staff.

Although you can define your own security levels and might already have some in place, Microsoft recommends that you develop a plan to use at least three different levels of security and protection that can be applied. Here is a list to get you started:

- **Baseline:** This is a minimum standard for protecting data and for the identities and devices that access your data. You can follow baseline security and protection recommendations to provide strong default protection that meets the needs of many organizations or their departments.
- **Sensitive:** This is additional protection for a subset of your data that must be protected beyond the baseline level. You can apply this increased protection to specific data sets in your Office 365 environment. Microsoft also recommends applying the sensitive security level to identities and devices that access sensitive data.
- **Highly regulated:** This is the highest level of protection for organizations that typically have a very small amount of data that is highly classified, considered intellectual property or trade secrets, or data that must adhere to strict security regulations. Microsoft 365 Enterprise has capabilities to help organizations meet these high security requirements, including equivalent protection for identities and devices.

For more information, see [Three tiers of protection](#).

The result is a determination of your security and information protection levels.

As an interim checkpoint, see the [exit criteria](#) corresponding to this step.

Next step

2

[Configure classification for your environment](#)

Step 2: Configure classification for your environment

1/8/2019 • 2 minutes to read • [Edit Online](#)

This step is optional and applies to both the E3 and E5 versions of Microsoft 365 Enterprise



In this step, you work with your legal and compliance teams to define a classification scheme for your organization's data.

Microsoft classifications

Microsoft 365 includes three types of classification:

- Sensitive information types for Office 365
- Office 365 retention labels
- Azure Information Protection labels and protection

Sensitive information types for Office 365

Sensitive information types for Office 365 define how automated processes such as search recognize specific information types such as health service numbers and credit card numbers. You use sensitive information types to find sensitive data and apply data loss prevention rules and policies to protect this data. For more information, see [Overview of data loss prevention policies](#). For example, sensitive information types are especially helpful for meeting compliance and regulation requirements, such as for the General Data Protection Regulation (GDPR).

Office 365 retention labels

You can use Office 365 retention labels for personal data and for highly regulated and trade secret files stored in SharePoint Online and OneDrive for Business. For more information, including how to create them, see [Overview of retention labels](#).

If you decide to use Office 365 retention labels, you should configure at least one for each level of protection. For example, create three labels for:

- Baseline
- Sensitive
- Highly regulated

Azure Information Protection labels and protection

You can use Azure Information Protection labels to classify, and optionally protect, your organization's documents and emails. These labels can apply to documents that are stored outside of Office 365. These labels can be applied automatically by administrators who define rules and conditions, manually by users, or a combination where users are given recommendations.

To plan and deploy Azure Information Protection labels and protection, do the following:

1. Review the [requirements for Azure Information Protection](#).
2. Follow the [deployment roadmap for classification, labeling, and protection](#).

For more information, see the [library of Azure Information Protection documentation](#).

Classification for GDPR

For an example classification scheme that includes personal data for GDPR, see [Architect a classification schema for personal data](#).



[Test Lab Guide: Data classification](#)

As an interim checkpoint, see the [exit criteria](#) corresponding to this step.

Next step

3

[Configure increased security for Office 365](#)

Step 3: Configure increased security for Office 365

1/8/2019 • 2 minutes to read • [Edit Online](#)

This step is required and applies to both the E3 and E5 versions of Microsoft 365 Enterprise



To ensure that your Office 365 subscription and its data start off and remain secure from malicious threats, configure the following additional security for Office 365:

- [Tune threat management policies](#)
- [Additional Exchange Online tenant-wide settings](#)
- [Tenant-wide sharing policies in the SharePoint admin center](#)
- [Settings in Azure Active Directory](#)

Once configured, you can obtain information about your security status from:

- [Dashboards and reports in the Security & Compliance Center](#)
- [Office 365 Secure Score](#)

You can also use Cloud App Security or Office 365 Cloud App Security to monitor for security events and act. For more information, see [Overview of Office 365 Cloud App Security](#).

An additional security feature is [Office 365 Advanced Threat Protection \(ATP\)](#), which helps your organization collaborate more securely by:

- Protecting [links](#) and [attachments](#) in email.
- Providing spoof intelligence and anti-phishing capabilities for email in Exchange Online and [files in SharePoint Online, OneDrive for Business, and Microsoft Teams](#).



[Test Lab Guide: Configure increased Office 365 security](#)

As an interim checkpoint, see the [exit criteria](#) corresponding to this step.

Next step

4

[Configure privileged access management](#)

Step 4: Configure privileged access management for Office 365

2/19/2019 • 2 minutes to read • [Edit Online](#)

This step is optional and applies only to the E5 and Advanced Compliance versions of Microsoft 365 Enterprise



Privileged access management is enabled by configuring policies that specify just-in-time access for task-based activities in your Office 365 tenant. It can help protect your organization from breaches that may use existing privileged administrator accounts with standing access to sensitive data or access to critical configuration settings. For example, you could configure a privileged access management policy that requires explicit approval to access and change organization mailbox settings in your Office 365 tenant.

In this step, you'll enable privileged access management in your Office 365 tenant and configure privileged access policies that provide additional security for task-based access to Office 365 data and configuration settings for your organization. There are three basic steps to get started with privileged access in your Office 365 organization:

- Creating an approver's group
- Enabling privileged access
- Creating approval policies

One configured, privileged access management will enable your organization to operate with zero standing privileges and provide a layer of defense against vulnerabilities arising because of such standing administrative access. Privileged access requires approvals for executing any task that has an associated approval policy defined. Users needing to execute tasks included in the an approval policy must request and be granted access approval in order to have permissions necessary to execute tasks defined in the policy.

To enable Office 365 privileged access management, see the [Configure privileged access management in Office 365](#) topic.

For more information, see the [Privileged access management in Office 365](#) topic.

Results

The result of this step is that you've increased the security of Office 365 by enabling just-in-time access control for key data and configuration settings for your organization.

As an interim checkpoint, see the [exit criteria](#) corresponding to this step.

Next Step

[Information protection infrastructure exit criteria](#)

Information protection infrastructure exit criteria

1/8/2019 • 2 minutes to read • [Edit Online](#)



Before you are complete with your foundation infrastructure, make sure that your information protection infrastructure meets these conditions.

Required: Security and information protection levels for your organization are defined

You've planned for and determined the security levels that your organization needs. These levels define a minimum level of security and additional levels for increasingly sensitive information and their required data security.

At a minimum, you are using three security levels:

- Baseline
- Sensitive
- Highly regulated

If needed, [Step 1](#) can help you meet this requirement.

Required: Increased security for Office 365 is configured

You've configured the following settings for [Office 365 increased security](#):

- Threat management policies in the Office 365 Security & Compliance Center
- Additional Exchange Online tenant-wide settings
- Tenant-wide sharing policies in SharePoint admin center
- Settings in Azure Active Directory

You've also [enabled Office 365 Advanced Threat Protection \(ATP\) for SharePoint, OneDrive, and Microsoft Teams](#).

If needed, [Step 3](#) can help you meet this requirement.

Optional: Classification is configured across your environment

You've worked with your legal and compliance teams to develop an appropriate classification and labeling scheme for your organization's data, which include the following:

- Sensitive data types
- Office 365 labels
- Azure Information Protection labels

If needed, [Step 2](#) can help you meet this requirement.

Optional: Configure privileged access management in Office 365

You've used the information in the [Configure privileged access management in Office 365](#) topic to enable privileged access and create one or more privileged access policies in your Office 365 organization. You've configured these policies and just-in-time access is enabled for access to sensitive data or access to critical configuration settings.

If needed, [Step 4](#) can help you meet this requirement.

Next Step

You're now ready to deploy [workloads and scenarios](#), such as Microsoft Teams and Exchange Online, that run on top of your Microsoft 365 Enterprise foundation infrastructure.

Microsoft 365 Enterprise foundation infrastructure deployment strategies

2/13/2019 • 7 minutes to read • [Edit Online](#)

There are many ways you can deploy the phases of the [foundation infrastructure](#) of Microsoft 365 Enterprise and roll out its capabilities, software, and services to your users. To get you started on the project management of this undertaking, which can be large and complex depending on the size of your organization and its existing infrastructure, consider the following deployment strategies:

- Serial deployment
- Parallel deployment with non-overlapping user rollout
- Parallel deployment with overlapping user rollout
- Up-front infrastructure and rollout of the end-to-end configuration

Use these strategies for ideas on how to manage the overall project and more quickly realize the business benefits of Microsoft 365 Enterprise.

NOTE

This article contains assumptions and simplifications for a consistent way to describe the deployment strategies. These deployment strategies are generalized and are not meant to imply any specific timeframes, nor are they meant to apply to all organizations and situations.

Elements of IT project management for typical enterprise organizations

IT infrastructure includes both backend services and the rollout of new or improved capabilities or installed software to end users. IT departments typically deploy elements of an IT infrastructure in a methodical way. One approach to the successful deployment of an element of IT infrastructure consists of:

- A pilot rollout

This includes initial infrastructure configuration and rollout to a pilot set of users, testing, and subsequent modifications to the infrastructure configuration.

- A user rollout

This includes the rollout to the rest of your organization based on regions, departments, groups, or other types of systematic propagation of configuration or software.

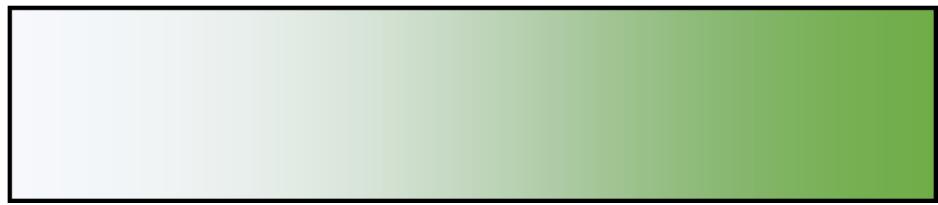
The set of users in the pilot rollout are not the same as those in the user rollout.

This article uses the following graphics to depict these definitions:

Pilot rollout



User rollout



The shading for the user rollout graphic indicates the percentage across your organization from 0% to 100% using a structured or methodical approach such as groups, departments, or regions.

Deployment strategies

Consider the following deployment strategies:

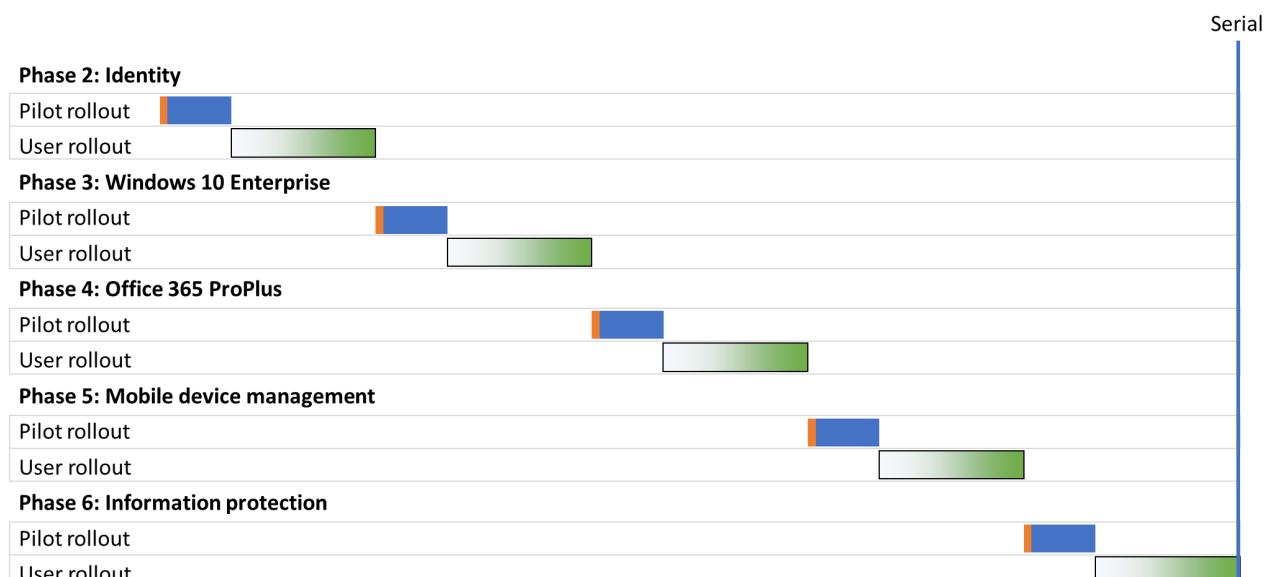
- Serial deployment
- Parallel deployment with non-overlapping user rollout
- Parallel deployment with overlapping user rollout
- Up-front infrastructure and rollout of the end-to-end configuration

Serial deployment

With a serial deployment, you completely roll out a phase, allowing the phase to reach 100% completion of deployment to all of your users, before moving on to the next one. Here are some of the reasons why you might deploy this way:

- Risk mitigation
- Resourcing constraints
- IT department funding cycles
- IT technology dependencies
- Business change management and end-user resistance

This Gantt chart shows a simplified serial deployment of phases 2-6 of the foundation infrastructure for Microsoft 365 Enterprise.



To simplify the discussion and example, each phase and deployment segment within each phase are assumed to take the same amount of time.

NOTE

Phase 1: Networking of the Microsoft 365 Enterprise Foundation Infrastructure is an IT department-only phase. Users reap the benefits of optimized connectivity to Microsoft's cloud resources but are not imposed upon to achieve it.

Simplified example pilot user experience:

- In December, I need to use my smart phone for MFA. (Identity)
- In March, I get Windows 10 Enterprise installed on my Windows 8.1 desktop. (Windows 10 Enterprise)
- In June, I get Office 365 ProPlus installed, replacing Office 2013. (Office 365 ProPlus)
- In September, I get device enrollment and app and conditional access policies applied. (Mobile device management)
- In December, I get the Azure Information Protection client installed and get trained on how to apply labels to documents. (Information protection)

The result is a 90-day cadence between successive pilot rollouts.

Simplified example end-user experience:

- In January, I need to use my smart phone for MFA. (Identity)
- In April, I get Windows 10 Enterprise installed on my Windows 8.1 desktop. (Windows 10 Enterprise)
- In July, I get Office 365 ProPlus installed, replacing Office 2013. (Office 365 ProPlus)
- In October, I get device enrollment and app and conditional access policies applied. (Mobile device management)
- In January of the following year, I get the Azure Information Protection client installed and get trained on how to apply labels to documents. (Information protection)

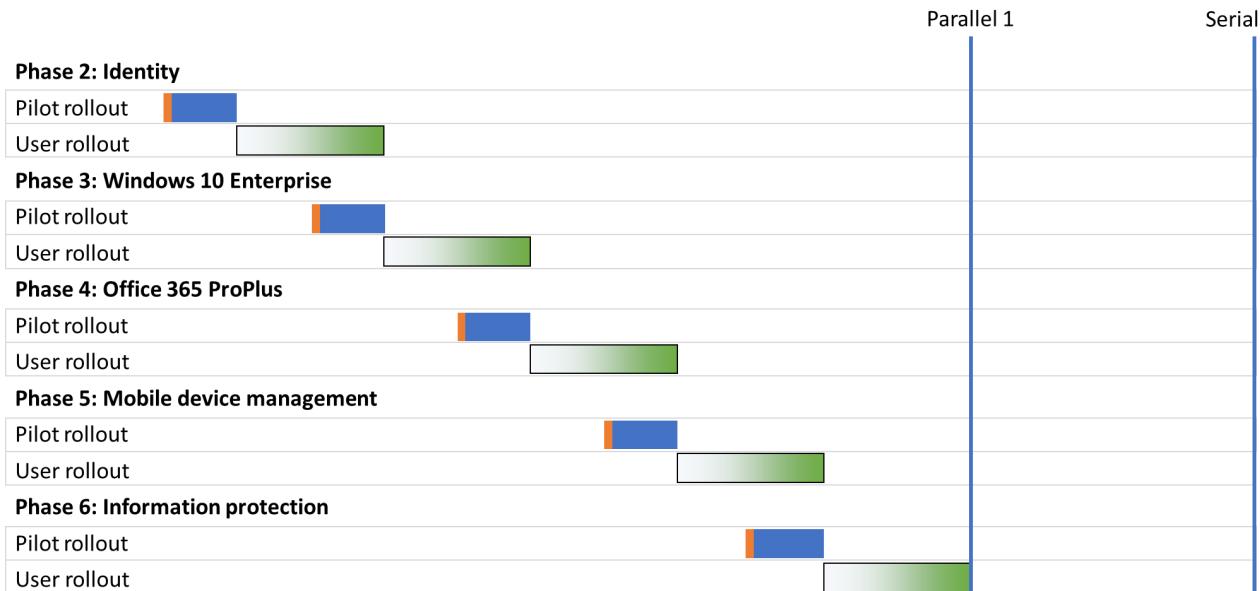
The result is a 90-day cadence between successive user rollouts.

The disadvantage to this deployment strategy is that it can take a long time to fully deploy the Microsoft 365 Enterprise foundation infrastructure.

Parallel deployment with non-overlapping user rollout (Parallel 1)

For this deployment strategy, you start the pilot rollout of the next phase during the last part of the user rollout of the current phase. Here is the deployment of phases 2-6 when the pilot rollout occurs as the user rollout of the previous phase is wrapping up.

Here is a simplified comparison between parallel and serial deployment strategies.



The end result is that user rollout for the current phase completes across your organization before the next one starts. Users that are not in pilot rollouts are not dealing with the rollouts of multiple phases at the same time, but pilot rollouts are done in parallel with user rollouts.

Simplified example pilot user experience:

- In December, I need to use my smart phone for MFA. (Identity)
- In February, I get Windows 10 Enterprise installed on my Windows 8.1 desktop. (Windows 10 Enterprise)
- In April, I get Office 365 ProPlus installed, replacing Office 2013. (Office 365 ProPlus)
- In June, I get device enrollment and app and conditional access policies applied. (Mobile device management)
- In August, I get the Azure Information Protection client installed and get trained on how to apply labels to documents. (Information protection)

The result is a 60-day cadence between successive pilot rollouts.

Simplified example end-user experience:

- In January, I need to use my smart phone for MFA. (Identity)
- In March, I get Windows 10 Enterprise installed on my Windows 8.1 desktop. (Windows 10 Enterprise)
- In May, I get Office 365 ProPlus installed, replacing Office 2013. (Office 365 ProPlus)
- In July, I get device enrollment and app and conditional access policies applied. (Mobile device management)
- In September, I get the Azure Information Protection client installed and get trained on how to apply labels to documents. (Information protection)

The result is a 60-day cadence between successive user rollouts.

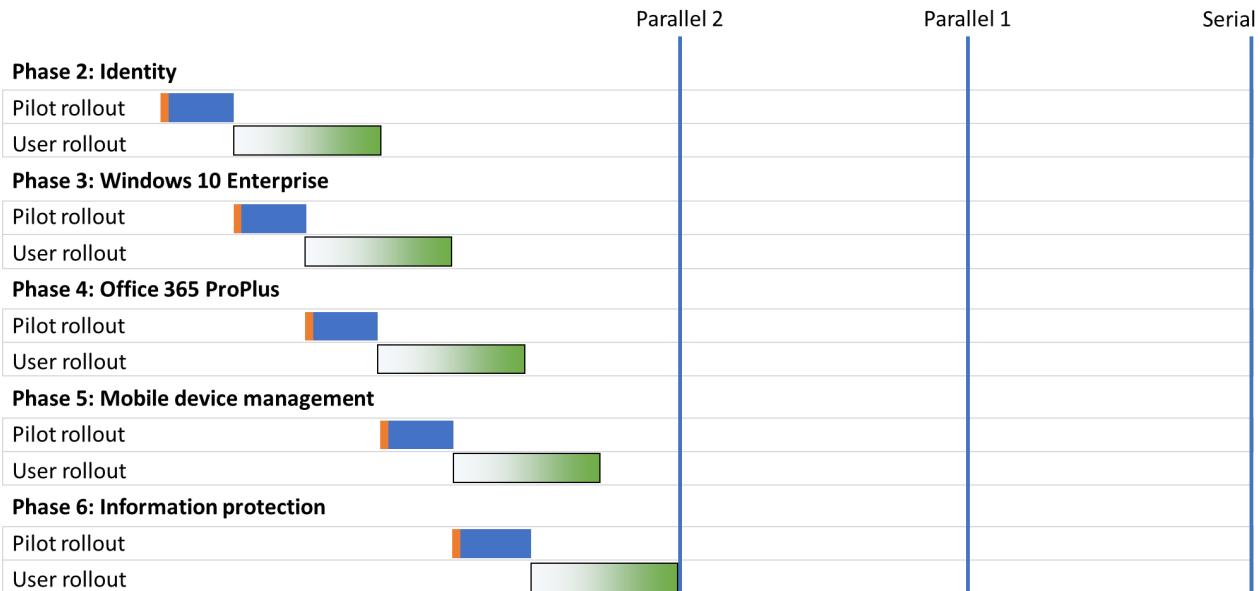
The advantage to this deployment strategy is that it can take less time to fully deploy the Microsoft 365 Enterprise foundation infrastructure, without having your IT department and users deal with multiple rollouts the same time.

Parallel deployment with overlapping user rollout (Parallel 2)

For this deployment strategy, you start the:

- Pilot rollout of the next phase during the last part of the user rollout of the current phase.
- User rollout of the next phase during the user rollout of the current phase in such a way that no user is dealing with the rollouts of multiple phases at the same time. This assumes that you are rolling out each phase of the foundation infrastructure in the same way, via regions, departments, or other.

Here is a simplified comparison between the different deployment strategies.



The end result is that:

- Pilot rollouts go from one phase to the next without a pause.
- The user rollout for a phase begins before the completion of the user rollout of the previous phase, but no individual user is rolling out more than one phase at a time.

Simplified example pilot user experience:

- In December, I need to use my smart phone for MFA. (Identity)
- In January, I get Windows 10 Enterprise installed on my Windows 8.1 desktop. (Windows 10 Enterprise)
- In February, I get Office 365 ProPlus installed, replacing Office 2013. (Office 365 ProPlus)
- In March, I get device enrollment and app and conditional access policies applied. (Mobile device management)
- In April, I get the Azure Information Protection client installed and get trained on how to apply labels to documents. (Information protection)

The result is a 30-day cadence between successive pilot rollouts.

Simplified example end-user experience:

- In January, I need to use my smart phone for MFA. (Identity)
- In February, I get Windows 10 Enterprise installed on my Windows 8.1 desktop. (Windows 10 Enterprise)
- In March, I get Office 365 ProPlus installed, replacing Office 2013. (Office 365 ProPlus)
- In April, I get device enrollment and app and conditional access policies applied. (Mobile device management)
- In May, I get the Azure Information Protection client installed and get trained on how to apply labels to documents. (Information protection)

The result is a 30-day cadence between successive user rollouts.

The advantage to this deployment strategy is that it can take even less time to fully deploy the Microsoft 365 Enterprise foundation infrastructure, still without having individual users deal with multiple rollouts the same time. However, users don't get a break between successive phases.

Up-front infrastructure and rollout of end-to-end configuration

For smaller organizations with the ability to compress phases 2-6 into a single deployment segment, the resulting deployment looks like this:

Phases 2-6

Configuration

End-to-end pilot



End-to-end rollout



The IT department configures the infrastructure for phases 2-6, then rolls out to the pilot users to check for the end-to-end functionality. For example, pilot users get all of this functionality at the same time:

- MFA and other identity features (Identity)
- Windows 10 Enterprise on Windows devices (Windows 10 Enterprise)
- Office 365 ProPlus for the Office suite (Office 365 ProPlus)
- App and conditional access policies (Mobile device management)
- Azure Information Protection client installed and training on how to apply labels to documents (Information protection)

Once the pilot rollout is concluded, the user rollout begins in which each user gets all the functionality the same time.

Next step

Start your deployment of Microsoft 365 Enterprise with the [foundation infrastructure](#).

Deployment of Microsoft 365 Enterprise with existing infrastructure

12/5/2018 • 20 minutes to read • [Edit Online](#)

Many organizations have existing networking, identity, and other components or Microsoft on-premises products and cloud-based services. This article steps through each phase of the deployment of Microsoft 365 Enterprise so you can quickly determine how to adapt or change your existing infrastructure.

Before you can exit each phase, you must examine its exit criteria, which is a set of required conditions that you must meet and optional conditions to consider. Exit criteria for each phase ensures that your on-premises and cloud infrastructure and resulting end-to-end configuration meets the requirements for a Microsoft 365 Enterprise deployment.

NOTE

FastTrack is an ongoing and repeatable benefit—available as part of your subscription—that is delivered by Microsoft engineers to help you move to the cloud at your own pace. FastTrack also gives you access to qualified partners for additional services, as needed. With over 40,000 customers enabled to date, FastTrack helps maximize ROI, accelerate deployment, and increase adoption across your organization. See [FastTrack for Microsoft 365](#).

Exit criteria for networking (phase 1)

Step through the following required and optional conditions for the networking infrastructure.

Required: Your network is ready for Microsoft 365 Enterprise

- Your offices have adequate Internet bandwidth for Microsoft 365 traffic, including Office 365, Microsoft Intune, and Windows 10 Enterprise installation and updates
- Your overall network maps to an Office 365 reference architecture
- Your network changes have been piloted and tested and meet with your traffic latency requirements

If needed, [Step 1](#) can help you with this requirement.

Required: Your local offices have local Internet connections and name resolution

You configured each local office with Internet access with a local ISP whose DNS servers use a local public IP address that identifies their location on the Internet. This ensures the best possible performance for users who access Office 365 and Intune.

If you don't use a local ISP for each branch office, performance can suffer because network traffic must traverse an organization's backbone or data requests are serviced by remote front-end servers.

How to test

Use a tool or web site from a device in that office to determine the public IP address that the proxy server is using. For example, use the [What Is My IP Address](#) web page. This public IP address assigned by your ISP should be geographically local. It should not be from a public IP address range for a central office or from a cloud-based network security vendor.

If needed, [Step 2](#) can help you with this requirement.

Optional: Unneeded network hairpins are removed

You examined your network hairpins and determined their impact on performance for all of your offices. You

removed network hairpins where possible or worked with your third-party network or security provider to implement optimal Microsoft 365 peering for their network.

If needed, [Step 3](#) can help you with this option.

Optional: You have configured traffic bypass on your Internet browsers and edge devices

You deployed the latest PAC files to your on-premises Internet browsers so that traffic to Microsoft 365 DNS domain names bypass proxy servers.

You configured your network perimeter devices—such as firewalls, and SSL Break and Inspect, and packet inspection devices—to use traffic bypass or to minimally process traffic to the Optimize and Allow categories of Microsoft 365 endpoints.

How to test

Use the logging tools on your network perimeter devices to ensure that traffic to Microsoft 365 destinations isn't being inspected, decrypted, or otherwise hindered.

If needed, [Step 4](#) can help you with this option.

Optional: Your clients and Office 365 applications are configured for optimal performance

You have optimized the Transmission Control Protocol (TCP) settings on your client devices and for Exchange Online, Skype for Business Online, SharePoint Online, and Project Online services.

If needed, [Step 5](#) can help you with this option.

Exit criteria for identity (phase 2)

Step through the following required and optional conditions for the identity infrastructure.

Also see [Prerequisites](#) for additional recommendations on identity infrastructure.

Required: All users, groups, and group memberships have been created

You've created user accounts and groups so that:

- Employees in your organization and the vendors, contractors, and partners that work for or with your organization have a corresponding user account in Azure Active Directory (Azure AD).
- Azure AD groups and their members contain user accounts and other groups for various purposes, such as the provisioning of security settings for Microsoft cloud services, automatic licensing, and other uses.

If needed, [Step 1](#) can help you meet this requirement.

Required: Your global administrator accounts are protected

You've [protected your Office 365 global administrator accounts](#) to avoid compromising credentials that can lead to breaches of an Office 365 subscription.

If you skip this requirement, your global administrator accounts can be susceptible to attack and compromise, allowing an attacker to gain system-wide access to your data for harvesting, destruction, or ransom.

If needed, [Step 2](#) can help you meet this requirement.

How to test

Use these steps to verify that you've protected your global administrator accounts:

1. Run the following Azure AD V2 command at the PowerShell command prompt. You should see only the list of dedicated global administrator accounts.

```
Get-AzureADDirectoryRole | where { $_.DisplayName -eq "Company Administrator" } | Get-AzureADDirectoryRoleMember | Ft DisplayName
```

- Sign in to Office 365 using each of the accounts from step 1. Each sign in must require multi-factor authentication and the strongest form of secondary authentication available in your organization.

NOTE

See [Connect to Office 365 PowerShell](#) for instructions on installing the Azure Active Directory PowerShell for Graph module and signing in to Office 365.

Optional: You have set up Privileged Identity Management to support on-demand assignment of the global administrator role

You've used the instructions in [Configure Azure AD Privileged Identity Management](#) to enable PIM in your Azure AD tenant and configured your global administrator accounts as eligible admins.

You've also used the recommendations in [Securing privileged access for hybrid and cloud deployments in Azure AD](#) to develop a roadmap that secures privileged access against cyber attackers.

If you skip this option, your global administrator accounts are subject to ongoing online attack and, if compromised, can allow an attacker to harvest, destroy, or hold your sensitive information for ransom.

If needed, [Step 2](#) can help you with this option.

Required: Users and groups are synchronized with Azure AD

If you have an existing on-premises identity provider, such as Active Directory Domain Services (AD DS), you have used Azure AD Connect to synchronize user accounts and groups from your on-premises identity provider to your Azure AD tenant.

With directory synchronization, your users can sign in to Office 365 and other Microsoft cloud services using the same credentials that they use to sign in to their computers and access on-premises resources.

If needed, [Step 3](#) can help you meet this requirement.

If you skip this requirement, you'll have two sets of user accounts and groups:

- User accounts and groups that exist in your on-premises identity provider
- User accounts and groups that exist in your Azure AD tenant

In this state, the two sets of user accounts and groups must be manually maintained by both IT administrators and users. This will inevitably lead to unsynchronized accounts, their passwords, and groups.

How to test

To verify that authentication with on-premises credentials works correctly, sign in to the Office portal with your on-premises credentials.

To verify that directory synchronization is working correctly, do the following:

- Create a new test group in Windows Server AD.
- Wait for the synchronization time.
- Check your Azure AD tenant to verify that the new test group name appears.

Optional: Directory synchronization is monitored

You've used [Azure AD Connect Health with sync](#) (for password synchronization) or [Using Azure AD Connect Health with AD FS](#) (for federated authentication) and have deployed Azure AD Connect Health, which involves:

- Installing the Azure AD Connect Health agent on each of your on-premises identity servers.
- Using the Azure AD Connect Health portal to monitor the state of the ongoing synchronization.

If you skip this option, you can more accurately assess the state of your cloud-based identity infrastructure.

If needed, [Step 3](#) can help you with this option.

How to test

The Azure AD Connect Health portal shows the current and correct state of your on-premises identity servers and the ongoing synchronization.

Optional: Multi-factor authentication is enabled for your users

You used [Plan for multi-factor authentication for Office 365 Deployments](#) and [Set up multi-factor authentication for Office 365 users](#) to enable multifactor authentication (MFA) for your user accounts.

If you skip this option, your user accounts are vulnerable to credential compromise by cyber attackers. If a user account's password is compromised, all the resources and capabilities of the account, such as administrator roles, are available to the attacker. This allows the attacker to copy, destroy, or hold for ransom internal documents and other data.

If needed, [Step 4](#) can help you with this option.

How to test

1. Create a test user account in the Office 365 Admin portal and assign them a license.
2. Configure multi-factor authentication for the test user account with the additional verification method that you are using for actual user accounts, such as sending a message to your phone.
3. Sign in to the Office 365 or Azure portal with the test user account.
4. Verify that MFA prompts you for the additional verification information and results in a successful authentication.
5. Delete the test user account.

Optional: Azure AD Identity Protection is enabled to protect against credential compromise

You've enabled Azure AD Identity Protection to:

- Address potential identity vulnerabilities.
- Detect possible credential compromise attempts.
- Investigate and address ongoing suspicious identity incidents.

If you skip this option, you won't be able to detect or automatically thwart credential compromise attempts or investigate identity-related security incidents. This potentially leaves your organization vulnerable to a successful credential compromise and the resulting threat to your organization's sensitive data.

If needed, [Step 4](#) can help you with this option.

Optional: Users can reset their own passwords

You've used [Azure AD self-service password reset rapid deployment](#) to configure password reset for your users.

If you don't meet this condition, users will be dependent on user account administrators to reset their passwords, resulting in additional IT administration overhead.

If needed, [Step 5](#) can help you with this option.

How to test

1. Create a test user account with an initial password.
2. Use the steps in [Let users reset their own passwords in Office 365](#) to reset the password on the test user account.
3. Sign out and then sign in to the test user account using the reset password.
4. Delete the test user account.

Optional: Password writeback is enabled for your users

You've used the instructions in [Azure AD SSPR with password writeback](#) to enable password writeback for the

Azure AD tenant of your Microsoft 365 Enterprise subscription.

If you skip this option, users who aren't connected to your on-premises network must reset or unlock their Windows Server AD passwords through an IT administrator.

If needed, [Step 5](#) can help you with this option.

NOTE

Password writeback is required to fully utilize Azure AD Identity Protection features, such as requiring users to change their on-premises passwords when Azure AD has detected a high risk of account compromise.

How to test

You test password writeback by changing your password in Office 365. You should be able to use your account and new password to access on-premises Windows Server AD resources.

1. Create a test user account in your on-premises Windows Server AD, allow directory synchronization to occur, and then grant it an Office 365 license in the Office 365 admin portal.
2. From a remote computer that is joined to your on-premises Windows Server AD domain, sign in to the computer and the Office portal using the credentials of the test user account.
3. Select **Settings > Office 365 settings > Password > Change password**.
4. Type the current password, type a new password, and then confirm it.
5. Sign out of the Office portal and the remote computer and then sign in to the computer using the test user account and its new password. This proves that you were able to change the password of an on-premises Windows Server AD user account using the Azure AD tenant.

Optional: Users can sign in using Azure AD Seamless Single Sign-on

You enabled [Azure AD Connect: Seamless Single Sign-On](#) for your organization to simplify how users sign in to cloud-based applications, such as Office 365.

If you skip this option, your users might be prompted to provide credentials when they access additional applications that use Azure AD.

If needed, [Step 5](#) can help you with this option.

Optional: The Office 365 sign-in screen is personalized for your organization

You have used [Add company branding to your sign-in and Access Panel pages](#) to add your organization's branding to the Office 365 sign-in page.

If you skip this option, your users will see a generic Office 365 sign-in screen and might not be confident that they're signing into your organization's site.

If needed, [Step 5](#) can help you with this option.

How to test

Sign in to the Office portal with your user account name and multi-factor authentication. You should see your custom branding elements on the sign-in page.

Optional: Self-service group management is enabled for specific Azure AD security and Office 365 groups

You've determined which groups are appropriate for self-service management, instructed their owners on group management workflow and responsibilities, and [set up self-service management in Azure AD](#) for those groups.

If you skip this option, all Azure AD group management tasks must be done by IT administrators.

If needed, [Step 6](#) can help you with this option.

How to test

1. Create a test user account in Azure AD with the Azure portal.
2. Sign-in as with the test user account and create a test Azure AD security group.
3. Sign out and then sign-in with your IT administrator account.
4. Configure the test security group for self-service management for the test user account.
5. Sign out and then sign-in with your test user account.
6. Use the Azure portal to add members to the test security group.
7. Delete the test security group and the test user account.

Optional: Dynamic group membership settings automatically add user accounts to groups based on user account attributes

You've determined the set of Azure AD dynamic groups and used the instructions in [Attribute-based dynamic group membership in Azure Active Directory](#) to create the groups and the rules that determine the set of user account attributes and values for group membership.

If you skip this option, group membership must be done manually as new accounts are added or as user account attributes change over time. For example, if someone moves from the Sales department to the Accounting department, you must:

- Update the value of the Department attribute for that user account.
- Manually remove them from the Sales group.
- Manually add them to the Accounting group.

If the Sales and Accounting groups were dynamic, you would only have to change the user account's Department value.

If needed, [Step 6](#) can help you with this option.

How to test

1. Create a test dynamic group in Azure AD with the Azure portal and configure a rule for the Department equals "test1".
2. Create a test user account in Azure AD and set the Department property to "test1".
3. Examine the properties of the user account to ensure that it was made a member of the test dynamic group.
4. Change the value of the Department property for the test user account to "test2".
5. Examine the properties of the user account to ensure that it is no longer a member of the test dynamic group.
6. Delete the test dynamic group and the test user account.

Optional: Group-based licensing to automatically assign and remove licenses to user accounts based on group membership

You [enabled group-based licensing](#) for the appropriate Azure AD security groups so that licenses for both Office 365 and EMS are automatically assigned or removed.

If you skip this option, you must manually:

- Assign licenses to new users whom you intend to have access to Office 365 and EMS.
- Remove licenses from users who are no longer with your organization or do not have access to Office 365 and EMS.

If needed, [Step 6](#) can help you with this option.

How to test

1. Create a test security group in Azure AD with the Azure portal and configure group-based licensing to assign Office 365 and EMS licenses.
2. Create a test user account in Azure AD and add it to the test security group.
3. Examine the properties of the user account in the Office 365 admin portal to ensure that it was assigned the Office 365 and EMS licenses.

4. Remove the test user account from the test security group.
5. Examine the properties of the user account to ensure that it no longer has the Office 365 and EMS licenses assigned.
6. Delete the test security group and the test user account.

Exit criteria for Windows 10 Enterprise (phase 3)

Step through the following required and optional conditions for the Windows 10 Enterprise infrastructure.

Required: Your Microsoft 365 domains are added and verified

The Azure AD tenant for your Office 365 and Intune subscriptions are configured with your Internet domain names (such as contoso.com), rather than just a domain name that includes "onmicrosoft.com".

If you do not do so, you will be limited in the authentication methods that you can configure. For example, pass-through and federated authentication cannot use the "onmicrosoft.com" domain name.

If needed, [Step 1](#) can help you with this requirement.

Optional: Your users are added and licensed

The accounts corresponding to your users are added, either directly to your Azure AD tenant for your Office 365 and Intune subscriptions, or from directory synchronization from your on-premises Windows Server AD.

Once the users are added, you can assign them Microsoft 365 Enterprise licenses, either directly as a global or user administrator, or automatically through group membership.

If needed, [Step 1](#) can help you with this option.

Optional: Diagnostics are enabled

You have enabled diagnostic data settings using Group Policy, Microsoft Intune, the Registry Editor, or at the command prompt.

If needed, [Step 1](#) can help you with this option.

Required for in-place upgrade: Created a Configuration Manager task sequence for an operating system deployment

To start a Configuration Manager task sequence to do an in-place upgrade on a device running Windows 7 or Windows 8.1, you must have:

- Set the proper Windows diagnostics data level
- Verified the readiness to upgrade Windows
- Created a Configuration Manager task sequence that includes a device collection and an operating system deployment with a Windows 10 OS image

Once this is in place, you can perform in-place upgrades on devices that are ready to upgrade Windows. To get the maximum benefit out of Microsoft 365 Enterprise, upgrade as many devices running Windows 7 and Windows 8.1 as you can.

Each device running Windows 10 Enterprise can participate in the benefits of the integrated solution of Microsoft 365 Enterprise. The remaining devices running Windows 7 or Windows 8.1 cannot use the cloud-connected technologies and advanced security features of Windows 10 Enterprise.

If needed, [Step 2](#) can help you with this requirement.

Required for new devices: Configured Windows Autopilot

To use Windows Autopilot to deploy and customize Windows 10 Enterprise on a new device, you must have:

- Configured the proper Windows diagnostics data level

- Configured the prerequisites for Windows Autopilot, which include:
 - Device registration and OOOE customization
 - Company branding for OOOE
 - MDM auto-enrollment in Microsoft Intune
 - Network connectivity to cloud services used by Windows Autopilot
- Devices that are pre-installed with Windows 10, version 1703 or later
- Selected the Windows Autopilot Deployment Program for your organization

Once the Windows Autopilot configuration is in place, you can use it to configure and customize Windows 10 Enterprise for the out-of-the-box experience (OOBE) for:

- New devices
- Devices that have already completed an out-of-box setup in your organization.

Windows Autopilot configures the device and connects it to Azure AD.

Without Windows Autopilot, you must manually configure new devices, including the connection to Azure AD.

If needed, [Step 3](#) can help you with this requirement.

Optional: You are using Windows Analytics Device Health to monitor your Windows 10 Enterprise-based devices

You used the information in Monitor the health of devices with Device Health to detect and remediate issues affecting end users. Quickly addressing end-user issues can reduce your support costs and demonstrate to your users the IT commitment to Windows 10 Enterprise, which can help drive adoption across your organization.

If needed, [Step 4](#) can help you with this option.

Required: You are using Windows Defender Antivirus or your own antimalware solution

You deployed Windows Defender Antivirus or your own antivirus solution to protect your devices running Windows 10 Enterprise from malicious software. If you deployed Windows Defender Antivirus, you have implemented a reporting method, such as System Center Configuration Manager or Microsoft Intune, to monitor antivirus events and activity.

If needed, [Step 5](#) can help you with this requirement.

Required: You are using Windows Defender Exploit Guard

You deployed Windows Defender Exploit Guard to protect your devices running Windows 10 Enterprise from intrusion and have implemented a reporting method, such as System Center Configuration Manager or Microsoft Intune, to monitor intrusion events and activity.

If needed, [Step 5](#) can help you with this requirement.

Required: You are using Windows Defender Advanced Threat Protection (Microsoft 365 Enterprise E5 only)

You deployed Windows Defender Advanced Threat Protection (ATP) to detect, investigate, and respond to advanced threats against your network and devices running Windows 10 Enterprise.

Optionally, you have integrated Windows Defender ATP with other tools to expand its capabilities.

If needed, [Step 5](#) can help you with this requirement.

Exit criteria for Office 365 ProPlus (phase 4)

Meet the requirements for assessment, deployment planning, and deployment of the Office 365 ProPlus infrastructure for Microsoft 365 Enterprise.

- Assessment of infrastructure and environment is complete, including:

- Client device details
- Deployment tools
- Office 365 licensing and accounts
- Network capability
- Application compatibility
- Deployment plan is complete, including:
 - How to deploy Office 365 ProPlus
 - How to manage updates to Office 365 ProPlus
 - Whether to deploy and install from a local source on your network or from the cloud
 - Which client devices get which update channels
 - Installation packages defined
 - All client devices assigned to deployment groups
 - Which Office applications, architectures, and languages go to which client devices
- Deployment of Office 365 ProPlus is complete, including:
 - All client devices have Office 365 ProPlus installed
 - All client devices are in the appropriate update channel and are receiving updates
 - All client devices have the appropriate languages installed or available

Exit criteria for mobile device management (phase 5)

Meet the following requirements for the mobile device management infrastructure.

- Intune is set up, including the creation of Azure AD users and groups to apply your organization's rules for devices.
- You have enrolled devices in Intune so that the devices can receive the policies you create.
- Apps are added to devices so your users get access to your organization's Microsoft 365 cloud services, such as Exchange Online and SharePoint Online.
- Features and settings are configured and applied to your devices using the Azure AD users and groups you create, which might include enabling anti-virus and restricting specific apps.
- Compliance policies are in place to require a firewall or a password length on a device. If devices aren't compliant, conditional access blocks access to your organization's data.

Exit criteria for information protection (phase 6)

Step through the following required and optional conditions for the information protection infrastructure.

Required: Security and information protection levels for your organization are defined

You've planned for and determined the security levels that your organization needs. These levels define a minimum level of security and additional levels for increasingly sensitive information and their required data security.

At a minimum, you are using three levels of information protection:

- Baseline
- Sensitive
- Highly regulated

If needed, [Step 1](#) can help you meet this requirement.

Required: Increased security for Office 365 is configured

You've configured the following settings for increased security based on the information in [Configure your Office](#)

365 tenant for increased security:

- Threat management policies in the Office 365 Security & Compliance Center
- Additional Exchange Online tenant-wide settings
- Tenant-wide sharing policies in SharePoint admin center
- Settings in Azure Active Directory

You've also [enabled Office 365 Advanced Threat Protection \(ATP\) for SharePoint, OneDrive, and Microsoft Teams](#).

If needed, [Step 3](#) can help you meet this requirement.

Optional: Classification is configured across your environment

You've worked with your legal and compliance teams to develop an appropriate classification and labeling scheme for your organization's data, which can include the following:

- Sensitive data types
- Office 365 labels
- Azure Information Protection labels

If needed, [Step 2](#) can help you meet this requirement.

Optional: Configure privileged access management in Office 365

You've used the information in the [Configure privileged access management in Office 365](#) topic to enable privileged access and create one or more privileged access policies in your Office 365 organization. You've configured these policies and just-in-time access is enabled for access to sensitive data or access to critical configuration settings.

If needed, [Step 4](#) can help you meet this requirement.

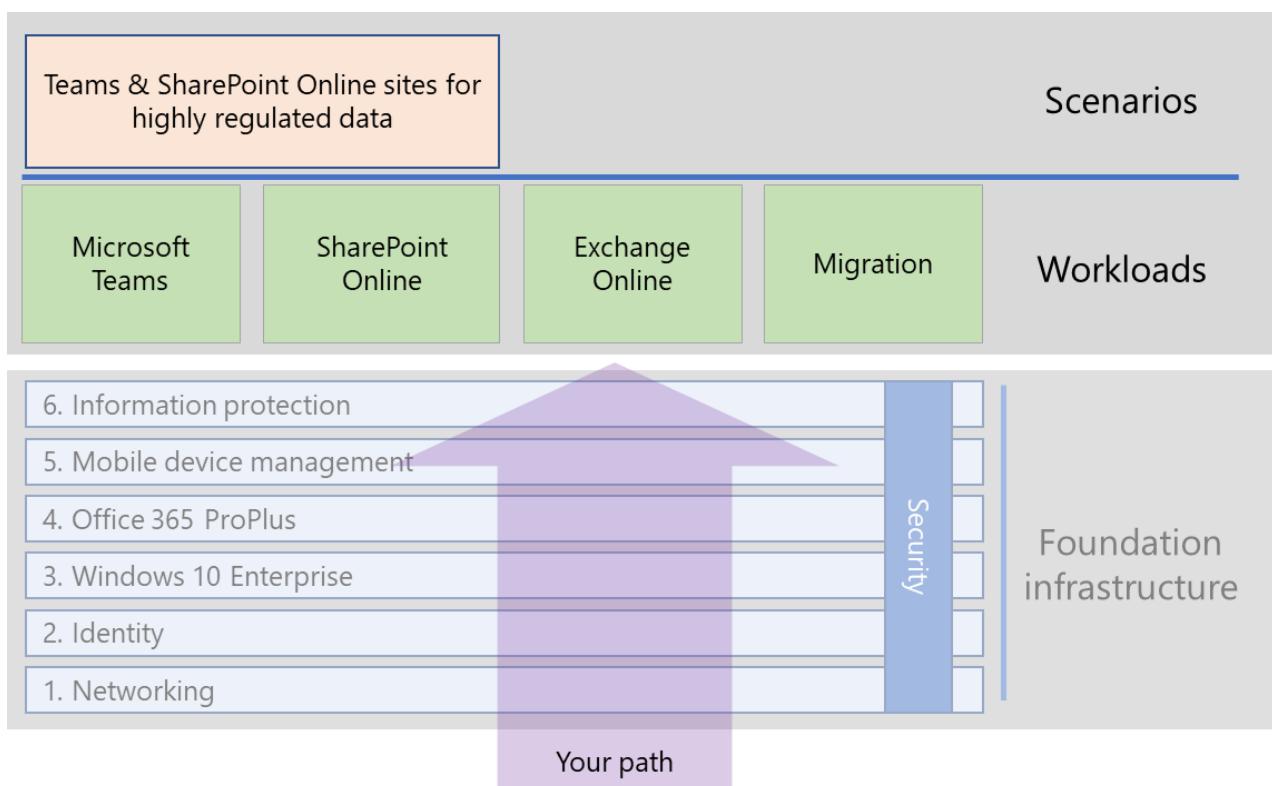
Microsoft 365 Enterprise workloads and scenarios

2/13/2019 • 2 minutes to read • [Edit Online](#)

To get the creativity and teamwork benefits of Microsoft 365 Enterprise, deploy these workloads and scenarios over your foundation infrastructure:

- Microsoft Teams
- Exchange Online
- SharePoint Online
- Migration to Microsoft 365 Enterprise
- Microsoft Teams and SharePoint Online sites for highly regulated data

Here are the workloads and scenarios in the overall Microsoft 365 Enterprise deployment guide:



Foundation infrastructure prerequisites

Ideally, you should deploy workloads and scenarios after you have configured all of the phases of the [foundation infrastructure](#). This ensures that all of the underlying layers are in place to provide integration, security, and the best experience for your users.

PHASE	RESULT
Network	Your network is updated for optimum performance to Microsoft 365 cloud services.
Identity	Identity is synchronized and secured with strong authentication for user accounts and protection for admin accounts.

PHASE	RESULT
Windows 10 Enterprise	Your computers running Windows 7 or Windows 8.1 can upgrade to Windows 10 Enterprise and new devices are installed with Windows 10 Enterprise.
Office 365 ProPlus	Your existing users of Microsoft Office can upgrade to Office 365 ProPlus.
Mobile device management	Your devices can be enrolled and managed.
Information protection	Your labels are ready to protect documents and Office 365 security features are enabled.

This is ideal but can take some time to plan for, configure, test, and pilot. Putting all of these layers in place is not necessary for you to more quickly realize the business value of Microsoft 365 Enterprise.

For example:

- Organizations often deploy [Exchange Online](#) after the **Identity** layer of the foundation infrastructure is rolled out to users so that they can begin using cloud-based email.
- Organizations that don't have an immediate need for storing highly regulated digital assets in the cloud can deploy [Microsoft Teams](#) and [SharePoint Online](#) for their users prior to the **Information protection** phase.

You must decide on how to best order the configuration of prerequisite layers of foundation infrastructure to meet your business needs.

Best practice

We highly recommend that you deploy and roll out the **Identity** phase of the foundation infrastructure prior to onboarding your users to any workloads or scenarios.

The **Identity** phase ensures that your cloud-based identity, whether cloud-only or synchronized with your on-premises Active Directory Domain Services (AD DS), contains the user and computer accounts and groups to manage authentication and access. Strong authentication for all your users along with strong protection of admin accounts is required before placing your organization's digital assets in the Microsoft 365 cloud.

Although foundational and very important to overall performance, the rollout of the **Networking** phase on your network can be in progress while onboarding your users to workloads, with the understanding that Microsoft 365 application and service performance will improve over time.

Deploy Microsoft Teams for Microsoft 365 Enterprise

2/13/2019 • 8 minutes to read • [Edit Online](#)

This workload is included in both the E3 and E5 versions of Microsoft 365 Enterprise

Microsoft Teams brings together chat, conferencing, document sharing, and threaded conversations in a way that makes it easy to create and share content across groups. Teams is the way you do teamwork and collaboration for Microsoft 365 Enterprise and is a key element of the Built for Teamwork value of Microsoft 365. If you are brand new to Teams, see [Overview of Microsoft Teams](#).

If you're currently using Skype for Business, we're building Skype for Business capabilities into Teams. This will happen over time, and ultimately Teams will become the single client experience. As a valued Skype for Business customer, Microsoft is here to support you. See the [Journey from Skype for Business to Microsoft Teams](#) for more information.

The following phases and steps guide you through the process of envisioning the role of Teams in your organization, onboarding your organization to Teams through a series of progressive rollouts, and driving usage of Teams and its value to your end users.

Before you begin, make sure you've configured the right [foundation infrastructure](#) phases so that your teams have the security capabilities you need.

Phase 1: Envision

In this phase, you gather the people for your Teams deployment and determine how your organization will use Teams to address its business needs.

Step 1: Gather your Teams deployment members

For a successful deployment of Teams on top of the Microsoft 365 [foundation infrastructure](#), you need to get the right people for input and feedback. Key people include business decision makers, IT staff such as architects and implementers, and advocates for your end users.

These three groups ensure that your Teams deployment includes considerations that address business needs, technical aspects of licensing and security, and that Teams will be something that your typical users will use.

Result

A list of people that represent the business, technical, and end user aspects of your organization.

Step 2: Determine and prioritize your Teams business scenarios

Teams can be used for many different purposes. You need to figure out which purposes map to your business needs on the separate levels of your organization, your business groups, your departments, and individual working and project teams. Take a look at the [Microsoft 365 Productivity Library](#) for examples to help you define Teams scenarios.

You should target Teams to address fast-moving and highly collaborative teams that work closely together and require many more facilities than just email with Exchange Online can provide. Examples are live group chats with a recorded history and a common and easy-to-find place to store files and notes.

One way to see the benefits of Teams is to examine how a team or v-team interacts today, and then find an appropriate Teams scenario that replaces the interaction and provides easier ways to collaborate and provide additional capabilities.

Teams enables these strategic business scenarios for Microsoft 365 Enterprise:

- Communicate with your team to stay informed, solicit input, and build cohesion and consensus
- Engage your firstline workers to enable your Digital Transformation
- Understand your work habits to improve your influence and impact

For more information, see the [Digital transformation using Microsoft 365](#).

Microsoft Teams for highly regulated data

Highly regulated data is subject to regional regulations or is the most valuable data for your organization, such as trade secrets, financial or human resources information, and organization strategy. You can configure a team for restricted access, data classification, data loss prevention, and encryption for this type of data. For the details, see [Microsoft Teams and SharePoint Online sites for highly regulated data](#).

Result

A list of Teams scenarios that address your organization's needs for collaboration and teamwork.

Phase 2: Onboard

In this phase, you plan for the technical aspects of a Teams deployment and start rolling out Teams to selected groups of users.

Prerequisites: Identity and device access configuration

To protect access to teams, ensure that you have configured [identity and device access policies](#) and the [recommended SharePoint Online access policies](#).

Step 1: Complete your technical planning

Before you begin technical planning, determine whether you want to use FastTrack. If your organization has over 50 seats and is participating in an [eligible plan](#), you can use [FastTrack for Microsoft 365](#), available at no additional cost to guide you through planning, deployment and service adoption. Or, you can complete this work yourself using our FastTrack Onboarding Wizards, which are available from [FastTrack](#) once you sign in with your Office 365 account.

If you are doing your own planning (or in conjunction with FastTrack), you need to determine if your network and organization are ready for Teams. It is especially important that you meet the exit criteria for networking in your [foundation infrastructure](#), with special attention to bandwidth, throughput, and traffic delays to maximize performance for Teams-based meetings.

Use these resources to prepare the technical aspects of your organization for a Teams rollout:

- [Check your environment's readiness for Teams](#)
- [Prepare your network for Teams](#)
- [Office 365 URLs and IP address ranges](#)

For a better understanding of security in Teams, review the following additional resources:

- [Overview of security and compliance in Teams](#)
- [Office 365 groups and Teams](#)
- [Guest access in Teams](#)

Next, use these resources to understand Teams licensing and to perform the setup of Teams for your organization:

- [Office 365 licensing for Teams](#)
- [Manage user access to Microsoft Teams](#)
- [Get clients for Microsoft Teams](#)
- [Turn on Microsoft Teams in your Office 365 organization](#)
- [Manage Microsoft Teams features in your Office 365 organization](#)

Result

Your network, security, and Office 365 licensing planning is done and you are ready to begin rolling out Teams to selected groups in your organization.

Step 2: Run an IT pilot

In most medium-sized and large organizations, you should run an IT pilot with your stakeholders from Phase 1 and early adopters and technical enthusiasts. During the IT pilot:

- Choose a Teams business scenario in which your IT pilot participants can practice. See the [Microsoft Teams getting started kit](#) for ideas.
- Give your pilot participants a set of exercises to test Teams-based chats, file storage, meetings, and other capabilities.
- Determine your change management strategy and produce materials to drive organization-wide user adoption. Change management materials can include email announcement text, internal training plans, hallway posters, and presentations. These materials will inform your organization about Teams and its benefits with the goals of raising awareness and driving usage. See [change management strategy for Microsoft Teams](#) for some ideas.
- Have your IT pilot participants review the change management strategy materials based on their experiences. They can provide tips on best practices and advice on how to best describe the benefits of Teams and how to use it for collaboration and teamwork.

Result

Your Teams IT pilot is complete and the initial change management materials have been developed, reviewed, and refined.

Step 3: Roll out to a business group

After completing your IT pilot, roll out Teams to a business group or department in your organization. This rollout should include:

- Identification of key business scenarios for Teams within the business group.
- Announcement activities to inform users of the expectations and timelines for Teams usage for departmental, work, or project teams.
- Direct user training on Teams or links to resources to introduce Teams and how to use it.
- A feedback mechanism, such as a central team containing everyone in the business group, to collect comments and issues from users in the business group.

During the rollout, you can refine your change management materials in preparation for the organization-wide rollout.

Result

A business group is up and running with Teams and the change management materials have been tested and refined.

Phase 3: Drive value

In this phase, you complete the rollout of Teams to your organization and support your users so that they are realizing its benefits.

Step 1: Roll out Teams to the rest of your organization

After completing your rollout to a targeted business group, roll out Teams to the rest of your organization. This rollout should include:

- Identification of key business scenarios for Teams within your separate business groups.
- Use of your refined change management materials for announcement activities to inform your organization of the expectations and timelines for Teams usage for departmental, work, or project teams.

- Delivering user training on Teams or links to resources to introduce Teams and how to use it. See the training resources at [End user training for Microsoft Teams](#).
- A feedback mechanism, such as a central team containing everyone, to collect comments and act on issues from organization users. If your organization has less than 2500 individuals, use a public channel in Teams. Otherwise, use a public group in Yammer.

Result

Your organization is up and running and your change management strategy is in place to inform, train, and enable users to begin using Teams.

Step 2: Measure usage, manage satisfaction, and drive adoption

After rolling out Teams to your entire organization, you must continue to employ your change management strategy to:

- Have your leadership promote Teams as the teamwork and collaboration tool for the organization.
- Encourage individuals to use it for business group, departmental, work, and project team communications and collaboration.

Here are some suggested activities:

- See [Office 365 adoption guidance](#) to learn about general best practices for cloud service adoption.
- See [Office 365 activity reports](#) to understand Office 365 service usage across your organization. If you aren't an Office 365 global admin for your organization, ask someone who is to grant your user account Reports Reader permissions so you can access activity reports.
- Monitor your feedback venue (a public channel in a central team or Yammer) for issues and feedback from individuals about their experiences with Teams. Address questions and issues as quickly as you can to prevent frustration and abandonment of Teams by individuals.
- Identify and nurture your champions in each business group and highlight their accomplishments and best practices using Teams. Reflect their successes out to the organization to show project success and adoption. Endorsement by technical leaders within a business group can exert a powerful influence over leaders and peers.

Result

Your organization has adopted Teams as its collaboration and teamwork tool.

How Microsoft does Microsoft 365 Enterprise

To peek inside Microsoft and learn how the company deployed and is using Microsoft Teams for collaboration, see:

- [Deploying Microsoft Teams streamlines collaboration and improves teamwork](#)
- [Microsoft Teams increases collaboration in the modern workplace at Microsoft](#)

Next steps

- [Manage Microsoft Teams features in your Office 365 organization](#)
- [Admin training for Microsoft Teams](#)

Deploy Exchange Online for Microsoft 365 Enterprise

2/13/2019 • 9 minutes to read • [Edit Online](#)

This workload is included in both the E3 and E5 versions of Microsoft 365 Enterprise

Exchange Online is your primary cloud service for email and calendaring that helps your users collaborate in ways that do not require real-time chatting or centralized document storage. Exchange Online is how you do individual and small group short-lived communication and scheduling and is a key element of the Built for Teamwork value of Microsoft 365 Enterprise. Exchange Online lets you accomplish more and work more effectively with the well-known Outlook application, no matter what device you're on.

Exchange Online also has advanced security capabilities including anti-malware and anti-spam filtering to protect mailboxes and data loss prevention capabilities that prevent users from mistakenly sending sensitive information to unauthorized people. Exchange Online security is a key element of the Intelligent Security value of Microsoft 365 Enterprise.

If you are brand new to Exchange Online, see [Microsoft Exchange Online](#).

The following phases and steps guide you through the process of envisioning the role of Exchange Online in your organization, onboarding your organization to Exchange Online through a series of progressive rollouts, and driving usage of Exchange Online and its value to your end users.

NOTE

These deployment instructions should be followed only after you've completed [Phase 2-Identity](#) of the Microsoft 365 Enterprise foundation infrastructure.

Phase 1: Envision

In this phase, you gather the people for your Exchange Online deployment and determine how your organization will use Exchange Online to address its business needs.

Step 1: Gather your Exchange Online deployment members

For a successful deployment of Exchange Online on top of [Phase 2-Identity](#) of the Microsoft 365 Enterprise foundation infrastructure, you need to get the right people for input and feedback. Key people include business decision makers, IT staff such as architects and implementers, and advocates for your end users.

These three groups ensure that your Exchange Online deployment includes considerations that address business needs, technical aspects of mailbox migration and security, and that the result will be something that typical users will use.

Result

A list of people that represent the business, technical, and end user aspects of your organization.

Step 2: Determine and prioritize your Exchange Online business scenarios

Exchange Online can be used for different purposes. You need to figure out which purposes map to your business needs on the separate levels of your organization, your business groups, your departments, or individual working and project teams. You should target Exchange Online to address your individual and small group short-lived communication and scheduling needs.

One way to see the benefits of Exchange Online is to examine how individuals, a team, or v-team interact today, and then find an appropriate scenario that provides easier ways to communicate, schedule meetings, and

collaborate. Keep in mind that [Microsoft Teams](#) might be a better choice for some of your collaboration scenarios.

Exchange Online enables these strategic business scenarios for Microsoft 365 Enterprise:

- Collaborate on documents in real time or on your own time to simplify the cocreation process
- Manage projects, tasks, and deadlines to meet your business objectives
- Understand your work habits to improve your influence and impact
- Communicate with your team to stay informed, solicit input, and build cohesion and consensus
- Store and share files inside and outside your organization to work seamlessly across organizational boundaries
- Work securely from anywhere, anytime across your device to achieve more while maintaining a flexible workstyle
- Protect your information and reduce the risk of data loss
- Detect and protect against external threats
- Monitor, report and analyze activity to react promptly to provide organizational security
- Support your organization with enhanced privacy and compliance to meet the General Data Protection Regulation (GDPR)

For more information, see the [Digital transformation using Microsoft 365](#).

Result

A list of Exchange Online scenarios that address your organization's needs for communication, scheduling, and short-lived collaboration.

Phase 2: Onboard

In this phase, you plan for the technical aspects of an Exchange Online deployment and start rolling it out to selected groups of users.

Prerequisites: Identity and device access configuration

To protect access to Exchange Online mailboxes, ensure that you have configured [identity and device access policies](#) and the [recommended Exchange Online access policies](#).

Step 1: Complete your technical planning

Before you begin technical planning, determine whether you want to use FastTrack. If your organization has over 50 seats and is participating in an [eligible plan](#), you can use [FastTrack for Microsoft 365](#), available at no additional cost to guide you through planning, deployment, and service adoption. Or, you can complete this work yourself using FastTrack Onboarding Wizards, which are available from [FastTrack](#) once you sign in with your Office 365 account.

If you are doing your own planning, or in conjunction with FastTrack, you need to determine if your network and organization are ready for Exchange Online. It is especially important that you meet the exit criteria for networking in your foundation infrastructure, with special attention to Internet bandwidth, throughput, and traffic delays to maximize performance for the additional traffic for Exchange Online-based email and attachments.

Use these resources to prepare for the technical aspects of an Exchange Online rollout:

- [Ways to migrate multiple email accounts to Office 365](#)
- [Office 365 mail migration advisor](#) (must be signed in to your Office 365 subscription)
- [Collaboration in Exchange Online](#)
- [Recipients in Exchange Online](#)

For a better understanding of security in Exchange Online, review the following resources:

- [Permissions in Exchange Online](#)
- [Security and compliance for Exchange Online](#)

- [Anti-spam and anti-malware protection](#)

Next, use these resources to understand Exchange Online mailbox management:

- [Create user mailboxes in Exchange Online](#)
- [Manage user mailboxes](#)
- [Create and manage distribution groups](#)

Result

You understand mailbox migration, security, and management and are ready to begin rolling out Exchange Online to selected groups in your organization.

Step 2: Run an IT pilot

In most medium-sized and large organizations, you should run an IT pilot with your stakeholders from Phase 1 and early adopters and technical enthusiasts. During the IT pilot:

- Choose an Exchange Online business scenario in which your IT pilot participants can practice.
- Give your pilot participants Office 365 licenses and migrate their on-premises mailboxes to Exchange Online.
- Give your pilot participants a set of exercises to test Exchange Online email, scheduling, and other capabilities.
- Determine your change management strategy and produce materials to drive organization-wide user adoption of Exchange Online. Change management materials can include email announcement text, internal training plans, hallway posters, and presentations. These materials will inform your organization about Exchange Online and its benefits with the goals of raising awareness and driving usage. See the [change management strategy for Microsoft Teams](#) article for some ideas.
- Have your IT pilot participants review the change management materials based on their experiences. They can provide tips on best practices and advice on how to best describe the benefits of Exchange Online and how to use it for communication and scheduling.

Result

Your Exchange Online IT pilot is complete and the initial change management materials have been developed, reviewed, and refined.

Step 3: Roll out to a business group

After completing your IT pilot, roll out Exchange Online to a business group or department in your organization. If your organization is using an on-premises email service such as Exchange Server, this rollout consists of mailbox migration. This rollout should include:

- Identification of key business scenarios for Exchange Online within the business group.
- Announcement activities to inform users of the expectations and timelines for Exchange Online usage for departments and work or project teams.
- Migration of on-premises mailboxes of your business group members to Exchange Online.
- Delivering user training on Exchange Online or links to resources to introduce Exchange Online and how to use it.
- A feedback mechanism, such as a central Microsoft Teams team containing everyone in the business group, to collect comments and act on issues from users in the business group.

During the rollout, you can refine your change management materials in preparation for the organization-wide rollout.

Result

A business group is up and running with Exchange Online and the change management materials have been tested and refined.

Phase 3: Drive value

In this phase, you complete the rollout of Exchange Online and support your users to help them realize its benefits.

Step 1: Roll out Exchange Online to the rest of your organization

The rollout to the rest of your organization should include:

- Identification of key business scenarios for Exchange Online within separate business groups.
- Use of your refined change management materials for announcement activities to inform your organization of the expectations and timelines for Exchange Online usage.
- Migration of the mailboxes for the rest of your organization to Exchange Online.
- Delivering user training on Exchange Online or provide links to resources to introduce Exchange Online and how to use it.
- A feedback mechanism, such as a central Team containing everyone, to collect comments and issues from organization users. If your organization has less than 2500 individuals, use a public channel in Teams. Otherwise, use a public group in Yammer.

Result

Your organization is up and running and your change management strategy is in place to inform, train, and enable users to use Exchange Online.

Step 2: Measure usage, manage satisfaction, and drive adoption

After rolling out Exchange Online to your entire organization, you must continue to employ your change management strategy to:

- Have your leadership promote Exchange Online as the primary tool for individual and short-lived communication and scheduling.
- Encourage individuals to use it for business group, departmental, work, and project team communications, calendaring, and collaboration.

Here are some suggested activities:

- See [Office 365 adoption guidance](#) to learn about general best practices for cloud service adoption.
- See [Office 365 activity reports](#) to understand Office 365 service usage across your organization. If you aren't an Office 365 global admin for your organization, ask someone who is a global admin to grant Reports Reader permissions to your user account so you can access activity reports.
- Monitor your feedback venue (a public channel in a central Teams team or Yammer) for issues and feedback from individuals about their experiences with Exchange Online. Address questions and issues as quickly as you can to prevent frustrated individuals and demonstrate support for the rollout.
- Identify and nurture champions in each business group and highlight their accomplishments and best practices using Exchange Online. Reflect their successes out to the organization to show project success and adoption. Endorsement by technical leaders within a business group can exert a powerful influence over leaders and peers.

Result

Your organization has adopted Exchange Online as its primary individual and small group short-lived communication and scheduling tool.

How Microsoft does Microsoft 365 Enterprise

To peek inside Microsoft and learn how the company migrated to Exchange Online and is using Exchange Online Protection to protect against cyber attacks, see:

- [Microsoft migrates 150,000 mailboxes to Exchange Online](#)
- [Microsoft uses threat intelligence to protect, detect, and respond to threats](#)

- Microsoft thwarts phishing attempts with Office 365

Next steps

See these resources for the ongoing maintenance of Exchange Online:

- [Exchange admin center in Exchange Online](#)
- [Monitoring, reporting, and message tracing in Exchange Online](#)
- [Backing up email in Exchange Online](#)

Deploy SharePoint Online and OneDrive for Business for Microsoft 365 Enterprise

2/13/2019 • 9 minutes to read • [Edit Online](#)

This workload is included in both the E3 and E5 versions of Microsoft 365 Enterprise

SharePoint Online and Microsoft Teams is how you do file storage and sharing, content management, and collaboration and is a key element of the Built for Teamwork value of Microsoft 365 Enterprise.

SharePoint Online also has advanced security capabilities including access control and permissions and encryption in flight and at rest. SharePoint Online security is a key element of the Intelligent Security value of Microsoft 365 Enterprise.

If you are brand new to SharePoint Online, see [SharePoint Online](#) and [Get Started with SharePoint](#).

The following phases and steps guide you through the process of envisioning the role of SharePoint Online in your organization, onboarding your organization through a series of progressive rollouts, and driving usage its value to your end users. Before you begin, make sure you've configured the right [foundation infrastructure](#) phases so that your SharePoint Online sites have the security capabilities you need.

To deploy OneDrive for Business for Microsoft 365 Enterprise, see the [OneDrive guide for enterprises](#).

Phase 1: Envision

In this phase, you gather the people for your SharePoint Online deployment and determine how your organization will use them to address its business needs.

Step 1: Gather your SharePoint Online deployment members

For a successful deployment of SharePoint Online on top of the [Microsoft 365 Enterprise foundation infrastructure](#), you need to get the right people for input and feedback. Key people include business decision makers, IT staff such as architects and implementers, and advocates for your end users.

These three groups ensure that your deployment includes considerations that address business needs, technical aspects of folder and document migration and security, and that the result will be something that typical users will use.

Result

A list of people that represent the business, technical, and end user aspects of your organization.

Step 2: Determine and prioritize your SharePoint Online business scenarios

SharePoint Online can be used for different purposes. You need to figure out which purposes map to your business needs. You should target SharePoint Online to address the document storage and sharing, content management, and collaboration needs of your teams, your division, or your entire organization.

See the list of scenarios and capabilities at [SharePoint Online](#).

The following business pillars can address your organization's needs:

Share and Work Together	Take advantage of team sites, collaboration sites, and sync.
Inform and Engage	Information coming in the future.

Transform	Uses Flow to create a store or workflow.
Harness Collective Knowledge	Uses Search to give the desired results within your organization.
Protect	Ensures your organization is secured and has the correct compliance.
External/Develop	Lets your organization develop customize solutions and apps by using the SharePoint Framework.

See [SharePoint Online admin](#) for resources on how to configure SharePoint Online for your needs.

One way to see the benefits of SharePoint Online is to examine how individuals, a team, a division, or your entire organization interact today, and then find an appropriate scenario that provides easier ways to store and share files collaborate. Keep in mind that [Microsoft Teams](#) might be a better choice for some of your scenarios.

SharePoint Online enables these strategic business scenarios for Microsoft 365 Enterprise:

- Communicate with your team to stay informed, solicit input, and build cohesion and consensus
- Harness collective knowledge
- Empower users to transform business processes
- Shape the company culture
- Manage projects, tasks, and deadlines to meet your business objectives
- Engage your firstline workers to enable your Digital Transformation
- Understand your work habits to improve your influence and impact
- Communicate with partners, colleagues, and customers
- Store and share files inside and outside your organization to work seamlessly across organizational boundaries
- Work securely from anywhere, anytime across your device to achieve more while maintaining a flexible workstyle
- Protect your information and reduce the risk of data loss
- Support your organization with enhanced privacy and compliance to meet the General Data Protection Regulation (GDPR)

For more information, see the [Digital transformation using Microsoft 365](#).

SharePoint Online site for highly regulated data

Highly regulated data is subject to regional regulations or is the most valuable data for your organization, such as trade secrets, financial or human resources information, and organization strategy. You can configure a SharePoint Online site for restricted access, data classification, data loss prevention, and encryption for this type of data. For the details, see [Microsoft Teams and SharePoint Online sites for highly regulated data](#).

Result

A list of SharePoint Online scenarios that address your organization's needs for document storage and sharing, content management, and collaboration.

Phase 2: Onboard

In this phase, you plan for the technical aspects of a SharePoint Online deployment and start rolling them out to selected groups of users.

Prerequisites: Identity and device access configuration

To protect access to SharePoint Online sites, ensure that you have configured identity and device access policies and the [recommended SharePoint Online access policies](#).

Step 1: Complete your technical planning

Before you begin technical planning, determine whether you want to use FastTrack. If your organization has over 50 seats and is participating in an [eligible plan](#), you can use FastTrack benefits, available at no additional cost to guide you through planning, deployment, and service adoption. Or, you can complete this work yourself using FastTrack Onboarding Wizards, which are available from [FastTrack](#) once you sign in with your Office 365 account.

If you are doing your own planning, or in conjunction with FastTrack, you need to determine if your network and organization are ready for SharePoint Online. It is especially important that you meet the exit criteria for networking in your foundation infrastructure, with special attention to Internet bandwidth, throughput, and traffic delays to maximize performance for the additional traffic for SharePoint Online-based documents.

Use these resources to prepare for the technical aspects of a SharePoint Online rollout:

- [SharePoint Online Planning Guide](#)
- [Migrate to SharePoint Online](#)

For a better understanding of security in SharePoint Online, review the following resources:

- [How SharePoint Online and OneDrive safeguard your data in the cloud](#)
- [Data Encryption in OneDrive for Business and SharePoint Online](#)

Result

You understand SharePoint Online sites and on-premises folder and document migration and security and are ready to begin rolling out SharePoint Online to selected groups in your organization.

Step 2: Run an IT pilot

In most medium-sized and large organizations, you should run an IT pilot with your stakeholders from Phase 1 and early adopters and technical enthusiasts. During the IT pilot:

- Choose a SharePoint Online business scenario in which your IT pilot participants can practice.
- Give your pilot participants a set of exercises to test SharePoint Online document storage, sharing, collaboration, team-based scheduling, and other capabilities.
- Determine your change management strategy and produce materials to drive organization-wide user adoption of SharePoint Online. Change management materials can include email announcement text, internal training plans, hallway posters, and presentations. These materials will inform your organization about SharePoint Online and its benefits with the goals of raising awareness and driving usage. See the change management strategy for [Microsoft Teams](#) article for some ideas.
- Have your IT pilot participants review the change management materials based on their experiences. They can provide tips on best practices and advice on how to best describe the benefits of SharePoint Online and how to use it for communication and scheduling.

Result

Your SharePoint Online IT pilot is complete and the initial change management materials have been developed, reviewed, and refined.

Step 3: Roll out to a business group

After completing your IT pilot, roll out SharePoint Online to a business group or department in your organization. This rollout should include:

- Identification of key business scenarios for SharePoint Online within the business group.
- Announcement activities to inform users of the expectations and timelines for SharePoint Online usage for departments and work or project teams.
- Migration of on-premises folders and documents of your business group members to SharePoint Online.

- Delivering user training or links to resources to introduce SharePoint Online and how to use it. See [SharePoint Online](#) video training.
- A feedback mechanism, such as a central Microsoft Teams team containing everyone in the business group, to collect comments and act on issues from users in the business group.

During the rollout, you can refine your change management materials in preparation for the organization-wide rollout.

Result

A business group is up and running with SharePoint Online and the change management materials have been tested and refined.

Phase 3: Drive value

In this phase, you complete the rollout of SharePoint Online support your users to help them realize its benefits.

Step 1: Roll out to the rest of your organization

The rollout to the rest of your organization should include:

- Identification of key business scenarios for SharePoint Online within separate business groups.
- Use of your refined change management materials for announcement activities to inform your organization of the expectations and timelines for usage.
- Migration of folders and documents for the rest of your organization to SharePoint Online.
- Delivering user training or provide links to resources to introduce SharePoint Online and how to use it.
- A feedback mechanism, such as a central Team containing everyone, to collect comments and issues from organization users. If your organization has less than 2500 individuals, use a public channel in Teams. Otherwise, use a public group in Yammer.

Result

Your organization is up and running and your change management strategy is in place to inform, train, and enable users to use SharePoint Online.

Step 2: Measure usage, manage satisfaction, and drive adoption

After rolling out to your entire organization, you must continue to employ your change management strategy to:

- Have your leadership promote SharePoint Online as the primary tool for document storage and sharing and team, division, or organization-wide collaboration.
- Encourage individuals to use it for business group, departmental, work, and project team collaboration and calendaring.

Here are some suggested activities:

- See [Office 365 adoption guidance](#) to learn about general best practices for cloud service adoption.
- See [Office 365 activity reports](#) to understand Office 365 service usage across your organization. If you aren't an Office 365 global admin for your organization, ask someone who is a global admin to grant Reports Reader permissions to your user account so you can access activity reports.
- Monitor your feedback venue (a public channel in a central Teams team or Yammer) for issues and feedback from individuals about their experiences with SharePoint Online. Address questions and issues as quickly as you can to prevent frustrated individuals and demonstrate support for the rollout.
- Identify and nurture champions in each business group and highlight their accomplishments and best practices by using SharePoint Online. Reflect their successes out to the organization to show project success and adoption. Endorsement by technical leaders within a business group can exert a powerful influence over leaders and peers.

Result

Your organization has adopted SharePoint Online as a service to support documentation storage and collaboration.

How Microsoft does Microsoft 365 Enterprise

To peek inside Microsoft and learn how the company deployed SharePoint Online, see [SharePoint to the cloud: Learn how Microsoft ran its own migration](#).

Next steps

See these resources for the ongoing maintenance of SharePoint Online:

- [Understanding permission levels in SharePoint](#)
- [Customize SharePoint site permissions](#)
- [Turn external sharing on or off for SharePoint Online](#)
- [Set up and manage access requests](#)

Migration to Microsoft 365 Enterprise

2/13/2019 • 6 minutes to read • [Edit Online](#)

Most enterprise organizations have a heterogeneous environment with multiple releases of operating systems, client software, and server software. Microsoft 365 Enterprise includes the most secure versions of these key components of your IT infrastructure with productivity features that are designed to take advantage of cloud technologies.

To maximize the business value of the Microsoft 365 Enterprise integrated suite of products, begin planning and implementing a strategy to migrate releases of:

- The Office client installed on your computers to Office 365 ProPlus
- Office servers installed on your servers to their equivalent services in Office 365
- Windows 7 and Windows 8.1 on your devices to Windows 10 Enterprise

Accomplishing all of these migrations over time gets your organization closer to the [modern workplace](#), a secure and integrated environment that unlocks teamwork and creativity in your organization, all of which is enabled and empowered by Microsoft 365 Enterprise.

For information about migrating users and data for specific Office 365 workloads:

- User mailboxes from Exchange Server to Exchange Online, see the [Exchange Online workload](#).
- SharePoint data from SharePoint Server to SharePoint Online, see the [SharePoint Online workload](#).
- Skype for Business Online to Microsoft Teams, see the [Microsoft Teams workload](#).

Migration for Microsoft Office client products

In many organizations both large and small, you might be using a combination of older versions of the Office client products, such as Word, Excel, and PowerPoint. These older versions:

- Can be [updated](#) with the latest security updates and support fixes, but the process is sometimes manual and might not scale across your organization.
- Are not optimally enabled to leverage Microsoft's cloud technologies and help you digitally transform your business.

Microsoft 365 Enterprise includes Office 365 ProPlus, a version of the Office client products that is available with a Microsoft 365 Enterprise license and is installed and updated from the Microsoft cloud. See [About Office 365 ProPlus in the enterprise](#) for more information.

Office 2007

For versions of Office in the Office 2007 release, the end of support has already passed. See [Office 2007 End of Support Roadmap](#) for more information.

Rather than upgrading your computers running Office 2007 with Office 2010, Office 2013, or Office 2016, consider:

1. Obtaining and assigning a Microsoft 365 license for your users.
2. Uninstalling Office 2007 on their computers.
3. Installing Office 365 ProPlus, either individually or in conjunction with an IT rollout. For more information, see [Phase 4: Office 365 ProPlus](#).

Office 365 ProPlus installs updates automatically and can take advantage of cloud-based services in Office 365 for

enhanced security and productivity.

Office 2010

For versions of Office in the Office 2010 release, the end of support is October 13, 2020. For more information, see [Office 2010 end of support roadmap](#).

Rather than upgrading your computers running Office 2010 with Office 2013 or Office 2016, both of which must be manually updated, consider:

1. Obtaining and assigning a Microsoft 365 license for your users.
2. Uninstalling Office 2010 on their computers.
3. Installing Office 365 ProPlus, either individually or in conjunction with an IT rollout. For more information, see [Phase 4: Office 365 ProPlus](#).

Office 365 ProPlus installs updates automatically and can take advantage of cloud-based services in Office 365 for enhanced security and productivity.

Office 2013 and Office 2016

The end of support roadmap for the Office 2013 and Office 2016 versions of Office has not yet been determined. However, like Office 2010, you must still [install updates](#), which might not scale well depending on the size of your organization. Rather than keep updating your computers with the latest updates for Office 2013 or Office 2016 or update your computers from Office 2013 to Office 2016, consider:

1. Obtaining and assigning a Microsoft 365 license for your users.
2. Uninstalling Office 2013 or Office 2016 on their computers.
3. Installing Office 365 ProPlus, either individually or in conjunction with an IT rollout. For more information, see [Phase 4: Office 365 ProPlus](#).

Office 365 ProPlus installs updates automatically and can take advantage of cloud-based services in Office 365 for enhanced security and productivity.

Migration for Microsoft Office server products

In many organizations both large and small, you might be using a combination of older versions of the Office Server products, such as Exchange Server and SharePoint Server. These older versions:

- Should be updated with the latest security updates and support fixes. In some cases, these updates are released monthly.
- Are not optimally enabled to leverage Microsoft's cloud technologies and help you digitally transform your business.
- Do not include new productivity applications, such as Microsoft Teams.
- Do not include the latest security features, such as Exchange Advanced Threat Protection.

Microsoft 365 Enterprise includes Office 365, which includes cloud-based versions of Office server services that use some of the same tools as on-premises versions of Office server software, such as web browsers and the Outlook client. These services are continually updated without involving IT, saving you the time it takes to maintain and update on-premises servers. These services also have enhancements not present in Office server software.

Office Server 2007

For server products in the Office 2007 release, the end of support has already passed. See these articles for the details:

- [Exchange 2007 end of support roadmap](#)
- [SharePoint Server 2007 end of support roadmap](#)
- [Project Server 2007 end of support roadmap](#)

- [Office Communications Server end of support roadmap](#)
- [PerformancePoint Server 2007 end of support roadmap](#)

Rather than upgrading your server products in the Office 2007 release with server products in the Office 2010, Office 2013, or Office 2016 releases, consider:

1. Migrating the data on your Office 2007 servers to Office 365. To help with this, hire a Microsoft partner.
2. Rolling out the new functionality and work processes to your users.
3. When there is no longer a need for the on-premises servers running Office 2007 server products, decommissioning them.

Office Server 2010

For server products in the Office 2010 release, the end of support has been determined for the following:

- [Exchange Server 2010](#)
- [SharePoint Server 2010](#)

Rather than upgrading these server products in the Office 2010 release with server products in the Office 2013 or Office 2016 release, consider:

1. Migrating the data on your Office 2010 servers to Office 365. To help with this, see [FastTrack for Microsoft 365](#) or hire a Microsoft partner.
2. Rolling out the new functionality and work processes to your users.
3. When there is no longer a need for the on-premises servers running Office 2010 server products, decommissioning them.

Office Server 2013

For server products in the Office 2013 release, the end of support has not been determined. Rather than upgrading your server products in the Office 2013 release with server products in the Office 2016 release, consider:

1. Migrating the data on your Office 2013 servers to Office 365. To help with this, see [FastTrack for Microsoft 365](#) or hire a Microsoft partner.
2. Rolling out the new functionality and work processes to your users.
3. When there is no longer a need for the on-premises servers running Office 2013 server products, decommissioning them.

Office Server 2016

For server products in the Office 2016 release, the end of support has not been determined. To take advantage of the cloud-based service and enhancements to digitally transform your business, consider:

1. Migrating the data on your Office 2016 servers to Office 365. To help with this, see [FastTrack for Microsoft 365](#) or hire a Microsoft partner.
2. Rolling out the new functionality and work processes to your users.
3. When there is no longer a need for the on-premises servers running Office 2016 server products, decommissioning them.

Migration for Microsoft Windows

To migrate your devices running Windows 7 or Windows 8.1, you can perform an [in-place upgrade](#).

For additional methods, see [Windows 10 deployment scenarios](#). You can also [plan for Windows 10 deployment](#) on your own.

How Microsoft does Microsoft 365 Enterprise

See how IT experts at Microsoft migrated the company to Microsoft 365 Enterprise with these resources:

- [Deploying and updating Microsoft Office 365 ProPlus](#)
- [Microsoft migrates 150,000 mailboxes to Exchange Online](#)
- [SharePoint to the cloud: Learn how Microsoft ran its own migration](#)
- [Deploying Windows 10 at Microsoft as an in-place upgrade](#)
- [Windows 10 deployment: tips and tricks from Microsoft IT](#) (video)

Result

Your organization has migrated older versions of Microsoft Office, Office servers, and Windows to Microsoft 365 Enterprise.

Microsoft Teams and SharePoint Online sites for highly regulated data

2/13/2019 • 9 minutes to read • [Edit Online](#)

This scenario applies to both the E3 and E5 versions of Microsoft 365 Enterprise

Microsoft 365 Enterprise includes a full suite of cloud-based services so that you can create, store, and secure your highly regulated data. This includes data that is:

- Subject to regional regulations.
- The most valuable data for your organization, such as trade secrets, financial or human resources information, and organization strategy.

A Microsoft 365 Enterprise cloud-based solution that meets this business need requires that you:

- Store digital assets (documents, slide decks, spreadsheets, etc.) in a SharePoint Online team site or in the **Files** tab of a Microsoft Teams team.
- Lock down the site or team to prevent:
 - Access to all except a specific set of user accounts through group membership, which includes those who can access the SharePoint Online team site and at what level of permission, and those who can administer it.
 - Members of the site from granting access to others.
 - Non-members of the site from requesting access to the site.
- Configure an Office 365 retention label for your SharePoint Online sites or teams as a default way to classify digital assets on the site.
- Block users from sending files outside the organization.
- Encrypt the most sensitive digital assets of the site or team.
- Add permissions to the most sensitive digital assets so that if even if they get shared outside of the site, opening the asset still requires the valid credentials of a user account that has permission.

The following table maps the requirements of this solution to a feature of Microsoft 365 Enterprise.

Requirement	Microsoft 365 Enterprise feature
Store digital assets	SharePoint Online team sites and teams in Office 365
Lock down the site	Azure AD groups and SharePoint Online team site permissions
Label the digital assets of the site	Office 365 retention labels
Block users when sending files outside the organization	Data Loss Prevention (DLP) policies in Office 365
Encrypt all of the digital assets of the site	Azure Information Protection sub-labels in Enterprise Mobility + Security (EMS)
Add permissions to the digital assets of the site	Azure Information Protection sub-labels in EMS

This solution requires that you have already deployed:

- Your [foundation infrastructure](#).
- For highly regulated data in SharePoint Online team sites, [SharePoint Online](#).
- For highly regulated data in Microsoft Teams teams, [Microsoft Teams](#).

The following phases step you through the design, configuration, and driving adoption for SharePoint Online sites and teams for highly regulated data.

To see how the Contoso Corporation, a fictional but representative multi-national organization, designed a SharePoint Online site for its research teams, see this [example configuration](#).

NOTE

A team for highly regulated data requires that you first create a SharePoint Online team site for highly regulated data. You then create a new team that uses the Office 365 group of the SharePoint Online team site. See Phase 2, Step 4 for more information.

Identity and device access prerequisites

To protect access to the team or SharePoint Online site, ensure that you have configured [identity and device access policies](#) and the [recommended SharePoint Online access policies](#).

Phase 1: Design

To create a SharePoint Online site or team for highly regulated data, you must first identify its purpose. For example, the research and development department of a manufacturing organization needs a SharePoint Online site to store current design specifications for existing products and a place to collaborate on new products. Only members of the Research & Development department and selected executives will be allowed to access the site.

That purpose will drive the determination of essential configuration items such as:

- The set of SharePoint Online permission sets and SharePoint groups
- The set of access groups, the Azure AD security groups and their members to add to the SharePoint groups
- The Office 365 retention label to assign to the site and the set of DLP policies for the label
- The settings of an Azure Information Protection sub-label that users apply to highly sensitive digital assets stored in the site

Once determined, you use these settings to configure the site in Phase 2.

Step 1: An isolated SharePoint Online site

The locked-down version of a SharePoint Online team site is known as an isolated site. Unlike the default settings of private team sites, isolated sites are configured to prevent:

- Access to those who are not members of specified groups.
- The requesting of access.
- The unauthorized granting of access by current members of specified groups.
- Administration of the site by access group members.

The security of SharePoint Online team sites that contain highly regulated assets do not change unless done by a SharePoint administrator for the site.

See [Design an isolated SharePoint Online team site](#) for the details to determine the set of permission levels, SharePoint groups, access groups, and group members.

Step 2: Office 365 retention labels and DLP policies

When applied to a SharePoint Online team site, Office 365 retention labels provide a default method of classifying all digital assets stored on the site.

For SharePoint Online sites for highly regulated data, you need to determine which Office 365 retention label to use.

For the design considerations of Office 365 labels, see [Office 365 classification and labels](#).

To protect sensitive information and prevent its accidental or intentional disclosure, you use DLP policies. For more information, see this [overview](#).

For SharePoint Online sites for highly regulated data, you must configure a DLP policy for the Office 365 retention label assigned to the site to block users when they attempt to share digital assets with external users.

Step 3: Your Azure Information Protection sub-label

To provide encryption and a set of permissions to your most sensitive digital assets, users must apply an Azure Information Protection label using the Azure Information Protection client. To use Azure Information Protection labels for SharePoint Online sites for highly regulated data, you must configure an Azure Information Protection sub-label in a scoped policy.

A sub-label exists under an existing label. For example, you can create a Research & Development sub-label under the Highly Confidential label. A scoped policy is one that applies only to a subset of users. For SharePoint Online sites for highly regulated data, the scope is the set of users that are members of the access groups for the site.

The settings of the applied sub-label travel with the asset. Even if it is downloaded and shared outside the site, only authenticated user accounts that have permissions can open it.

For the design considerations of Azure Information Protection labels, see [Azure Information Protection](#).

Design results

You have determined the following:

- The set of SharePoint groups and permission levels
- The set of access groups and their members for each permission level
- The appropriate Office 365 retention label and the DLP policy that is associated with the label
- The settings of the Azure Information Protection sub-label that include encryption and permissions

Phase 2: Configure

In this phase, you take the settings determined in Phase 1 and implement them to create a SharePoint Online site for highly regulated data.

Step 1: Create and configure an isolated SharePoint Online team site

Use the instructions in [Deploy an isolated SharePoint Online team site](#) to:

- Create and populate the access groups for each SharePoint permission level used on the site.
- Create and configure the isolated team site.

Step 2: Configure the site for an Office 365 retention label DLP policy

Use the instructions in [Protect SharePoint Online files with Office 365 labels and DLP](#) to:

- Identify or create the Office 365 retention label and apply it to your isolated SharePoint Online site.
- Create and configure the DLP policy that blocks users when they attempt to share a digital asset on your

SharePoint Online site outside the organization.

Step 3: Create an Azure Information Protection sub-label for the site

Use the instructions in [Protect SharePoint Online files with Azure Information Protection](#) to:

- Create and configure an Azure Information Protection sub-label in a scoped policy.
- Deploy the Azure Information Protection client to user computers.

Step 4 (optional): Create a team for the highly regulated data

If you want a team for highly regulated data, you first create a SharePoint Online site for highly regulated data. When you create the initial private SharePoint Online team site, you specify an Office 365 group name.

After the SharePoint Online site for highly regulated data is fully configured, use these steps to convert it into a team for highly regulated data:

1. Sign in to Office 365.
2. From the **Microsoft Office Home** tab, click **Teams**.
3. From the **Microsoft Teams** tab, in the **Join or create a team** pane, click **Create team**.
4. In the **Create your team** pane, click **Create a team from an existing Office 365 group**.
5. In the list of Office 365 groups, select the name of the Office 365 group corresponding to the SharePoint Online site for highly regulated data, and then click **Choose team**.

The **Files** tab of the new team lists the contents of the **General** folder of the **Documents** area of the corresponding SharePoint Online site. To see the rest of the resources of the SharePoint Online site for the team, click the ellipsis, and then click **Open in SharePoint**.

Configuration results

You have configured the following:

- A SharePoint Online isolated site
- An Office 365 retention label assigned to the SharePoint Online isolated site
- A DLP policy for the Office 365 retention label
- An Azure Information Protection sub-label of a scoped policy that users can apply to the most sensitive digital assets stored in the site that encrypts the asset and enforces permissions
- If needed, a team for highly regulated data based on the SharePoint Online site

Phase 3: Drive user adoption

A SharePoint Online site or team for highly regulated data can only protect that data if it is consistently used for storage and access of sensitive digital assets. This is the hardest phase because it relies on users changing their ways.

For example, executives that are used to storing sensitive files on USB drives or on personal cloud-based storage solutions will now have to store them exclusively in a SharePoint Online site or team for highly regulated data.

Step 1: Train your users

After completing your configuration, train the set of users who are members of the site access groups:

- On the importance of using the new site or team to protect valuable assets and the consequences of a highly regulated data leak, such as legal ramifications, regulatory fines, ransomware, or loss of competitive advantage.
- How to access the site and its assets.
- How to create new files on the site and upload new files stored locally.
- How the DLP policy blocks them from sharing files externally.
- How to use the Azure Information Protection client to label the most sensitive digital assets with the configured sub-label.

- How the Azure Information Protection sub-label protects an asset even when it is leaked off the site or team.

This training should include hands-on exercises so that the users can experience these operations and their results.

Step 2: Conduct periodic reviews of usage and files

In the weeks after training, the SharePoint administrator for the SharePoint Online site or team can:

- Analyze usage for the site or team and compare it with usage expectations.
- Verify that highly sensitive files have been properly labeled with the Azure Information Protection sub-label.

Retrain your users as needed.

User adoption results

Sensitive digital assets are stored exclusively on SharePoint Online sites or teams for highly regulated data and that the most sensitive assets have the configured Azure Information Protection sub-label applied.

See also

[Deployment guide](#)

[Test lab guides](#)

[Secure SharePoint Online sites in a dev/test environment](#)

Microsoft 365 Enterprise Test Lab Guides

2/13/2019 • 2 minutes to read • [Edit Online](#)

Test Lab Guides (TLGs) help you quickly learn about Microsoft products. They provide prescriptive instructions to configure simplified but representative test environments. You can use these environments for demonstration, customization, or creation of complex proofs of concept for the duration of a trial or paid subscription.

TLGs are designed to be modular. They build upon each other to create multiple configurations that more closely match your learning or test configuration needs. The "I built it out myself and it works" hands-on experience helps you understand the deployment requirements of a new product or scenario so you can better plan for hosting it in production.

You can also use TLGs to create representative environments for development and testing of applications, also known as dev/test environments.



TIP

Click [here](#) for a visual map to all the articles in the Microsoft 365 Enterprise Test Lab Guide stack.

Base configuration

First, you create a test environment for [Microsoft 365 Enterprise](#) that includes Office 365 E5, Enterprise Mobility + Security (EMS) E5, and Windows 10 Enterprise. You can create two different types of base configurations:

- Use the [lightweight base configuration](#) when you want to configure and demonstrate Microsoft 365 Enterprise features and capabilities in a cloud-only environment, which does not include any on-premises components.
- Use the [simulated enterprise base configuration](#) when you want to configure and demonstrate Microsoft 365 Enterprise features and capabilities in a hybrid cloud environment, which uses on-premises components such as an Active Directory Domain Services (AD DS) domain.

Identity

To demonstrate identity-related features and capabilities, see:

- [Password hash synchronization](#)

Enable and test password hash-based directory synchronization from a Windows Server AD domain controller.

- [Pass-through authentication](#)

Enable and test pass-through authentication to a Windows Server AD domain controller.

- [Azure AD Seamless Single Sign-on](#)

Enable and test Azure AD Seamless Single Sign-on (SSO) with a Windows Server AD domain controller.

- [Multi-factor authentication](#)

Enable and test smart phone-based multi-factor authentication for a specific user account.

- [Protect global administrator accounts](#)

Lock down your global administrator accounts with Office 365 Cloud App Security and conditional access policies.

- [Password reset](#)

Use self-service password reset (SSPR) to reset your password.

- [Password writeback](#)

Use password writeback to change the password on your Windows Server AD user account from Azure AD.

- [Automatic licensing and group membership](#)

Make administering new accounts easier than ever with automatic licensing and dynamic group membership.

- [Azure AD Identity Protection](#)

Scan your current user accounts for vulnerabilities.

Mobile device management

To demonstrate mobile device management-related features and capabilities, see:

- [Device compliance policies](#)

Create a user group and a device compliance policy for Windows 10 devices.

- [Enroll iOS and Android devices](#)

Enroll iOS or Android devices and manage them remotely.

Information protection

To demonstrate information protection-related features and capabilities, see:

- [Increased Office 365 security](#)

Configure settings for increased Office 365 security and investigate built-in security tools.

- [Data classification](#)

Configure and apply Office 365 labels to a document in a SharePoint Online team site.

- [Privileged access management](#)

Configure privileged access management for just-in-time access to elevated and privileged tasks in your Office 365 organization.

See also

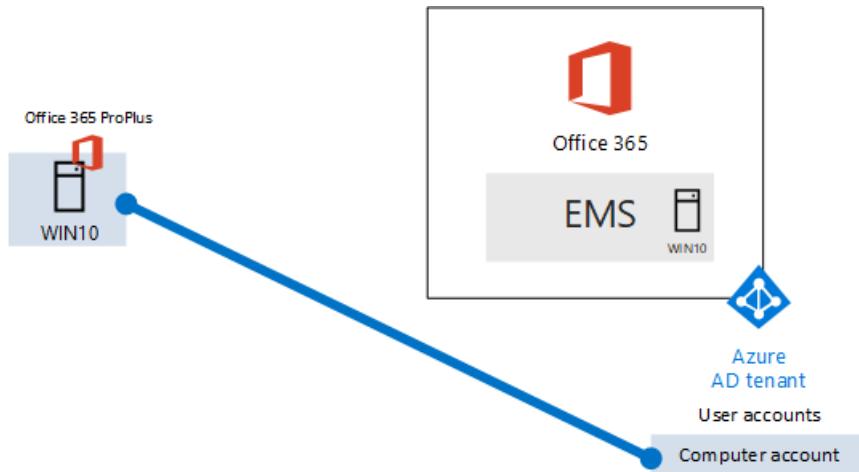
[Experience the Microsoft Cloud with Cloud Adoption Test Lab Guides](#)

One Microsoft Cloud Test Lab Guide stack

The lightweight base configuration

2/13/2019 • 6 minutes to read • [Edit Online](#)

This article provides you with step-by-step instructions to create a simplified environment that includes Office 365 E5, Enterprise Mobility + Security (EMS) E5, and a computer running Windows 10 Enterprise.



Use the resulting environment to test the features and functionality of [Microsoft 365 Enterprise](#).



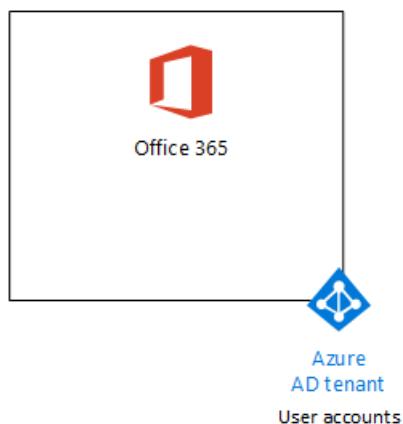
TIP

Click [here](#) for a visual map to all the articles in the Microsoft 365 Enterprise Test Lab Guide stack.

Phase 1: Create your Office 365 E5 subscription

Follow the steps in Phase 2 and Phase 3 of the [Office 365 dev/test environment](#) to create a lightweight Office 365 dev/test environment, as shown in Figure 1.

Figure 1: Your Office 365 E5 subscription with its Azure Active Directory (Azure AD) tenant and user accounts



NOTE

The Office 365 E5 trial subscription is 30 days, which can be easily extended to 60 days. For a permanent test environment, create a new paid subscription with a small number of licenses.

Phase 2: Add EMS

In this phase, you sign up for the EMS E5 trial subscription and add it to the same organization as your Office 365 E5 trial subscription.

First, add the EMS E5 trial subscription and assign an EMS license to your global administrator account.

1. With a private instance of an Internet browser, sign in to the Office portal with your global administrator account credentials. For help, see [Where to sign in to Office 365](#).
2. Click the **Admin** tile.
3. On the **Office Admin center** tab in your browser, in the left navigation, click **Billing > Purchase services**.
4. On the **Purchase services** page, find the **Enterprise Mobility + Security E5** item. Hover your mouse pointer over it and click **Start free trial**.
5. On the **Confirm your order** page, click **Try now**.
6. On the **Order receipt** page, click **Continue**.
7. On the **Office 365 Admin center** tab in your browser, in the left navigation, click **Users > Active users**.
8. Click your global administrator account, and then click **Edit for Product licenses**.
9. On the **Product licenses** pane, turn the product license for **Enterprise Mobility + Security E5** to **On**, click **Save**, and then click **Close** twice.

NOTE

The Enterprise Mobility + Security E5 trial subscription is 90 days. For a permanent test environment, create a new paid subscription with a small number of licenses.

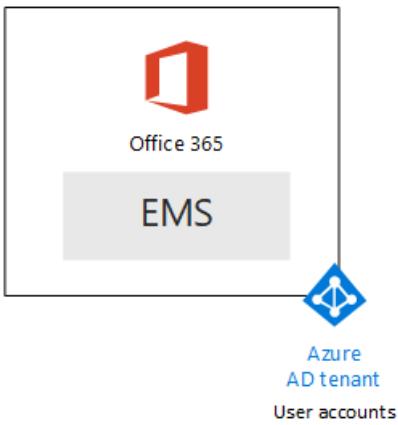
If you completed Phase 3 of the Office 365 dev/test environment, repeat steps 8 and 9 of the previous procedure for all of your other accounts (User 2, User 3, User 4, and User 5).

Your test environment now has:

- Office 365 E5 Enterprise and EMS E5 trial subscriptions sharing the same Azure AD tenant with your list of user accounts.
- All your appropriate user accounts (either just the global administrator or all five user accounts) are enabled to use Office 365 E5 and EMS E5.

Figure 2 shows your resulting configuration, which adds EMS.

Figure 2: Adding the EMS trial subscription



Phase 3: Create a Windows 10 Enterprise computer

In this phase, you create a standalone computer running Windows 10 Enterprise as either a physical computer, a virtual machine, or an Azure virtual machine.

Physical computer

Obtain a personal computer and install Windows 10 Enterprise on it. You can download the Windows 10 Enterprise trial [here](#).

Virtual machine

Create a virtual machine using the hypervisor of your choice and install Windows 10 Enterprise on it. You can download the Windows 10 Enterprise trial [here](#).

Virtual machine in Azure

To create a Windows 10 virtual machine in Microsoft Azure, ***you must have a Visual Studio-based subscription***, which has access to the image for Windows 10 Enterprise. Other types of Azure subscriptions, such as trial and paid subscriptions, do not have access to this image. For the latest information, see [Use Windows client in Azure for dev/test scenarios](#).

NOTE

The following command sets use the latest version of Azure PowerShell. See [Get started with Azure PowerShell cmdlets](#). These command sets build a Windows 10 Enterprise virtual machine named WIN10 and all of its required infrastructure, including a resource group, a storage account, and a virtual network. If you are already familiar with Azure infrastructure services, please adapt these instructions to suit your currently deployed infrastructure.

First, start a Microsoft PowerShell prompt.

Sign in to your Azure account with the following command.

```
Login-AzureRMAccount
```

Get your subscription name using the following command.

```
Get-AzureRMSubscription | Sort Name | Select Name
```

Set your Azure subscription. Replace everything within the quotes, including the < and > characters, with the correct name.

```
$subscr=<subscription name>
Get-AzureRmSubscription -SubscriptionName $subscr | Select-AzureRmSubscription
```

Next, create a new resource group. To determine a unique resource group name, use this command to list your existing resource groups.

```
Get-AzureRMResourceGroup | Sort ResourceGroupName | Select ResourceGroupName
```

Create your new resource group with these commands. Replace everything within the quotes, including the < and > characters, with the correct names.

```
$rgName=<resource group name>
$locName=<location name, such as West US>
New-AzureRMResourceGroup -Name $rgName -Location $locName
```

Next, you create a new virtual network and the WIN10 virtual machine with these commands. When prompted, provide the name and password of the local administrator account for WIN10 and store these in a secure location.

```
$corpNetSubnet=New-AzureRMVirtualNetworkSubnetConfig -Name Corpnet -AddressPrefix 10.0.0.0/24
New-AzureRMVirtualNetwork -Name "M365Ent-TestLab" -ResourceGroupName $rgName -Location $locName -
AddressPrefix 10.0.0.0/8 -Subnet $corpNetSubnet
$rule1=New-AzurermNetworkSecurityRuleConfig -Name "RDPTraffic" -Description "Allow RDP to all VMs on the
subnet" -Access Allow -Protocol Tcp -Direction Inbound -Priority 100 -SourceAddressPrefix Internet -
SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange 3389
New-AzurermNetworkSecurityGroup -Name Corpnet -ResourceGroupName $rgName -Location $locName -SecurityRules
$rule1
$vnet=Get-AzureRMVirtualNetwork -ResourceGroupName $rgName -Name "M365Ent-TestLab"
$nsg=Get-AzurermNetworkSecurityGroup -Name Corpnet -ResourceGroupName $rgName
Set-AzureRMVirtualNetworkSubnetConfig -VirtualNetwork $vnet -Name Corpnet -AddressPrefix "10.0.0.0/24" -
NetworkSecurityGroup $nsg
$PIP=New-AzureRMPublicIpAddress -Name WIN10-PIP -ResourceGroupName $rgName -Location $locName -
AllocationMethod Dynamic
$nic=New-AzurermNetworkInterface -Name WIN10-NIC -ResourceGroupName $rgName -Location $locName -SubnetId
$vnet.Subnets[0].Id -PublicIpAddressId $PIP.Id
$vm=New-AzurermVMConfig -VMName WIN10 -VMSize Standard_D1_V2
$cred=Get-Credential -Message "Type the name and password of the local administrator account for WIN10."
$vm=Set-AzurermVMOperatingSystem -VM $vm -Windows -ComputerName WIN10 -Credential $cred -ProvisionVMAgent -
EnableAutoUpdate
$vm=Set-AzurermVMSourceImage -VM $vm -PublisherName MicrosoftWindowsDesktop -Offer Windows-10 -Skus RS3-Pro -
Version "latest"
$vm=Add-AzurermVMNetworkInterface -VM $vm -Id $nic.Id
$vm=Set-AzurermVMOSDisk -VM $vm -Name WIN10-TestLab-OSDisk -DiskSizeInGB 128 -CreateOption FromImage
New-AzurermVM -ResourceGroupName $rgName -Location $locName -VM $vm
```

Phase 4: Join your Windows 10 computer to Azure AD

After the physical or virtual machine with Windows 10 Enterprise is created, sign in with a local administrator account.

NOTE

For a virtual machine in Azure, connect to it using [these instructions](#).

Next, join the WIN10 computer to the Azure AD tenant of your Office 365 and EMS subscriptions.

1. At the desktop of the WIN10 computer, click **Start > Settings > Accounts > Access work or school > Connect**.
2. In the **Set up a work or school account** dialog box, click **Join this device to Azure Active Directory**.
3. In **Work or school account**, type the global administrator account name of your Office 365 subscription, and then click **Next**.
4. In **Enter password**, type the password for your global administrator account, and then click **Sign in**.
5. When prompted to make sure this is your organization, click **Join**, and then click **Done**.
6. Close the settings window.

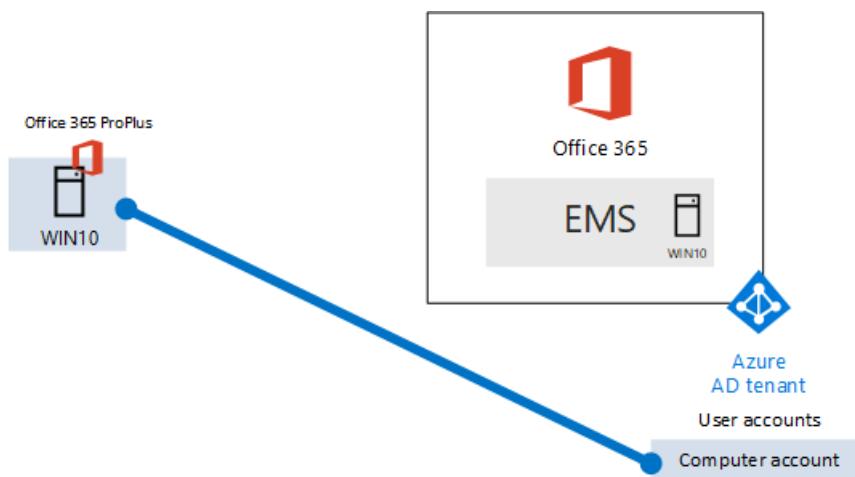
Next, install Office 365 ProPlus on the WIN10 computer.

1. Open the Microsoft Edge browser and sign in to the Office portal with your global administrator account credentials. For help, see [Where to sign in to Office 365](#).
2. On the **Microsoft Office Home** tab, click **Install Office 2016**.
3. When prompted with what to do, click **Run**, and then click **Yes** for **User Account Control**.
4. Wait for Office to complete its installation. When you see **You're all set!**, click **Close** twice.

Figure 3 shows your resulting environment, which includes the WIN10 computer that has:

- Joined the Azure AD tenant of your Office 365 and EMS subscriptions.
- Enrolled as an Azure AD device in Intune (EMS).
- Has Office 365 ProPlus installed.

Figure 3: The final configuration of the Microsoft 365 test environment



You are now ready to experiment with additional features of [Microsoft 365 Enterprise](#).

Next steps

Explore these additional sets of Test Lab Guides:

- [Identity](#)
- [Mobile device management](#)
- [Information protection](#)

See also

[Microsoft 365 Enterprise Test Lab Guides](#)

[Deploy Microsoft 365 Enterprise](#)

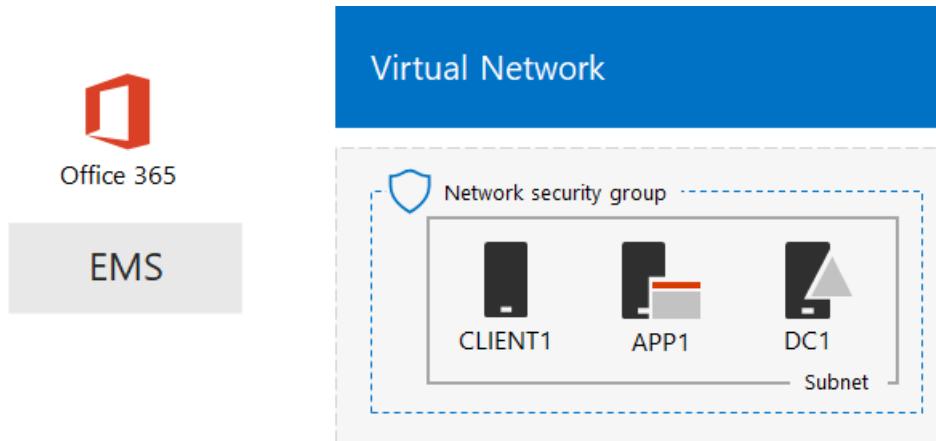
[Microsoft 365 Enterprise documentation](#)

The simulated enterprise base configuration

2/13/2019 • 13 minutes to read • [Edit Online](#)

This article provides you with step-by-step instructions to create a simplified environment for Microsoft 365 Enterprise that includes:

- Office 365 E5 and EMS E5 trial or permanent subscriptions.
- A simplified organization intranet connected to the Internet, consisting of three virtual machines on an Azure virtual network (DC1, APP1, and CLIENT1).



You can use the resulting environment to test the features and functionality of [Microsoft 365 Enterprise](#) with additional [Test Lab Guides](#) or on your own.



TIP

Click [here](#) for a visual map to all the articles in the Microsoft 365 Enterprise Test Lab Guide stack.

Phase 1: Create a simulated intranet

In this phase, you build a simulated intranet in Azure infrastructure services that includes an Active Directory Domain Services (AD DS) domain controller, an application server, and a client computer.

You'll use these computers in additional [Microsoft 365 Enterprise Test Lab Guides](#) to configure and demonstrate hybrid identity and other capabilities.

Method 1: Build your simulated intranet with an Azure Resource Manager template

In this method, you use an Azure Resource Manager (ARM) template to build out the simulated intranet. ARM templates contain all of the instructions to create the Azure networking infrastructure, the virtual machines, and their configuration.

Prior to deploying the template, read through the [template README page](#) and have the following information ready:

- The public DNS domain name of your test environment (testlab.<your public domain>). You'll need to enter

this name in the **Domain Name field** of the **Custom deployment** page.

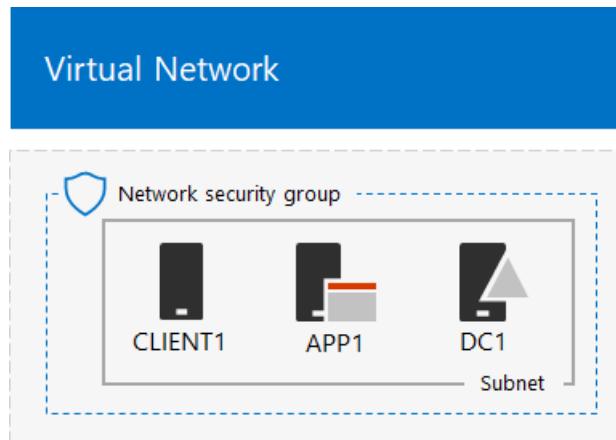
- A DNS label prefix for the URLs of the public IP addresses of your virtual machines. You'll need to enter this label in the **Dns Label Prefix** field of the **Custom deployment** page.

After reading through the instructions, click **Deploy to Azure** on the [template README page](#) to get started.

NOTE

The simulated intranet built by the ARM template requires a paid Azure subscription.

Here is your configuration after the template is complete.



Method 2: Build your simulated intranet with Azure PowerShell

In this method, you use Windows PowerShell and the Azure PowerShell module to build out the networking infrastructure, the virtual machines, and their configuration.

Use this method if you want to get experience creating elements of Azure infrastructure one step at a time with PowerShell. You can then customize the PowerShell command blocks for your own deployment of other virtual machines in Azure.

Step 1: Create DC1

In this step, we create an Azure virtual network and add DC1, a virtual machine that is a domain controller for an AD DS domain.

First, start a Windows PowerShell command prompt on your local computer.

NOTE

The following command sets use the latest version of Azure PowerShell. See [Get started with Azure PowerShell cmdlets](#).

Sign in to your Azure account with the following command.

```
Login-AzureRMAccount
```

Get your subscription name using the following command.

```
Get-AzureRMSubscription | Sort Name | Select Name
```

Set your Azure subscription. Replace everything within the quotes, including the < and > characters, with the correct name.

```
$subscr=<subscription name>
Get-AzureRmSubscription -SubscriptionName $subscr | Select-AzureRmSubscription
```

Next, create a new resource group for your simulated enterprise test lab. To determine a unique resource group name, use this command to list your existing resource groups.

```
Get-AzureRMResourceGroup | Sort ResourceGroupName | Select ResourceGroupName
```

Create your new resource group with these commands. Replace everything within the quotes, including the < and > characters, with the correct names.

```
$rgName=<resource group name>
$locName=<location name, such as West US>
New-AzureRMResourceGroup -Name $rgName -Location $locName
```

Next, you create the TestLab virtual network that will host the Corpnet subnet of the simulated enterprise environment and protect it with a network security group. Fill in the name of your resource group and run these commands at the PowerShell command prompt on your local computer.

```
$rgName=<name of your new resource group>
$locName=(Get-AzureRmResourceGroup -Name $rgName).Location
$corpnetSubnet=New-AzureRMVirtualNetworkSubnetConfig -Name Corpnet -AddressPrefix 10.0.0.0/24
New-AzureRMVirtualNetwork -Name TestLab -ResourceGroupName $rgName -Location $locName -AddressPrefix
10.0.0.0/8 -Subnet $corpnetSubnet -DNSServer 10.0.0.4
$rule1=New-AzurermNetworkSecurityRuleConfig -Name "RDPTraffic" -Description "Allow RDP to all VMs on the
subnet" -Access Allow -Protocol Tcp -Direction Inbound -Priority 100 -SourceAddressPrefix Internet -
SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange 3389
New-AzurermNetworkSecurityGroup -Name Corpnet -ResourceGroupName $rgName -Location $locName -SecurityRules
$rule1
$vnet=Get-AzureRMVirtualNetwork -ResourceGroupName $rgName -Name TestLab
$nsg=Get-AzurermNetworkSecurityGroup -Name Corpnet -ResourceGroupName $rgName
Set-AzureRMVirtualNetworkSubnetConfig -VirtualNetwork $vnet -Name Corpnet -AddressPrefix "10.0.0.0/24" -
NetworkSecurityGroup $nsg
```

Next, you create the DC1 virtual machine and configure it as a domain controller for the **testlab.<your public domain>** Windows Server AD domain and a DNS server for the virtual machines of the TestLab virtual network. For example, if your public domain name is **contoso.com**, the DC1 virtual machine will be a domain controller for the **testlab.contoso.com** domain.

To create an Azure virtual machine for DC1, fill in the name of your resource group and run these commands at the PowerShell command prompt on your local computer.

```

$rgName=<resource group name>
$locName=(Get-AzureRmResourceGroup -Name $rgName).Location
$vnet=Get-AzureRMVirtualNetwork -Name TestLab -ResourceGroupName $rgName
$pip>New-AzureRMPublicIpAddress -Name DC1-PIP -ResourceGroupName $rgName -Location $locName -AllocationMethod Dynamic
$nic>New-AzureRMNetworkInterface -Name DC1-NIC -ResourceGroupName $rgName -Location $locName -SubnetId $vnet.Subnets[0].Id -PublicIpAddressId $pip.Id -PrivateIpAddress 10.0.0.4
$vm>New-AzureRMVMConfig -VMName DC1 -VMSize Standard_A1
$cred=Get-Credential -Message "Type the name and password of the local administrator account for DC1."
$vm=Set-AzureRMVMOperatingSystem -VM $vm -Windows -ComputerName DC1 -Credential $cred -ProvisionVMAgent -EnableAutoUpdate
$vm=Set-AzureRMVMSourceImage -VM $vm -PublisherName MicrosoftWindowsServer -Offer WindowsServer -Skus 2016-Datacenter -Version "latest"
$vm=Add-AzureRMVMNetworkInterface -VM $vm -Id $nic.Id
$vm=Set-AzureRmVMOSDisk -VM $vm -Name "DC1-OS" -DiskSizeInGB 128 -CreateOption FromImage
$diskConfig=New-AzureRmDiskConfig -AccountType "Standard_LRS" -Location $locName -CreateOption Empty -DiskSizeGB 20
$dataDisk1=New-AzureRmDisk -DiskName "DC1-DataDisk1" -Disk $diskConfig -ResourceGroupName $rgName
$vm=Add-AzureRmVMDataDisk -VM $vm -Name "DC1-DataDisk1" -CreateOption Attach -ManagedDiskId $dataDisk1.Id -Lun 1
New-AzureRMVM -ResourceGroupName $rgName -Location $locName -VM $vm

```

You will be prompted for a user name and password for the local administrator account on DC1. Use a strong password and record both the name and password in a secure location.

Next, connect to the DC1 virtual machine.

1. In the [Azure portal](#), click **Resource Groups** > [the name of your new resource group] > **DC1** > **Connect**.
2. In the open pane, click **Download RDP file**. Open the DC1.rdp file that is downloaded, and then click **Connect**.
3. Specify the DC1 local administrator account name:
 - For Windows 7:
In the **Windows Security** dialog box, click **Use another account**. In **User name**, type **DC1**[Local administrator account name].
 - For Windows 8 or Windows 10:
In the **Windows Security** dialog box, click **More choices**, and then click **Use a different account**. In **User name**, type **DC1**[Local administrator account name].
4. In **Password**, type the password of the local administrator account, and then click **OK**.
5. When prompted, click **Yes**.

Next, add an extra data disk as a new volume with the drive letter F: with this command at an administrator-level Windows PowerShell command prompt on DC1.

```
Get-Disk | Where PartitionStyle -eq "RAW" | Initialize-Disk -PartitionStyle MBR -PassThru | New-Partition -AssignDriveLetter -UseMaximumSize | Format-Volume -FileSystem NTFS -NewFileSystemLabel "WSAD Data"
```

Next, configure DC1 as a domain controller and DNS server for the **testlab.<your public domain>** domain. Specify your public domain name, remove the < and > characters, and then run these commands at an administrator-level Windows PowerShell command prompt on DC1.

```
$yourDomain="<your public domain>"  
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools  
Install-ADDSForest -DomainName testlab.$yourDomain -DatabasePath "F:\NTDS" -SysvolPath "F:\SYSVOL" -LogPath  
"F:\Logs"
```

You will need to specify a safe mode administrator password. Store this password in a secure location.

Note that these commands can take a few minutes to complete.

After DC1 restarts, reconnect to the DC1 virtual machine.

1. In the [Azure portal](#), click **Resource Groups** > [your resource group name] > **DC1** > **Connect**.
2. Run the DC1.rdp file that is downloaded, and then click **Connect**.
3. In **Windows Security**, click **Use another account**. In **User name**, type **TESTLAB\Local administrator account name**.
4. In **Password**, type the password of the local administrator account, and then click **OK**.
5. When prompted, click **Yes**.

Next, create a user account in Active Directory that will be used when logging in to TESTLAB domain member computers. Run this command at an administrator-level Windows PowerShell command prompt.

```
New-ADUser -SamAccountName User1 -AccountPassword (read-host "Set user password" -assecurestring) -name  
"User1" -enabled $true -PasswordNeverExpires $true -ChangePasswordAtLogon $false
```

Note that this command prompts you to supply the User1 account password. Because this account will be used for remote desktop connections for all TESTLAB domain member computers, choose a strong password. Record the User1 account password and store it in a secured location.

Next, configure the new User1 account as a domain, enterprise, and schema administrator. Run this command at the administrator-level Windows PowerShell command prompt.

```
$yourDomain="<your public domain>"  
$domainName = "testlab"+$yourDomain  
$userName="user1@" + $domainName  
$userSID=(New-Object  
System.Security.Principal.NTAccount($userName)).Translate([System.Security.Principal.SecurityIdentifier]).Value  
$groupNames=@("Domain Admins","Enterprise Admins","Schema Admins")  
ForEach ($name in $groupNames) {Add-ADPrincipalGroupMembership -Identity $userSID -MemberOf (Get-ADGroup -  
Identity $name).SID.Value}
```

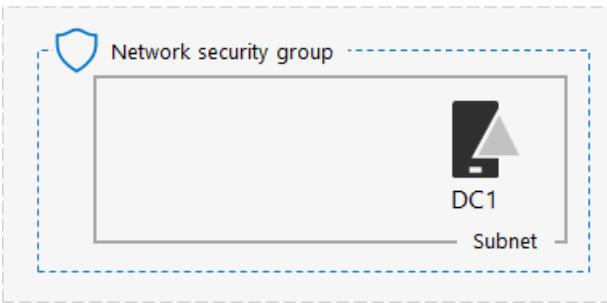
Close the Remote Desktop session with DC1 and then reconnect using the TESTLAB\User1 account.

Next, to allow traffic for the Ping tool, run this command at an administrator-level Windows PowerShell command prompt.

```
Set-NetFirewallRule -DisplayName "File and Printer Sharing (Echo Request - ICMPv4-In)" -enabled True
```

This is your current configuration.

Virtual Network



Step 2: Configure APP1

In this step, you create and configure APP1, which is an application server that initially provides web and file sharing services.

To create an Azure Virtual Machine for APP1, fill in the name of your resource group and run these commands at the command prompt on your local computer.

```
$rgName=<resource group name>
$locName=(Get-AzureRmResourceGroup -Name $rgName).Location
$vnet=Get-AzureRMVirtualNetwork -Name TestLab -ResourceGroupName $rgName
$PIP>New-AzureRMPublicIpAddress -Name APP1-PIP -ResourceGroupName $rgName -Location $locName -AllocationMethod Dynamic
$nic>New-AzureRMNetworkInterface -Name APP1-NIC -ResourceGroupName $rgName -Location $locName -SubnetId $vnet.Subnets[0].Id -PublicIpAddressId $PIP.Id
$vm>New-AzureRMVMConfig -VMName APP1 -VMSize Standard_A1
$cred=Get-Credential -Message "Type the name and password of the local administrator account for APP1."
$vm=Set-AzureRMVMOperatingSystem -VM $vm -Windows -ComputerName APP1 -Credential $cred -ProvisionVMAgent -EnableAutoUpdate
$vm=Set-AzureRMVMSourceImage -VM $vm -PublisherName MicrosoftWindowsServer -Offer WindowsServer -Skus 2016-Datacenter -Version "latest"
$vm=Add-AzureRMVMNetworkInterface -VM $vm -Id $nic.Id
$vm=Set-AzureRmVMOSDisk -VM $vm -Name "APP1-OS" -DiskSizeInGB 128 -CreateOption FromImage
New-AzureRMVM -ResourceGroupName $rgName -Location $locName -VM $vm
```

Next, connect to the APP1 virtual machine using the APP1 local administrator account name and password, and then open a Windows PowerShell command prompt.

To check name resolution and network communication between APP1 and DC1, run the **ping dc1.testlab.<your public domain name>** command and verify that there are four replies.

Next, join the APP1 virtual machine to the TESTLAB domain with these commands at the Windows PowerShell prompt.

```
$yourDomain=<your public domain name>
Add-Computer -DomainName ("testlab" + $yourDomain)
Restart-Computer
```

Note that you must supply the TESTLAB\User1 domain account credentials after running the **Add-Computer** command.

After APP1 restarts, connect to it using the TESTLAB\User1 account, and then open an administrator-level Windows PowerShell command prompt.

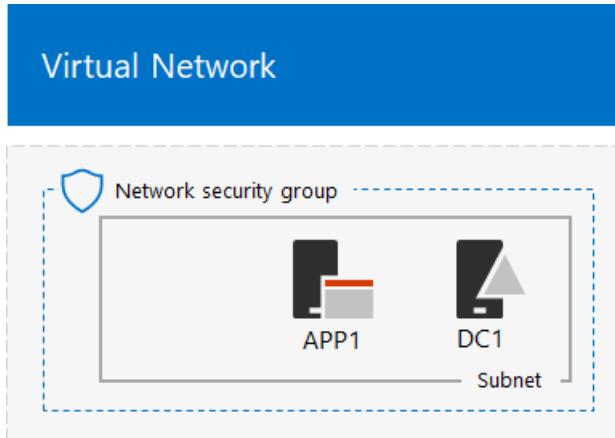
Next, make APP1 a web server with this command at an administrator-level Windows PowerShell command prompt on APP1.

```
Install-WindowsFeature Web-WebServer -IncludeManagementTools
```

Next, create a shared folder and a text file within the folder on APP1 with these PowerShell commands.

```
New-Item -path c:\files -type directory  
Write-Output "This is a shared file." | out-file c:\files\example.txt  
New-SmbShare -name files -path c:\files -changeaccess TESTLAB\User1
```

This is your current configuration.



Step 3: Configure CLIENT1

In this step, you create and configure CLIENT1, which acts as a typical laptop, tablet, or desktop computer on the intranet.

NOTE

The following command set creates CLIENT1 running Windows Server 2016 Datacenter, which can be done for all types of Azure subscriptions. If you have an Visual Studio-based Azure subscription, you can create CLIENT1 running Windows 10 with the [Azure portal](#).

To create an Azure Virtual Machine for CLIENT1, fill in the name of your resource group and run these commands at the command prompt on your local computer.

```
$rgName=<resource group name>  
$locName=(Get-AzureRmResourceGroup -Name $rgName).Location  
$vnet=Get-AzureRMVirtualNetwork -Name TestLab -ResourceGroupName $rgName  
$pip>New-AzureRMPublicIpAddress -Name CLIENT1-PIP -ResourceGroupName $rgName -Location $locName -AllocationMethod Dynamic  
$nic=New-AzureRMNetworkInterface -Name CLIENT1-NIC -ResourceGroupName $rgName -Location $locName -SubnetId $vnet.Subnets[0].Id -PublicIpAddressId $pip.Id  
$vm>New-AzureRMVMConfig -VMName CLIENT1 -VMSize Standard_A1  
$cred=Get-Credential -Message "Type the name and password of the local administrator account for CLIENT1."  
$vm=Set-AzureRMVMOperatingSystem -VM $vm -Windows -ComputerName CLIENT1 -Credential $cred -ProvisionVMAgent -EnableAutoUpdate  
$vm=Set-AzureRMVMSourceImage -VM $vm -PublisherName MicrosoftWindowsServer -Offer WindowsServer -Skus 2016-Datacenter -Version "latest"  
$vm=Add-AzureRMVMNetworkInterface -VM $vm -Id $nic.Id  
$vm=Set-AzureRmVMOSDisk -VM $vm -Name "CLIENT1-OS" -DiskSizeInGB 128 -CreateOption FromImage  
New-AzureRMVM -ResourceGroupName $rgName -Location $locName -VM $vm
```

Next, connect to the CLIENT1 virtual machine using the CLIENT1 local administrator account name and password, and then open an administrator-level Windows PowerShell command prompt.

To check name resolution and network communication between CLIENT1 and DC1, run the **ping**

dc1.testlab.<your public domain name> command at a Windows PowerShell command prompt and verify that there are four replies.

Next, join the CLIENT1 virtual machine to the TESTLAB domain with these commands at the Windows PowerShell prompt.

```
$yourDomain="<your public domain name>"  
Add-Computer -DomainName ("testlab" + $yourDomain)  
Restart-Computer
```

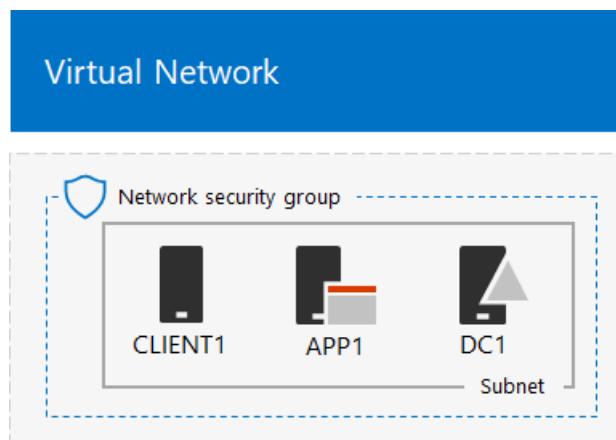
Note that you must supply your TESTLAB\User1 domain account credentials after running the **Add-Computer** command.

After CLIENT1 restarts, connect to it using the TESTLAB\User1 account name and password, and then open an administrator-level Windows PowerShell command prompt.

Next, verify that you can access web and file share resources on APP1 from CLIENT1.

1. In Server Manager, in the tree pane, click **Local Server**.
2. In **Properties for CLIENT1**, click **On** next to **IE Enhanced Security Configuration**.
3. In **Internet Explorer Enhanced Security Configuration**, click **Off** for **Administrators** and **Users**, and then click **OK**.
4. From the Start screen, click **Internet Explorer**, and then click **OK**.
5. In the Address bar, type **http://app1.testab.<your public domain name>/**, and then press ENTER. You should see the default Internet Information Services web page for APP1.
6. From the desktop taskbar, click the File Explorer icon.
7. In the address bar, type **\app1\Files**, and then press ENTER. You should see a folder window with the contents of the Files shared folder.
8. In the **Files** shared folder window, double-click the **Example.txt** file. You should see the contents of the Example.txt file.
9. Close the **example.txt - Notepad** and the **Files** shared folder windows.

This is your current configuration.



Phase 2: Create your Office 365 E5 and EMS E5 subscriptions

In this phase, you create new Office 365 E5 and EMS E5 subscriptions that use a new and common Azure AD tenant, one that is separate from your production subscription. You can do this in two ways:

- Use trial subscriptions of Office 365 E5 and EMS E5.

The Office 365 E5 trial subscription is 30 days, which can be easily extended to 60 days. The EMS E5 trial subscription is 90 days. When the trial subscriptions expire, you must either convert them to paid subscriptions or create new trial subscriptions. Creating new trial subscriptions means you will leave your configuration, which could include complex scenarios, behind.

- Use a separate production subscription of Microsoft 365 Enterprise with a small number of licenses.

This is an additional cost, but ensures that you have a working test environment to try features, configurations, and scenarios that does not expire. You can use the same test environment over the long term for proofs of concept, demonstration to peers and management, and application development and testing. This is the recommended method.

Use trial subscriptions

If you must use trial subscriptions, follow the steps in Phase 2 and Phase 3 of the [Office 365 dev/test environment](#).

Next, you sign up for the EMS E5 trial subscription and add it to the same organization as your Office 365 E5 subscription.

First, add the EMS E5 trial subscription and assign an EMS license to your global administrator account.

1. With a private instance of an Internet browser, sign in to the Office portal with your global administrator account credentials. For help, see [Where to sign in to Office 365](#).
2. Click the **Admin** tile.
3. On the **Office Admin center** tab in your browser, in the left navigation, click **Billing > Purchase services**.
4. On the **Purchase services** page, find the **Enterprise Mobility + Security E5** item. Hover your mouse pointer over it and click **Start free trial**.
5. On the **Confirm your order** page, click **Try now**.
6. On the **Order receipt** page, click **Continue**.
7. On the **Office 365 Admin center** tab in your browser, in the left navigation, click **Users > Active users**.
8. Click your global administrator account, and then click **Edit** for **Product licenses**.
9. On the **Product licenses** pane, turn the product license for **Enterprise Mobility + Security E5** to **On**, click **Save**, and then click **Close** twice.

NOTE

For a permanent test environment, create a new permanent subscription with a small number of licenses.

Next, repeat steps 8 and 9 of the previous procedure for all of your other accounts (User 2, User 3, User 4, and User 5).

Results

Your test environment now has:

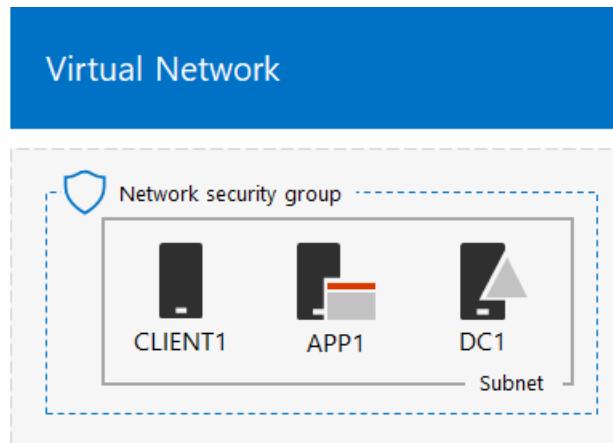
- Office 365 E5 Enterprise and EMS E5 trial subscriptions sharing the same Azure AD tenant with your list of user accounts.
- All your appropriate user accounts (either just the global administrator or all five user accounts) are enabled to use Office 365 E5 and EMS E5.

This is your final configuration.



Office 365

EMS



You are now ready to experiment with additional features of [Microsoft 365 Enterprise](#).

Next steps

Explore these additional sets of Test Lab Guides:

- [Identity](#)
- [Mobile device management](#)
- [Information protection](#)

See also

[Microsoft 365 Enterprise Test Lab Guides](#)

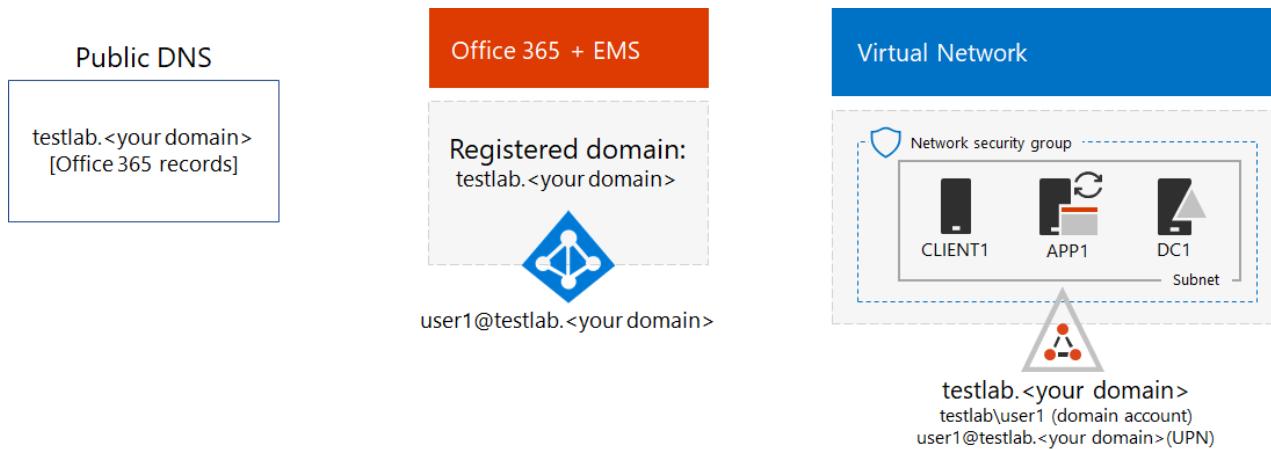
[Deploy Microsoft 365 Enterprise](#)

[Microsoft 365 Enterprise documentation](#)

Password hash synchronization for your Microsoft 365 test environment

2/13/2019 • 4 minutes to read • [Edit Online](#)

Many organizations use Azure AD Connect and password hash synchronization to synchronize the set of accounts in their on-premises Active Directory Domain Services (AD DS) forest to the set of accounts in the Azure AD tenant of their Office 365 and EMS E5 subscriptions. This article describes how you can add password hash synchronization to your Microsoft 365 test environment, resulting in the following configuration:



There are two phases to setting up this test environment:

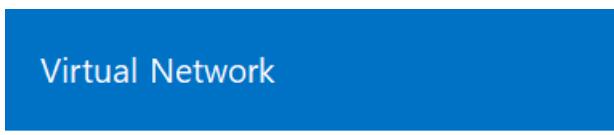
1. Create the Microsoft 365 simulated enterprise test environment.
2. Install and configure Azure AD Connect on APP1.

TIP

Click [here](#) for a visual map to all the articles in the Microsoft 365 Enterprise Test Lab Guide stack.

Phase 1: Create the Microsoft 365 simulated enterprise test environment

Follow the instructions in [simulated enterprise base configuration for Microsoft 365](#). Here is your resulting configuration.



This configuration consists of:

- Office 365 E5 and EMS E5 trial or permanent subscriptions.
- A simplified organization intranet connected to the Internet, consisting of the DC1, APP1, and CLIENT1 virtual machines in an Azure virtual network. DC1 is a domain controller for the testlab.<your public domain name> Windows Server AD domain.

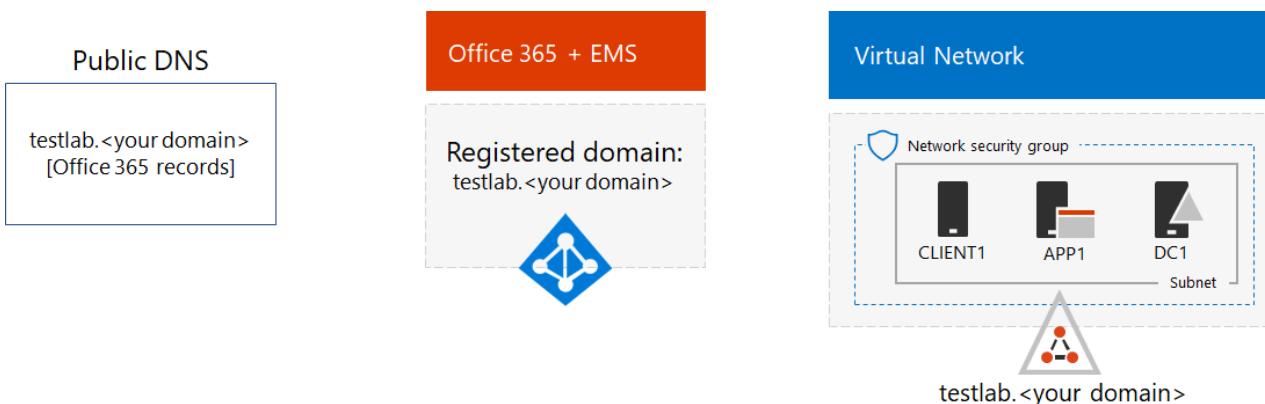
Phase 2: Create and register the testlab domain

In this phase you add a public DNS domain and add it to your subscription.

First, work with your public DNS registration provider to create a new public DNS domain name based on your current domain name and add it to your Office 365 subscription. We recommend using the name **testlab.<your public domain>**. For example, if your public domain name is **contoso.com**, add the public domain name **testlab.contoso.com**.

Next, you add the **testlab.<your public domain>** domain to your Office 365 trial or permanent subscription by going through the domain registration process. This consists of adding additional DNS records to the **testlab.<your public domain>** domain. For more information, see [Add users and domain to Office 365](#).

Here is your resulting configuration.



This configuration consists of:

- Office 365 E5 and EMS E5 trial or permanent subscriptions with the DNS domain testlab.<your public domain name> registered.
- A simplified organization intranet connected to the Internet, consisting of the DC1, APP1, and CLIENT1 virtual machines on a subnet of an Azure virtual network.

Notice how the testlab.<your public domain name> is now:

- Supported by public DNS records.
- Registered in your Office 365 and EMS subscriptions.
- The Windows Server AD domain on your simulated intranet.

Phase 3: Install Azure AD Connect on APP1

In this phase, you install and configure the Azure AD Connect tool on APP1, and then verify that it works.

First, you install and configure Azure AD Connect on APP1.

1. From the [Azure portal](#), sign in with your global administrator account, and then connect to APP1 with the TESTLAB\User1 account.
2. From the desktop of APP1, open an administrator-level Windows PowerShell command prompt, and then run these commands:

```
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Active Setup\Installed Components\{A509B1A7-37EF-4b3f-8CFC-4F3A74704073}" -Name "IsInstalled" -Value 0  
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Active Setup\Installed Components\{A509B1A8-37EF-4b3f-8CFC-4F3A74704073}" -Name "IsInstalled" -Value 0  
Stop-Process -Name Explorer -Force
```

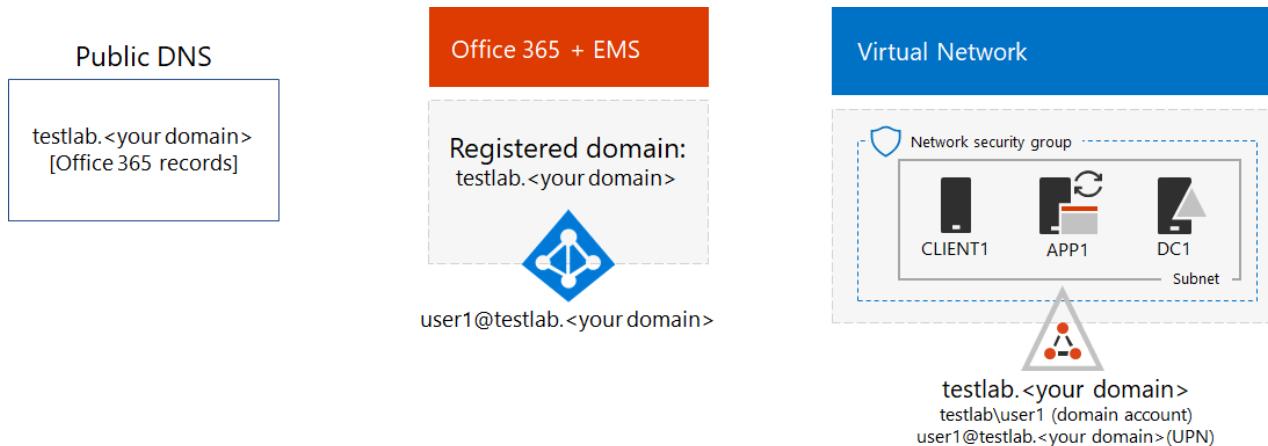
3. From the task bar, click **Internet Explorer** and go to <https://aka.ms/aadconnect>.
 4. On the Microsoft Azure Active Directory Connect page, click **Download**, and then click **Run**.
 5. On the **Welcome to Azure AD Connect** page, click **I agree**, and then click **Continue**.
 6. On the **Express Settings** page, click **Use express settings**.
 7. On the **Connect to Azure AD** page, type your Office 365 global administrator account name in **Username**, type its password in **Password**, and then click **Next**.
 8. On the **Connect to AD DS** page, type **TESTLAB\User1** in **Username**, type its password in **Password**, and then click **Next**.
 9. On the **Ready to configure** page, click **Install**.
 10. On the **Configuration complete** page, click **Exit**.
 11. In Internet Explorer, go to the Office portal (<https://office.com>).
 12. From the main portal page, click **Admin**.
 13. In the left navigation, click **Users > Active users**.
- Note the account named **User1**. This account is from the TESTLAB Windows Server AD domain and is proof that directory synchronization has worked.
14. Click the **User1** account. For product licenses, click **Edit**.
 15. In **Product licenses**, select your scountry, and then click the **Off** control for **Office 365 Enterprise E5** (switching it to **On**). Do the same for the **Enterprise Mobility + Security E5** license.
 16. Click **Save** at the bottom of the page, and then click **Close**.

Next, you test the ability to sign in to your Office 365 subscription with the **user1@testlab.<your domain name>** user name of the User1 account.

1. From APP1, sign out of Office 365, and then sign in again, this time specifying a different account.
2. When prompted for a user name and password, specify **user1@testlab.<your domain name>** and the User1 password. You should successfully sign in as User1.

Notice that although User1 has domain administrator permissions for the TESTLAB Windows Server AD domain, it is not an Office 365 global administrator. Therefore, you will not see the **Admin** icon as an option.

Here is your resulting configuration.



This configuration consists of:

- Office 365 E5 and EMS E5 trial or permanent subscriptions with the DNS domain TESTLAB.<your domain name> registered.
- A simplified organization intranet connected to the Internet, consisting of the DC1, APP1, and CLIENT1 virtual machines on a subnet of an Azure virtual network. Azure AD Connect runs on APP1 to synchronize the TESTLAB Windows Server AD domain to the Azure AD tenant of your Office 365 and EMS E5 subscriptions periodically.
- The User1 account in the TESTLAB Windows Server AD domain has been synchronized with the Azure AD tenant.

Next step

Explore additional [identity](#) features and capabilities in your test environment.

See also

[Microsoft 365 Enterprise Test Lab Guides](#)

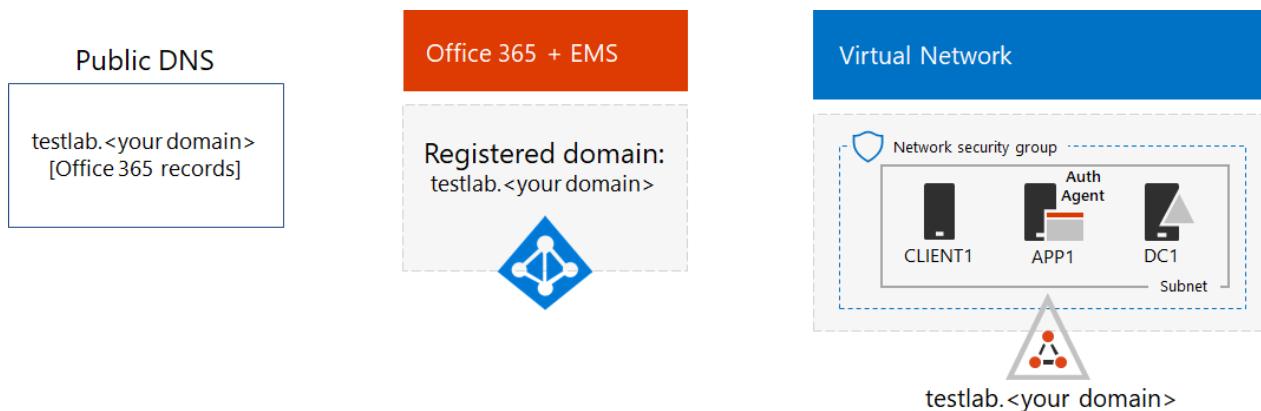
[Deploy Microsoft 365 Enterprise](#)

[Microsoft 365 Enterprise documentation](#)

Pass-through authentication for your Microsoft 365 test environment

2/26/2019 • 2 minutes to read • [Edit Online](#)

Organizations that want to directly use their on-premises Active Directory Domain Services (AD DS) infrastructure for authentication to Microsoft cloud-based services and applications can use pass-through authentication. This article describes how you can configure your Microsoft 365 test environment for pass-through authentication, resulting in the following configuration:



There are two phases to setting up this test environment:

1. Create the Microsoft 365 simulated enterprise test environment with password hash synchronization.
2. Configure Azure AD Connect on APP1 for pass-through authentication.

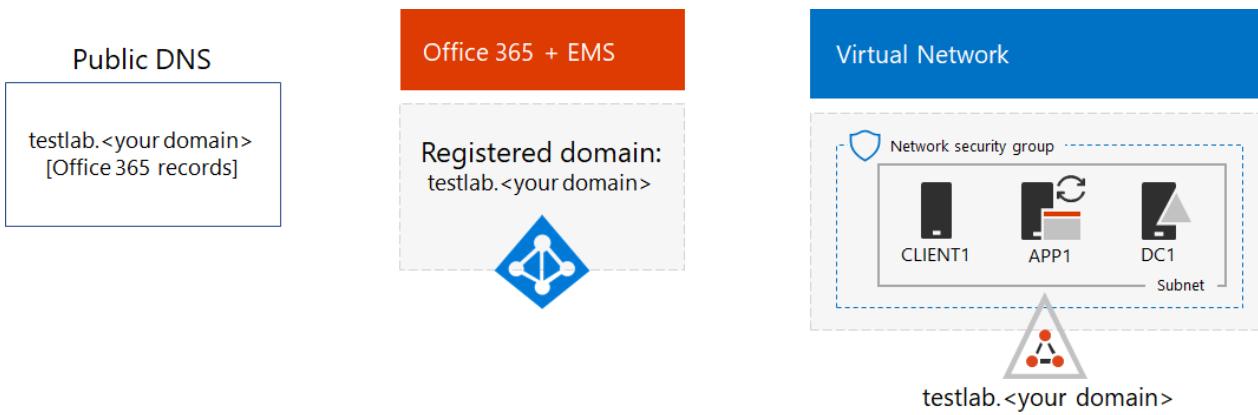


TIP

Click [here](#) for a visual map to all the articles in the Microsoft 365 Enterprise Test Lab Guide stack.

Phase 1: Configure password hash synchronization for your Microsoft 365 test environment

Follow the instructions in [password hash synchronization for Microsoft 365](#). Here is your resulting configuration.



This configuration consists of:

- Office 365 E5 and EMS E5 trial or permanent subscriptions.
- A simplified organization intranet connected to the Internet, consisting of the DC1, APP1, and CLIENT1 virtual machines on a subnet of an Azure virtual network. Azure AD Connect runs on APP1 to synchronize the TESTLAB Windows Server AD domain to the Azure AD tenant of your Office 365 and EMS E5 subscriptions periodically.

Phase 2: Configure Azure AD Connect on APP1 for pass-through authentication

In this phase, you configure Azure AD Connect on APP1 to use pass-through authentication, and then verify that it works.

Configure Azure AD Connect on APP1

1. From the [Azure portal](#), sign in with your global administrator account, and then connect to APP1 with the TESTLAB\User1 account.
2. From the desktop of APP1, run Azure AD Connect.
3. On the **Welcome page**, click **Configure**.
4. On the Additional tasks page, click **Change user sign-in**, and then click **Next**.
5. On the **Connect to Azure AD** page, type your global administrator account credentials, and then click **Next**.
6. On the **User sign-in** page, click **Pass-through authentication**, and then click **Next**.
7. On the **Ready to configure** page, click **Configure**.
8. On the **Configuration complete** page, click **Exit**.
9. From the Azure portal, in the left pane, click **Azure Active Directory > Azure AD Connect**. Verify that the **Pass-through authentication** feature appears as **Enabled**.
10. Click **Pass-through authentication**. The **Pass-through authentication** pane lists the servers where your Authentication Agents are installed. You should see APP1 in the list. Close the **Pass-through authentication** pane.

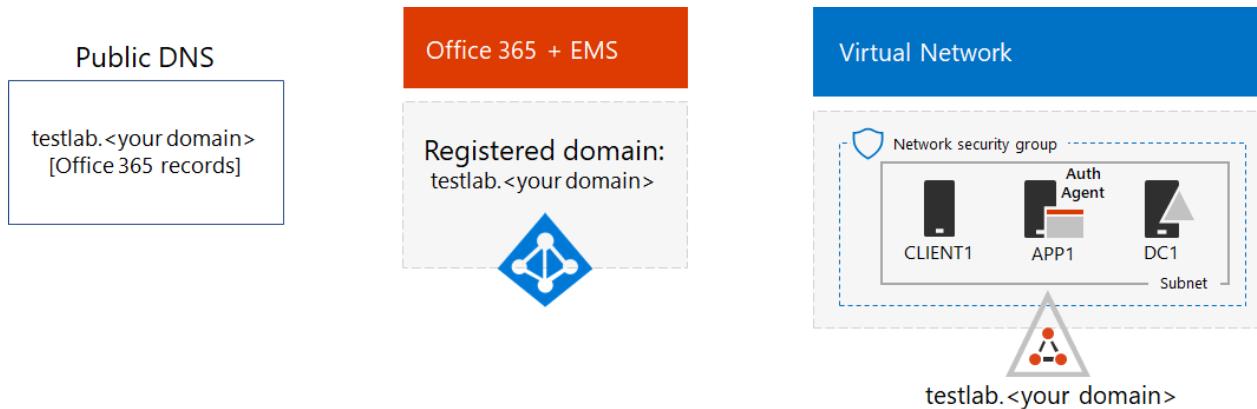
Next, test the ability to sign in to your Office 365 subscription with the **user1@testlab.<your public domain>** user name of the User1 account.

1. From APP1, sign out of Office 365, and then sign in again, this time specifying a different account.
2. When prompted for a user name and password, specify **user1@testlab.<your public domain>** and the

User1 password. You should successfully sign in as User1.

Notice that although User1 has domain administrator permissions for the TESTLAB Windows Server AD domain, it is not an Office 365 global administrator. Therefore, you will not see the **Admin** icon as an option.

Here is your resulting configuration:



This configuration consists of:

- Office 365 E5 and EMS E5 trial or permanent subscriptions with the DNS domain `testlab.<your domain name>` registered.
- A simplified organization intranet connected to the Internet, consisting of the DC1, APP1, and CLIENT1 virtual machines on a subnet of an Azure virtual network. An Authentication Agent runs on APP1 to handle pass-through authentication requests from the Azure AD tenant of your Office 365 and EMS E5 subscriptions.

Next step

Explore additional [identity](#) features and capabilities in your test environment.

See also

[Microsoft 365 Enterprise Test Lab Guides](#)

[Deploy Microsoft 365 Enterprise](#)

[Microsoft 365 Enterprise documentation](#)

Azure AD Seamless Single Sign-on for your Microsoft 365 test environment

2/26/2019 • 3 minutes to read • [Edit Online](#)

Azure AD Seamless Single Sign-On (SSO) automatically signs in users when they are on their PCs or devices that are connected to their organization network. Azure AD Seamless SSO provides users with easy access to cloud-based applications without needing any additional on-premises components.

This article describes how you can configure your Microsoft 365 test environment for Azure AD Seamless SSO.

There are two phases to setting this up:

1. Create the Microsoft 365 simulated enterprise test environment with password hash synchronization.
2. Configure Azure AD Connect on APP1 for Azure AD Seamless SSO.

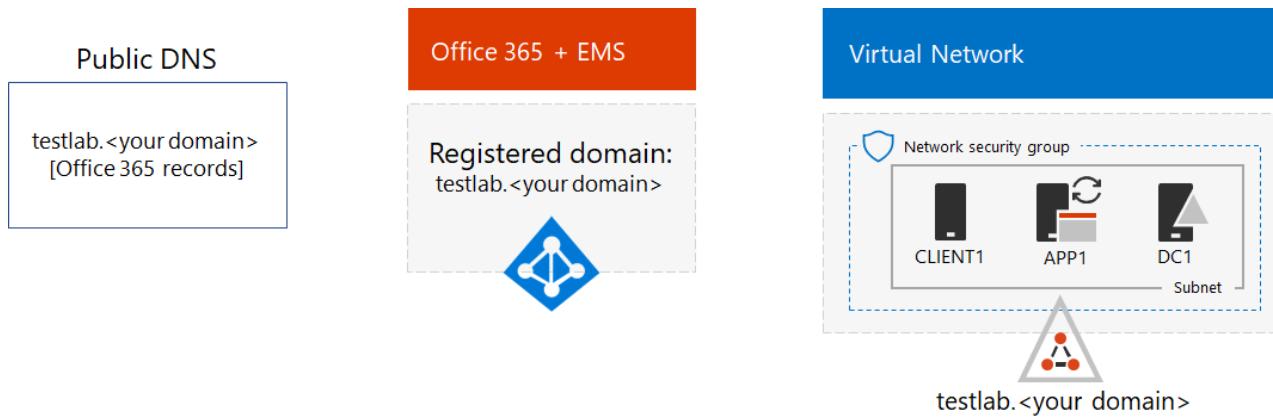


TIP

Click [here](#) for a visual map to all the articles in the Microsoft 365 Enterprise Test Lab Guide stack.

Phase 1: Configure password hash synchronization for your Microsoft 365 test environment

Follow the instructions in [password hash synchronization for Microsoft 365](#). Here is your resulting configuration.



This configuration consists of:

- Office 365 E5 and EMS E5 trial or permanent subscriptions.
- A simplified organization intranet connected to the Internet, consisting of the DC1, APP1, and CLIENT1 virtual machines on a subnet of an Azure virtual network.
- Azure AD Connect runs on APP1 to synchronize the TESTLAB Windows Server AD domain to the Azure AD tenant of your Office 365 and EMS E5 subscriptions periodically.

Phase 2: Configure Azure AD Connect on APP1 for Azure AD Seamless SSO

In this phase, you configure Azure AD Connect on APP1 for Azure AD Seamless SSO, and then verify that it works.

Configure Azure AD Connect on APP1

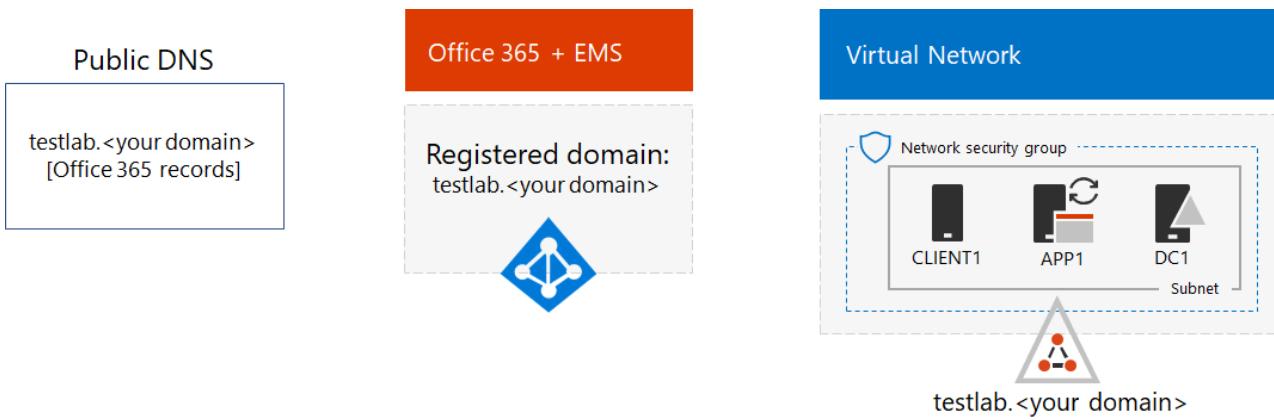
1. From the [Azure portal](#), sign in with your global administrator account, and then connect to APP1 with the TESTLAB\User1 account.
2. From the desktop of APP1, run Azure AD Connect.
3. On the **Welcome page**, click **Configure**.
4. On the **Additional tasks** page, click **Change user sign-in**, and then click **Next**.
5. On the **Connect to Azure AD** page, type your global administrator account credentials, and then click **Next**.
6. On the **User sign-in** page, select **Enable single sign-on**, and then click **Next**.
7. On the **Enable single sign-on** page, click **Enter credentials**.
8. In the **Windows Security** dialog box, type **user1** and the password of the user1 account, and then click **OK**. Click **Next**.
9. On the **Ready to Configure** page, click **Configure**.
10. On the **Configuration complete** page, click **Exit**.
11. From the Azure portal, in the left pane, click **Azure Active Directory > Azure AD Connect**. Verify that the **Seamless single sign-on** feature appears as **Enabled**.

Next, test the ability to sign in to your Office 365 subscription with the **user1@testlab.<your public domain>** user name of the User1 account.

1. From Internet Explorer on APP1, click the settings icon, and then click **Internet Options**.
2. In **Internet Options**, click the **Security** tab.
3. Click **Local intranet**, and then click **Sites**.
4. In **Local intranet**, click **Advanced**.
5. In **Add this website to the zone**, type <https://autologon.microsoftazuread-sso.com>, click **Add > Close > OK > OK**.
6. Sign out of Office 365, and then sign in again, this time specifying a different account.
7. When prompted to sign in, specify **user1@testlab.<your public domain>** name, and then click **Next**. You should successfully sign in as User1 without being prompted for a password. This proves that Azure AD Seamless SSO is working.

Notice that although User1 has domain administrator permissions for the TESTLAB Windows Server AD domain, it is not a global administrator for Azure AD and Office 365. Therefore, you will not see the **Admin** icon as an option.

Here is your resulting configuration:



This configuration consists of:

- Office 365 E5 and EMS E5 trial or permanent subscriptions with the DNS domain `testlab.<your domain name>` registered.
- A simplified organization intranet connected to the Internet, consisting of the `DC1`, `APP1`, and `CLIENT1` virtual machines on a subnet of an Azure virtual network.
- Azure AD Connect runs on `APP1` to synchronize the list of accounts and groups from the Azure AD tenant of your Office 365 and EMS E5 subscriptions to the TESTLAB Windows Server AD domain.
- Azure AD Seamless SSO is enabled so that computers on the simulated intranet can sign in to Microsoft 365 cloud resources without specifying a user account password.

See the [Simplify user sign-in](#) step in the Identity phase for information and links to configure Azure AD Seamless SSO in production.

Next step

Explore additional [identity](#) features and capabilities in your test environment.

See also

[Microsoft 365 Enterprise Test Lab Guides](#)

[Deploy Microsoft 365 Enterprise](#)

[Microsoft 365 Enterprise documentation](#)

Multi-factor authentication for your Microsoft 365 Enterprise test environment

2/26/2019 • 3 minutes to read • [Edit Online](#)

For an additional level of security for signing in to Office 365 or any service or application that uses the Azure AD tenant for your organization, you can enable Azure multi-factor authentication, which requires more than just a username and password to verify an account. With multi-factor authentication, users are required to acknowledge a phone call, type a verification code sent in a text message, or specify an app password on their smart phones after correctly entering their passwords. They can sign in only after this second authentication factor has been satisfied.

This article describes how to enable and test text message-based authentication for a specific account.

There are two phases to setting up multi-factor authentication for an account in your Microsoft 365 Enterprise test environment:

1. Create the Microsoft 365 Enterprise test environment.
2. Enable and test multi-factor authentication for the User 2 account.



TIP

Click [here](#) for a visual map to all the articles in the Microsoft 365 Enterprise Test Lab Guide stack.

Phase 1: Build out your Microsoft 365 Enterprise test environment

If you just want to test multi-factor authentication in a lightweight way with the minimum requirements, follow the instructions in [Lightweight base configuration](#).

If you want to test multi-factor authentication in a simulated enterprise, follow the instructions in [Pass-through authentication](#).

NOTE

Testing multi-factor authentication does not require the simulated enterprise test environment, which includes a simulated intranet connected to the Internet and directory synchronization for a Windows Server AD forest. It is provided here as an option so that you can test multi-factor authentication and experiment with it in an environment that represents a typical organization.

Phase 2: Enable and test multi-factor authentication for the User 2 account

Enable multi-factor authentication for the User 2 account with these steps:

1. Open a separate, private instance of your browser, go to the Office portal (<https://office.com>), and then sign

in with your global administrator account.

2. From the main portal page, click **Admin**.
3. In the left navigation, click **Users > Active users**.
4. In the Active users pane, click **More > Multi-factor authentication setup**.
5. In the list, select the **User 2** account.
6. In the **User 2** section, under **Quick steps**, click **Enable**.
7. In the **About enabling multi-factor auth** dialog box, click **Enable multi-factor auth**.
8. In the **Updates successful** dialog box, click **Close**.
9. On the **Microsoft Office Home** tab, click the user account icon in the upper right, and then click **Sign out**.
10. Close your browser instance.

Complete the configuration for the User 2 account to use a text message for validation and test it with these steps:

1. Open a new, private instance of your browser.
2. Go to the Office portal (<https://office.com>) and sign in with the User 2 account (user2@<organization name>.onmicrosoft.com) and password.
3. After signing in, you are prompted to set up the account for more information. Click **Next**.
4. On the **Additional security verification** page:
 - Select your country or region.
 - Type phone number of the smart phone that will receive text messages.
 - In **Method**, click **Send me a code by text message**.
5. Click **Next**.
6. Enter the verification code from the text message received on your smart phone, and then click **Verify**.
7. On the **Step 3: Keep your existing applications** page, record the displayed app password for the User 2 account in a secure location, and then click **Done**.
8. If this is the first time you signed in with the User 2 account, you are prompted to change the password. Type the original password and a new password twice, and then click **Update password and sign in**. Record the new password in a secure location.

You should see the Office portal for User 2 on the **Microsoft Office Home** tab of your browser.

See the [Set up multi-factor authentication](#) step in the Identity phase for information and links to deploy multi-factor authentication in production.

Next step

Explore additional [identity](#) features and capabilities in your test environment.

See also

[Phase 2: Identity](#)

[Microsoft 365 Enterprise Test Lab Guides](#)

[Microsoft 365 Enterprise deployment](#)

[Microsoft 365 Enterprise documentation](#)

Protect global administrator accounts in your Microsoft 365 Enterprise test environment

2/26/2019 • 4 minutes to read • [Edit Online](#)

You can prevent digital attacks on your organization by ensuring that your administrator accounts are as secure as possible. This article describes how to use Office 365 Cloud App Security and Azure AD conditional access policies to protect global administrator accounts.

There are two phases to protecting global administrator accounts in your Microsoft 365 Enterprise test environment:

1. Create the Microsoft 365 Enterprise test environment.
2. Protect your dedicated global administrator account.



TIP

Click [here](#) for a visual map to all the articles in the Microsoft 365 Enterprise Test Lab Guide stack.

Phase 1: Build out your Microsoft 365 Enterprise test environment

If you just want to test global administrator account protection in a lightweight way with the minimum requirements, follow the instructions in [Lightweight base configuration](#).

If you want to test global administrator account protection in a simulated enterprise, follow the instructions in [Pass-through authentication](#).

NOTE

Testing global administrator account protection does not require the simulated enterprise test environment, which includes a simulated intranet connected to the Internet and directory synchronization for a Windows Server AD forest. It is provided here as an option so that you can test global administrator account protection and experiment with it in an environment that represents a typical organization.

Phase 2: Configure Cloud App Security and conditional access policies

First, create an Office 365 Cloud App Security policy to monitor global administrator account activity and send alerts to the email address of your global administrator account.

1. Sign in to the Office portal at <http://portal.office.com> using your global administrator account.
2. Click the **Admin** tile. On the **Office Admin center** tab, click **Admin centers > Security & Compliance**.
3. In the left navigation pane, click **Alerts > Manage advanced alerts**.
4. On the **Manage advanced alerts** page, click **Turn on Office 365 Cloud App Security**, and then click **Go to Office 365 Cloud App Security**.
5. On the new **Dashboard** tab, click **Control > Policies**.

6. On the **Policy** page, click **Create policy**, and then click **Activity policy**.
7. In **Policy name**, type **Administrative activity**.
8. In **Policy severity**, click **High**.
9. In **Category**, click **Privileged accounts**.
10. In **Create filters for the policy**, in **Activities matching all of the following**, click **Administrative activity**.
11. In **Alerts**, click **Send alert as email**. In **To**, type the email address of your global administrator account.
12. At the bottom of the page, click **Create**.
13. Close the **Dashboard** tab.

Next, create a new user account as a dedicated global administrator.

1. On the **Office Admin center** tab, under **Active users**, click **Add a user**.
2. On the **New user** page, type **DedicatedAdmin** in **First name**, **Display name**, and **Username**.
3. Click **Password**, click **Let me create the password**, and then type a strong password. Record the password for this new account in a secure location.
4. Clear **Make this user change their password when they first sign in**.
5. Click **Roles**, and then click **Global administrator**.
6. Click **Product licenses**, and then turn the **Enterprise Mobility + Security E5** and **Office 365 Enterprise E5 licenses** on.
7. Click **Add**.
8. On the **User was added page**, clear **Send password in email**, and then click **Close**.

Next, create a new group named GlobalAdmins and add the DedicatedAdmin account to it.

1. On the **Office Admin center** tab, click the groups icon in the left navigation, and then click **Groups**.
2. Click **Add a group**.
3. On the **New Group** page, type **GlobalAdmins**.
4. Click **Select owner** click your global administrator account, and then click **Add > Close**.
5. In the list of groups, click the **GlobalAdmins** group.
6. On the **GlobalAdmins** page, click **Edit for Member**, and then click **Add members**.
7. In the list, click the **DedicatedAdmin** account, and then click **Save > Close > Close > Admin center**.

Next, create conditional access policies to require multifactor authentication for global administrator accounts and to deny authentication if the sign-in risk is medium or high.

This first policy requires that all global administrator accounts use MFA.

1. In a new tab of your browser, go to <https://portal.azure.com>.
2. Click **Azure Active Directory > Conditional access**.
3. On the **Conditional access – Policies** blade, click **Baseline policy: Require MFA for admins (preview)**.
4. On the **Baseline policies...** blade, click **Use policy immediately > Save**.

This second policy blocks access to global administrator account authentication when the sign-in risk is medium or high.

1. On the **Conditional access – Policies** blade, click **New policy**.
2. On the **New** blade, type **Global administrators** in **Name**.
3. In the **Assignments** section, click **Users and groups**.
4. On the **Include** tab of the **Users and groups** blade, click **Select users and groups > Users and groups > Select**.
5. On the **Select** blade, click the **GlobalAdmins > Select > Done**.
6. In the **Assignments** section, click **Conditions**.

7. On the **Conditions** blade, click **Sign-in risk**, click **Yes** for **Configure**, click **High** and **Medium**, and then click **Select** and **Done**.
8. In the **Access controls** section of the **New** blade, click **Grant**.
9. On the **Grant** blade, click **Block access**, and then click **Select**.
10. On the **New** blade, click **On** for **Enable policy**, and then click **Create**.
11. Close the **Azure portal** and **Office Admin center** tabs.

To test the first policy, sign out and sign in with the DedicatedAdmin account. You should be prompted to configure MFA on the user account. This demonstrates that the first policy is being applied.

See the [Protect global administrator accounts](#) step in the Identity phase for information and links to protect your global administrator accounts in production.

Next step

Explore additional [identity](#) features and capabilities in your test environment.

See also

[Phase 2: Identity](#)

[Microsoft 365 Enterprise Test Lab Guides](#)

[Microsoft 365 Enterprise deployment](#)

[Microsoft 365 Enterprise documentation](#)

Password reset for your Microsoft 365 test environment

2/26/2019 • 2 minutes to read • [Edit Online](#)

Azure AD self-service password reset (SSPR) allows users to reset or unlock their passwords or accounts.

This article describes how you can configure and test password resets in your Microsoft 365 test environment in two phases:

1. Create the Microsoft 365 Enterprise test environment.
2. Configure and test password reset for the User 2 account.



TIP

Click [here](#) for a visual map to all the articles in the Microsoft 365 Enterprise Test Lab Guide stack.

Phase 1: Build out your Microsoft 365 Enterprise test environment

If you just want to test password resets in a lightweight way with the minimum requirements, follow the instructions in [Lightweight base configuration](#).

If you want to test password resets in a simulated enterprise, follow the instructions in [Pass-through authentication](#).

NOTE

Testing password resets does not require the simulated enterprise test environment, which includes a simulated intranet connected to the Internet and directory synchronization for a Windows Server AD forest. It is provided here as an option so that you can test password resets and experiment with it in an environment that represents a typical organization.

Phase 2: Configure and test password reset

In this phase, you configure password reset in the Azure AD tenant through group membership, and then verify that it works.

First, enable password reset for the accounts in a specific Azure AD group.

1. From a private instance of your browser, open <https://portal.azure.com>, and then sign in with the credentials of your global administrator account.
2. In the Azure portal, click **Azure Active Directory > Groups > New group**.
3. Set the **Group type** to **Security**, **Group name** to **PWReset**, and the **Membership type** to **Assigned**. Click **Create**.
4. Click the **PWReset** group in the list, and then click **Members**.
5. Click **Add members**, click **User 2**, and then click **Select**. Close the **PWReset** and **Group** pages.

6. On the Azure Active Directory page, click **Password reset**.
7. From the **Properties** page, under the option **Self Service Password Reset Enabled**, choose **Selected**.
8. From **Select group**, select **PWReset**, and then click **Save**.
9. Close the private browser instance.

Next, you test password reset for the User 2 account.

1. Open a new private browser instance and browse to <https://aka.ms/ssprsetup>.
2. Sign in with the User 2 account credentials.
3. In **Don't lose access to your account**, set the authentication phone to your mobile phone number and the authentication email to your work or personal email account.
4. After both are verified, click **Looks good** and close the private instance of the browser.
5. Open a new private browser instance and go to <https://aka.ms/sspr>.
6. Sign in with the User 2 account credentials, type the characters from the CAPTCHA, and then click **Next**.
7. For **verification step 1**, click **Email my alternate email**, and then click **Email**. When you receive the email, type the verification code, and then click **Next**.
8. In **Get back into your account**, type a new password for the User 2 account, and then click **Finish**. Note the changed password of the User 2 account and store it in a safe location.
9. In a separate tab of the same browser, go to <https://office.com>, and then sign in with the User 2 account name and its new password. You should see the **Office Home** page.

See the [Simplify password resets](#) step in the Identity phase for information and links to configure password resets in production.

Next step

Explore additional [identity](#) features and capabilities in your test environment.

See also

[Microsoft 365 Enterprise Test Lab Guides](#)

[Deploy Microsoft 365 Enterprise](#)

[Microsoft 365 Enterprise documentation](#)

Password writeback for your Microsoft 365 test environment

2/26/2019 • 3 minutes to read • [Edit Online](#)

Password writeback allows users to update their passwords through Azure Active Directory (Azure AD), which is then replicated to your local Active Directory Domain Services (AD DS). With password writeback, users don't need to update their passwords through the on-premises Windows Server AD where their original user accounts are stored. This helps roaming or remote users who do not have a remote access connection to their on-premises network.

This article describes how you can configure your Microsoft 365 test environment for password writeback.

There are two phases to setting this up:

1. Create the Microsoft 365 simulated enterprise test environment with password hash synchronization.
2. Enable password writeback for the TESTLAB Windows Server AD domain.

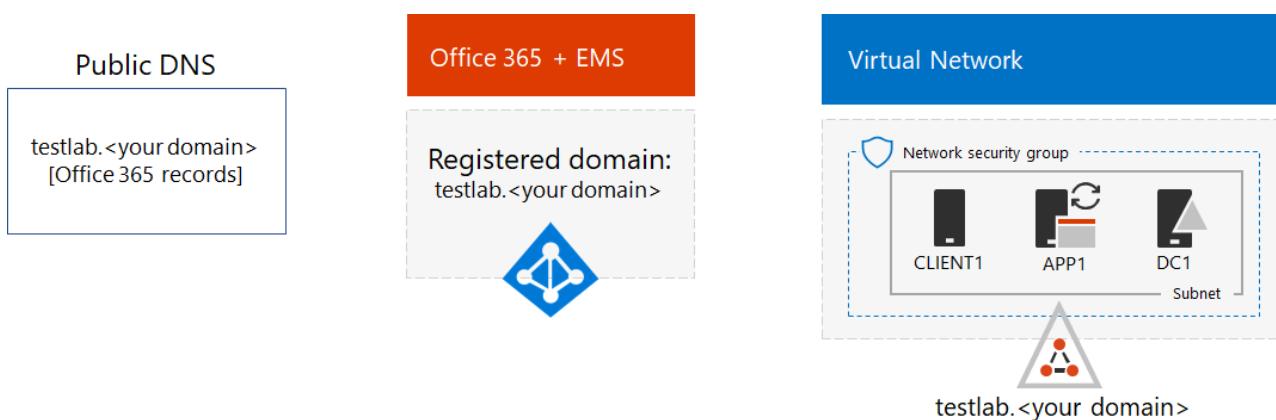


TIP

Click [here](#) for a visual map to all the articles in the Microsoft 365 Enterprise Test Lab Guide stack.

Phase 1: Configure password hash synchronization for your Microsoft 365 test environment

Follow the instructions in [password hash synchronization for Microsoft 365](#). Here is your resulting configuration.



This configuration consists of:

- Office 365 E5 and EMS E5 trial or permanent subscriptions.
- A simplified organization intranet connected to the Internet, consisting of the DC1, APP1, and CLIENT1 virtual machines on a subnet of an Azure virtual network.
- Azure AD Connect runs on APP1 to synchronize the TESTLAB Windows Server AD domain to the Azure AD tenant of your Office 365 and EMS E5 subscriptions.

Phase 2: Enable password writeback for the TESTLAB Windows Server AD domain

First, configure the User 1 account with the global administrator role.

1. From the [Office portal](#), sign in with your global administrator account.
2. Click the **Admin** tile. From the new **Microsoft 365 admin center** tab of your browser, click **Active users**.
3. On the **Active users** page, click the **user1** account,
4. On the **user1** pane, click **Edit** next to **Roles**.
5. On the **Edit user roles** pane for user1, click **Global administrator**. Click **Save**, and then click **Close**.

Next, configure the User 1 account with the security settings that allow it to change passwords on behalf of other users in the TESTLAB Windows Server AD domain.

1. From the [Azure portal](#), sign in with your global administrator account, and then connect to APP1 with the TESTLAB\User1 account.
2. From the desktop of APP1, click **Start**, type **active**, and then click **Active Directory Users and Computers**.
3. Click **View** in the menu bar. If **Advanced features** is not enabled, click it to enable it.
4. In the tree pane, right-click your domain, click **Properties**, and then click the **Security** tab.
5. Click **Advanced**.
6. On the **Permissions** tab, click **Add**.
7. Click **Select a principal**, type **User1**, and then click **OK**.
8. In **Applies to**, select **Descendant User objects**.
9. Under **Permissions**, select the following:
 - Change password
 - Reset password
10. Under **Properties**, select the following:
 - Write lockoutTime
 - Write pwdLastSet
11. Click **OK** three times to save the changes.
12. Close **Active Directory Users and Computers**.

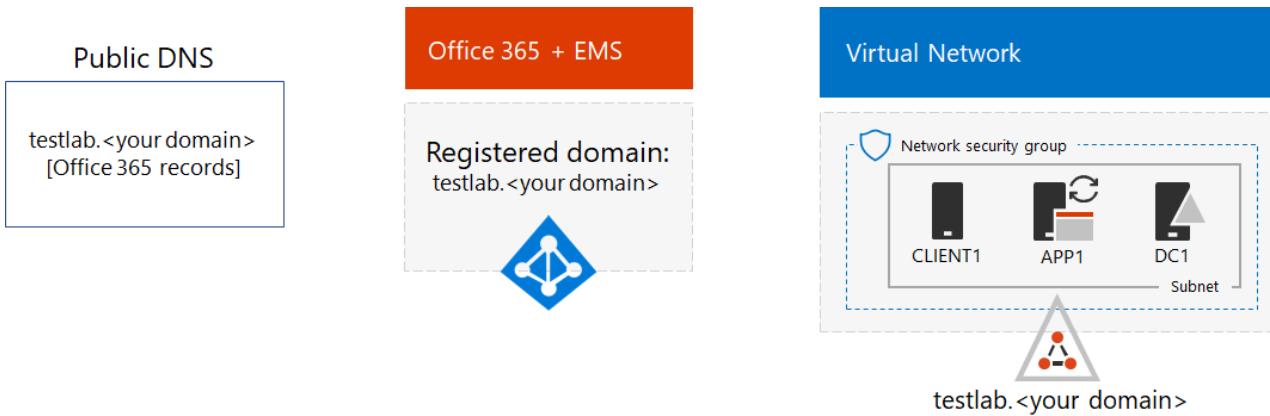
Next, configure Azure AD Connect on APP1 for password writeback.

1. If needed, connect to APP1 with the TESTLAB\User1 account.
2. From the desktop of APP1, double-click **Azure AD Connect**.
3. On the **Welcome page**, click **Configure**.
4. On the **Additional tasks** page, click **Customize synchronization options**, and then click **Next**.
5. On the **Connect to Azure AD** page, type the User 1 account credentials, and then click **Next**.
6. On the **Connect directories** and **Domain/OU filtering** pages, click **Next**.

7. On the **Optional features** page, select **Password writeback** and click **Next**.
8. On the **Ready to configure** page, click **Configure** and wait for the process to finish.
9. When you see the configuration finish, click **Exit**.

You are now ready to test password writeback for users on computers that are not connected to the virtual network of your simulated intranet.

Here is your resulting configuration:



This configuration consists of:

- Office 365 E5 and EMS E5 trial or permanent subscriptions with the DNS domain TESTLAB.<your domain name> registered.
- A simplified organization intranet connected to the Internet, consisting of the DC1, APP1, and CLIENT1 virtual machines on a subnet of an Azure virtual network.
- Azure AD Connect runs on APP1 to synchronize the list of accounts and groups from the Azure AD tenant of your Office 365 and EMS E5 subscriptions to the TESTLAB Windows Server AD domain.
- Password writeback is enabled so that users can change their passwords through Azure AD without having to be connected to the simplified intranet.

See the [Simplify password updates](#) step in the Identity phase for information and links to configure password writeback in production.

Next step

Explore additional [identity](#) features and capabilities in your test environment.

See also

[Microsoft 365 Enterprise Test Lab Guides](#)

[Deploy Microsoft 365 Enterprise](#)

[Microsoft 365 Enterprise documentation](#)

Automate licensing and group membership for your Microsoft 365 Enterprise test environment

2/26/2019 • 3 minutes to read • [Edit Online](#)

Group-based licensing automatically assigns or removes licenses for a user account based on group membership. Dynamic group membership adds or removes members to a group based on user account properties, such as Department or Country. This article steps you through a demonstration of both in your Microsoft 365 Enterprise test environment.

There are two phases to setting up auto-licensing and dynamic group membership in your Microsoft 365 Enterprise test environment:

1. Create the Microsoft 365 Enterprise test environment.
2. Configure and test dynamic group membership and automatic licensing.



TIP

Click [here](#) for a visual map to all the articles in the Microsoft 365 Enterprise Test Lab Guide stack.

Phase 1: Build out your Microsoft 365 Enterprise test environment

If you just want to test automated licensing and group membership in a lightweight way with the minimum requirements, follow the instructions in [Lightweight base configuration](#).

If you want to test automated licensing and group membership in a simulated enterprise, follow the instructions in [Pass-through authentication](#).

NOTE

Testing automated licensing and group membership does not require the simulated enterprise test environment, which includes a simulated intranet connected to the Internet and directory synchronization for a Windows Server AD forest. It is provided here as an option so that you can test automated licensing and group membership and experiment with it in an environment that represents a typical organization.

Phase 2: Configure and test dynamic group membership and automatic licensing

First, you create a new Sales group and add a dynamic group membership rule so that user accounts with the Department set to Sales are automatically added to the Sales group.

1. Using a private instance of your Internet browser, sign in to the Office portal at <https://office.com> with the global administrator account of your Office 365 E5 trial subscription.
2. On a separate tab of your browser, go to the Azure portal at <https://portal.azure.com>.
3. In the Azure portal, click **Azure Active Directory > Users and groups > All groups**.

4. On the **All groups** blade, click **New group**.
5. In **Group type**, select **Office 365**.
6. In **Group name**, type **Sales**.
7. In **Membership type**, select **Dynamic user**.
8. Click **Add dynamic query**.
9. In **Add users where**, select **department**.
10. In the next field, select **Equals**.
11. In the next field, type **Sales**.
12. Click **Add query**, and then click **Create**.
13. Close the **Group** and **Groups-All groups** blades.

Next, you configure the Sales group so that members are automatically assigned Office 365 E5 and Enterprise Mobility + Security E5 licenses.

1. On the **Overview** blade for Azure Active Directory, click **Licenses > All products**.
2. In the list, select **Enterprise Mobility + Security E5** and **Office 365 Enterprise E5**, and then click **Assign**.
3. On the **Assign license** blade, click **Users and groups**.
4. In the list of groups, select the **Sales** group.
5. Click **Select**, and then click **Assign**.
6. Close the Azure portal tab in your browser.

Next, you test dynamic group membership and automatic licensing on the User 4 account.

1. From the **Microsoft Office Home** tab in your browser, click **Admin**.
2. From the **Office Admin center** tab, click **Active users**.
3. On the **Active users** page, click the **User 4** account.
4. On the **User 4** pane, click **Edit for Product licenses**.
5. On the **Product licenses** pane, turn the **Enterprise Mobility + Security E5** and **Office 365 Enterprise E5** licenses off, and then click **Save > Close**.
6. In the properties of the User 4 account, verify that no product licenses have been assigned and there are no group memberships.
7. Click **Edit for Contact information**.
8. In the **Edit Contact information** pane, click **Contact information**.
9. In the **Department** field, type **Sales**, and then click **Save > Close**.
10. Wait a few minutes, and then periodically click the refresh icon in the upper-right of the User 4 account pane.

In time you should see the:

- **Group memberships** property updated with the **Sales** group.
- **Product licenses** property updated with the **Enterprise Mobility + Security E5** and **Office 365 Enterprise E5** licenses.

See these steps in the Identity phase for information and links to deploy dynamic group membership and automatic licensing in production:

- [Set up automatic licensing](#)
- [Set up dynamic group membership](#)

Next step

Explore additional [identity](#) features and capabilities in your test environment.

See also

[Phase 2: Identity](#)

[Microsoft 365 Enterprise Test Lab Guides](#)

[Microsoft 365 Enterprise deployment](#)

[Microsoft 365 Enterprise documentation](#)

Azure AD Identity Protection for your Microsoft 365 Enterprise test environment

2/26/2019 • 2 minutes to read • [Edit Online](#)

Azure AD Identity Protection allows you to detect potential vulnerabilities affecting your organization's identities, configure automated responses, and investigate incidents. This article describes how to enable Azure AD Identity Protection and view the analysis of your test environment accounts.

There are two phases to setting up Azure AD Identity Protection in your Microsoft 365 Enterprise test environment:

1. Create the Microsoft 365 Enterprise test environment.
2. Enable and use Azure AD Identity Protection.



TIP

Click [here](#) for a visual map to all the articles in the Microsoft 365 Enterprise Test Lab Guide stack.

Phase 1: Build out your Microsoft 365 Enterprise test environment

If you just want to test Azure AD Identity Protection in a lightweight way with the minimum requirements, follow the instructions in [Lightweight base configuration](#).

If you want to test Azure AD Identity Protection in a simulated enterprise, follow the instructions in [Pass-through authentication](#).

NOTE

Testing Azure AD Identity Protection does not require the simulated enterprise test environment, which includes a simulated intranet connected to the Internet and directory synchronization for a Windows Server AD forest. It is provided here as an option so that you can test Azure AD Identity Protection and experiment with it in an environment that represents a typical organization.

Phase 2: Enable and use Azure AD Identity Protection

1. Open a private instance of your browser and sign in to the Azure portal at <https://portal.azure.com> with the global administrator account of your Microsoft 365 Enterprise test environment.
2. In the Azure portal, click **All services > Marketplace**.
3. Type **Azure AD Identity Protection** and then click it.
4. On the **Getting Started** blade, click **Onboard** under **Settings**, click **Pin to dashboard**, and then click **Create**.
5. In the Azure portal, click **Azure AD Identity Protection** on the dashboard.

You should see an **Azure AD Identity Protection-Overview** blade with a dashboard. Under **Vulnerabilities**, notice that it determined the number of user accounts without multi-factor authentication registration. This number will vary based on previous Microsoft 365 Enterprise Test Lab Guides that you have done.

6. Click through the categories for **Investigate** to see if there are any users or events that have been detected.

For further testing and experimentation, see [Simulating risk events](#).

See the [Protect against credential compromise](#) step in the Identity phase for information and links to deploy Azure AD Identity Protection in production.

Next step

Explore additional [identity](#) features and capabilities in your test environment.

See also

[Phase 2: Identity](#)

[Microsoft 365 Enterprise Test Lab Guides](#)

[Microsoft 365 Enterprise deployment](#)

[Microsoft 365 Enterprise documentation](#)

Enroll iOS and Android devices in your Microsoft 365 Enterprise test environment

12/5/2018 • 2 minutes to read • [Edit Online](#)

By following the instructions provided in this article, you'll be able to enroll and test basic mobile device management capabilities for iOS and Android devices in your Microsoft 365 Enterprise test environment.



TIP

Click [here](#) for a visual map to all the articles in the Microsoft 365 Enterprise Test Lab Guide stack.

Phase 1: Build out your Microsoft 365 Enterprise test environment

If you just want to enroll iOS and Android devices in a lightweight way with the minimum requirements, follow the instructions in [Lightweight base configuration](#).

If you want to enroll iOS and Android devices in a simulated enterprise, follow the instructions in [Pass-through authentication](#).

NOTE

Testing automated licensing and group membership does not require the simulated enterprise test environment, which includes a simulated intranet connected to the Internet and directory synchronization for a Windows Server AD forest. It is provided here as an option so that you can test automated licensing and group membership and experiment with it in an environment that represents a typical organization.

Phase 2: Enroll your iOS and Android devices

First, use the instructions in [Install and sign in to the Company Portal app](#) to customize the Microsoft Intune Company Portal app for your test environment.

Next, use the instructions in [Set up access to your company resources](#) to enroll an iOS device.

Next, use the instructions in [Enroll your Android device in Intune](#) to enroll an Android device.

Phase 3: Manage your iOS and Android devices remotely

Microsoft Intune provides both remote lock and passcode reset capabilities. If someone loses their device, you can lock the device remotely. If someone forgets their passcode, you can reset it remotely.

To lock an iOS or Android device remotely:

1. Sign in to the Azure portal at <https://portal.azure.com> with the credentials of your global administrator account.
2. Click **All services**, type **Intune**, and then click **Intune**.
3. Click **Devices > All devices**.

4. In the list of devices, click an iOS or Android device, and then click the **Remote lock** action.

To reset the passcode remotely:

1. If needed, sign in to the Azure portal at <https://portal.azure.com> with the credentials of your global administrator account.
2. Click **All services**, type **Intune**, and then click **Intune**.
3. Click **Devices > All devices**.
4. From the list of devices you manage, click an iOS or Android device, and choose ...**More**. Then choose the **Remove passcode** device remote action.

For additional experimentation, see [Available device actions](#).

Next step

Explore additional [mobile device management](#) features and capabilities in your test environment.

See Also

[Microsoft 365 Enterprise Test Lab Guides](#)

[Device compliance policies for your Microsoft 365 Enterprise test environment](#)

[Deploy Microsoft 365 Enterprise](#)

[Enterprise Mobility + Security \(EMS\)](#)

Device compliance policies for your Microsoft 365 Enterprise test environment

12/5/2018 • 3 minutes to read • [Edit Online](#)

With the instructions in this article, you add an Intune device compliance policy to your Microsoft 365 Enterprise test environment.



TIP

[Click here](#) for a visual map to all the articles in the Microsoft 365 Enterprise Test Lab Guide stack.

Phase 1: Build out your Microsoft 365 Enterprise test environment

If you just want to configure MAM policies in a lightweight way with the minimum requirements, follow the instructions in [Lightweight base configuration](#).

If you want to configure MAM policies in a simulated enterprise, follow the instructions in [Pass-through authentication](#).

NOTE

Testing automated licensing and group membership does not require the simulated enterprise test environment, which includes a simulated intranet connected to the Internet and directory synchronization for a Windows Server AD forest. It is provided here as an option so that you can test automated licensing and group membership and experiment with it in an environment that represents a typical organization.

Phase 2: Create a device compliance policy for Windows 10 devices

In this phase, you create a device compliance policy for Windows 10 devices.

1. Go to the Office portal at (<https://office.com>) and sign in to your Office 365 trial subscription with your global administrator account.
2. On a new tab of your browser, open the Azure portal at <https://portal.azure.com>.
3. On the Azure portal tab in your browser, in the navigation pane, click **All services**, type **Intune**, and then click **Intune**.
4. If you see a **You haven't enabled device management yet** message on the **Microsoft Intune** blade, click it. On the **Mobile Device Management authority** blade, click **Intune MDM Authority**, and then click **Choose**. Refresh your browser tab.
5. In the left navigation pane, click **Groups**.
6. On the **Groups-All groups** blade, click **+ New Group**.

7. On the **Group** blade, select **Office 365** for **Group type?**, type **Managed Windows 10 device users** in **Name**, select **Assigned** in **Membership type**, and then click **Create**.
8. Close the **Group** blade.
9. Close the **Groups-All groups** blade.
10. On the **Microsoft Intune** blade, in the **Quick tasks** list, click **Create a compliance policy**.
11. On the **Compliance Policy Profiles** blade, click **Create Policy**.
12. On the **Create Policy** blade, in **Name**, type **Windows 10**. In **Platform**, select **Windows 10 and later**, click **OK** on the **Windows 10 compliance policy** blade, and then click **Create**. Close the **Windows 10** blade.
13. On the **Compliance Policy Profiles** blade, click the **Windows 10** policy name.
14. On the **Windows 10** blade, click **Assignments**, and then click **Select groups to include**.
15. On the **Select groups to include** blade, click the **Managed Windows 10 device users** group, and then click **Select**.
16. Click **Save**, and then close the **Windows 10 - Assignments** blade.
17. Close the **Compliance Policy Profiles** blade.
18. On the **Microsoft Intune** blade, click **Client apps** in the left navigation.
19. On the **Client Apps** blade, click **Apps**, and then click **Add**.
20. In the **Add app** blade, select **App type**, and then select **Windows 10** under **Office 365 Suite**.
21. Click **Configure App Suite**, and then click **OK**.
22. Click **App Suite Information**, type **Office Apps for Windows 10** in **Suite Name**, **Office Apps for Windows 10** in **Suite Description**, and then click **OK**.
23. Click **App Suite Settings**, select **Semi-Annual** in **Update channel**, and then click **OK**.
24. On the **Add app** blade, click **Add**.

You now have a device compliance policy for testing the selected apps in the **Windows 10** device compliance policy and for members of the **Managed Windows 10 device users** group.

Next step

Explore additional [mobile device management](#) features and capabilities in your test environment.

See also

[Microsoft 365 Enterprise Test Lab Guides](#).

[Enroll iOS and Android devices in your Microsoft 365 Enterprise test environment](#)

[Deploy Microsoft 365 Enterprise](#)

[Enterprise Mobility + Security \(EMS\)](#)

Increased Office 365 security for your Microsoft 365 Enterprise test environment

1/8/2019 • 5 minutes to read • [Edit Online](#)

With the instructions in this article, you configure additional Office 365 settings to increase security in your Microsoft 365 Enterprise test environment.



TIP

Click [here](#) for a visual map to all the articles in the Microsoft 365 Enterprise Test Lab Guide stack.

Phase 1: Build out your Microsoft 365 Enterprise test environment

If you just want to configure increased Office 365 security in a lightweight way with the minimum requirements, follow the instructions in [Lightweight base configuration](#).

If you want to configure increased Office 365 security in a simulated enterprise, follow the instructions in [Pass-through authentication](#).

NOTE

Testing increased Office 365 security does not require the simulated enterprise test environment, which includes a simulated intranet connected to the Internet and directory synchronization for a Windows Server AD forest. It is provided here as an option so that you can test automated licensing and group membership and experiment with it in an environment that represents a typical organization.

Phase 2: Configure increased Office 365 security

In this phase, you enable increased Office 365 security for your Microsoft 365 Enterprise test environment. For additional details and settings, see [Configure your Office 365 tenant for increased security](#).

Configure SharePoint Online to block apps that don't support modern authentication

Apps that do not support modern authentication cannot have [identity and device access configurations](#) applied to them, which is an important element of securing your Microsoft 365 subscription and its digital assets.

1. Go to the Office portal (<https://office.com>) and sign in to your Office 365 trial subscription with your global administrator account.
 - If you are using the lightweight Microsoft 365 test environment, sign in from your local computer.
 - If you are using the simulated enterprise Microsoft 365 test environment, use the [Azure portal](#) to connect to the CLIENT1 virtual machine, and then sign in from CLIENT1.
2. From the **Microsoft 365 admin center** tab, click **Admin**.
3. On the new **Microsoft 365 admin center** tab, click **Admin centers > SharePoint**.

4. On the new **SharePoint admin center** tab, click **Access control**.
5. Under **Apps that don't support modern authentication**, click **Block**, and then click **OK**.

Enable Advanced Threat Protection) for SharePoint, OneDrive for Business, and Microsoft Teams

Office 365 Advanced Threat Protection (ATP) is a feature of Exchange Online Protection (EOP) that helps keep malware out of your email. With ATP, you create policies in the Exchange Admin center (EAC) or the Security & Compliance center that help ensure your users access only links or attachments in emails that are identified as not malicious. For more information, see [Advanced threat protection for safe attachments and safe links](#).

1. On the **Microsoft 365 admin center** tab of your browser, click **Admin centers > Security & Compliance**.
2. On the new **Security & Compliance** tab, click **Threat management > Policy**.
3. Click **ATP safe attachments**.
4. In the **Safe attachments** pane, select **Turn on ATP for SharePoint, OneDrive, and Microsoft Teams**, and then click **Save**.

Enable anti-malware

Malware is comprised of viruses and spyware. Viruses infect other programs and data, and they spread throughout your computer looking for programs to infect. Spyware refers to malware that gathers your personal information, such as sign-in information and personal data, and sends it back to the malware author.

Office 365 has built-in malware and spam filtering capabilities that help protect inbound and outbound messages from malicious software and help protect you from spam. For more information, see [Anti-spam & anti-malware protection in Office 365](#)

To ensure that anti-malware processing is being performed on files with common attachment file types:

1. Click the back button on your browser to get back to the **Policy** page.
2. Click **Anti-malware**.
3. Double-click the policy named **Default**.
4. In the **Anti-malware policy** window, click **Settings**.
5. Under **Common Attachment Types filter**, click **On > Save**.

Phase 3: Examine Office 365 security tools and logs

In this phase, you look at built-in services that inform you about security events and measure your overall security posture.

Threat management dashboard

Office 365 Threat management can help you control and manage mobile device access to your organization's data, help protect your organization from data loss, and help protect inbound and outbound messages from malicious software and spam. You also use threat management to protect your domain's reputation and to determine whether or not senders are maliciously spoofing accounts from your domain. For more information, see [Threat management in the Office 365 Security & Compliance Center](#).

Use these steps to view the Office 365 Threat management dashboard:

1. On the **Microsoft 365 admin center** tab of your browser, click **Admin centers > Security & Compliance**.
2. On the new **Security & Compliance** tab, click **Threat management > Dashboard**.
3. On the new **Dashboard** tab in your browser, note the malware trends, insights, and other sections of the dashboard.

Office 365 Cloud App Security dashboard

Office 365 Cloud App Security, previously known as Office 365 Advanced Security Management, allows you to create policies that monitor for and inform you of suspicious activities in your Office 365 subscription, so that you

can investigate and take possible remediation action. For more information, see [Overview of Office 365 Cloud App Security](#).

1. On the **Microsoft 365 admin center** tab of your browser, click **Admin centers > Security & Compliance**.
2. On the new **Security & Compliance** tab, click **Alerts > Manage advanced alerts > Go to Office 365 Cloud App Security**.
3. On the new **Cloud App Security** tab, note the dashboard view and the list of default policies that monitor for various activities in your Office 365 subscription.
4. Click the dashboard icon to see a summary of Cloud App Security activities that are being tracked.
5. Click **Investigate** (the eyeglasses icon) and then **Activity log** to see the list of recent sign-ins and other activities.

Secure Score

1. Create a new tab in your browser and go to **securescore.office.com**.
2. On the **Dashboard tab**, note your current Secure Score and the list of actions in the queue to increase your score.

See the [Configure increased security for Office 365](#) step in the **Information protection** phase for information and links to configure these settings in production.

Next step

Explore additional [information protection](#) features and capabilities in your test environment.

See also

[Microsoft 365 Enterprise Test Lab Guides](#)

[Deploy Microsoft 365 Enterprise](#)

[Microsoft 365 Enterprise documentation](#)

Data classification for your Microsoft 365 Enterprise test environment

12/17/2018 • 3 minutes to read • [Edit Online](#)

With the instructions in this article, you configure data classification using Office 365 retention labels in your Microsoft 365 Enterprise test environment.



TIP

Click [here](#) for a visual map to all the articles in the Microsoft 365 Enterprise Test Lab Guide stack.

Phase 1: Build out your Microsoft 365 Enterprise test environment

If you just want to configure Office 365 labels in a lightweight way with the minimum requirements, follow the instructions in [Lightweight base configuration](#).

If you want to configure Office 365 labels in a simulated enterprise, follow the instructions in [Pass-through authentication](#).

NOTE

Testing Office 365 labels does not require the simulated enterprise test environment, which includes a simulated intranet connected to the Internet and directory synchronization for a Windows Server AD forest. It is provided here as an option so that you can test automated licensing and group membership and experiment with it in an environment that represents a typical organization.

Phase 2: Create Office 365 labels

In this phase, you create the labels for the different levels of retention for SharePoint Online documents folders.

1. If needed, use a private instance of your Internet browser and sign in to the Office portal with your global administrator account. For help, see [Where to sign in to Office 365](#).
2. From the **Microsoft Office Home** tab, click the **Admin** tile.
3. From the new **Office Admin center** tab of your browser, click **Admin centers > Security & Compliance**.
4. From the new **Home - Security & Compliance** tab of your browser, click **Classifications > Labels**. From the **Home > Labels** pane, click the **Retention** tab.
5. Click **Create a label**.
6. On the **Name your label** pane, type **Internal Public**, and then click **Next**.
7. On the **Label settings** pane, click **Next**.
8. On the **Review your settings** pane, click **Create this label**, and then click **Close**.

9. Repeat steps 5-8 for these additional labels:

- Private
- Sensitive
- Highly Confidential

10. From the **Home > Labels** pane, click **Publish labels**.

11. On the **Choose labels to publish** pane, click **Choose labels to publish**.

12. On the **Choose labels** pane, click **Add** and select all four labels.

13. Click **Done**.

14. On the **Choose labels to publish** pane, click **Next**.

15. On the **Choose locations** pane, click **Next**.

16. On the **Name your policy** pane, type **Example organization** in **Name**, and then click **Next**.

17. On the **Review your settings** pane, click **Publish labels**, and then click **Close**.

Note that it might take a few minutes for the labels to be published.

Phase 3: Apply Office 365 retention labels to documents

In this phase, you discover the default label behavior for files in the Documents folder of a SharePoint Online site and manually change the label of a document.

First, create a sensitive-level SharePoint Online team site:

1. Using a browser on your local computer, sign in to the Office portal using your global administrator account. For help, see [Where to sign in to Office 365](#).
2. In the list of tiles, click **SharePoint**.
3. On the new **SharePoint** tab in your browser, click **Create site**.
4. On the **Create a site** page, click **Team site**.
5. In **Team site name**, type **SensitiveFiles**.
6. In **Team site description**, type **SharePoint site for sensitive files**.
7. In **Privacy settings**, select **Private - only members can access this site**, and then click **Next**.
8. On the **Who do you want to add?** pane, click **Finish**.

Next, configure the Documents folder of the SensitiveFiles team site for the Sensitive label.

1. In the **SensitiveFiles** tab of your browser, click **Documents**.
2. Click the settings icon, and then click **Library settings**.
3. Under **Permissions and Management**, click **Apply label to items in this library**.
4. In **Settings-Apply Label**, select **Sensitive** in the drop-down box, and then click **Save**.

Next, create a new document in the SensitiveFiles site and change its label.

1. In the documents folder, click **New > Word document**.

2. Type some text in the blank document. Wait for the text to be saved.
3. In the menu bar, click **Shared Documents**.
4. Click the Word icon next to the **Document.docx** file name.
5. In the right-hand pane, in the **Properties** section, under **Apply retention label**, note that the document has had the **Sensitive** label automatically applied.
6. Click **Edit all**.
7. In the **Document.docx** pane, under **Apply label**, select the **Highly Confidential** label, and then click **Save**.

See the [Configure classification for your environment](#) step in the **Information protection** phase for information and links to Office 365 retention labels in production.

Next step

Explore additional [information protection](#) features and capabilities in your test environment.

See also

[Microsoft 365 Enterprise Test Lab Guides](#)

[Deploy Microsoft 365 Enterprise](#)

[Microsoft 365 Enterprise documentation](#)

Privileged access management for your Microsoft 365 Enterprise test environment

2/19/2019 • 5 minutes to read • [Edit Online](#)

With the instructions in this article, you configure privileged access management to increase security in your Microsoft 365 Enterprise test environment.



TIP

Click [here](#) for a visual map to all the articles in the Microsoft 365 Enterprise Test Lab Guide stack.

Phase 1: Build out your Microsoft 365 Enterprise test environment

If you just want to configure privileged access management in a lightweight way with the minimum requirements, follow the instructions in [Lightweight base configuration](#).

If you want to configure privileged access management in a simulated enterprise, follow the instructions in [Pass-through authentication](#).

NOTE

Testing privileged access management does not require the simulated enterprise test environment, which includes a simulated intranet connected to the Internet and directory synchronization for a Windows Server AD forest. It is provided here as an option so that you can test privileged access management and experiment with it in an environment that represents a typical organization.

Phase 2: Configure privileged access management

In this phase, you configure an approvers group and enable privileged access management for your Microsoft 365 Enterprise test environment. For additional details and an overview of privileged access management, see [Privileged access management in Office 365](#).

Follow these steps to set up and use privileged access in your Office 365 organization:

- [Step 1: Create an approver's group](#)

Before you start using privilege access, determine who will have approval authority for incoming requests for access to elevated and privileged tasks. Any user who is part of the Approvers' group will be able to approve access requests. This is enabled by creating a mail-enabled security group in Office 365. Create a new security group named "Privileged Access Approvers" in your test environment and add the "User 3" previously created in prior test lab guide steps.

- [Step 2: Enable privileged access](#)

Privileged access needs to be explicitly turned on in Office 365 with the default approver group and

including a set of system accounts that you'd want to be excluded from the privileged access management access control. Be sure to enable privileged access in your Office 365 organization before starting Phase 3 of this guide.

Phase 3: Verify that approval is required for elevated and privileged tasks

In this phase, you verify that the privileged access policy is working and users require approval to execute defined elevated and privileged tasks.

Test ability to execute a task NOT defined in a privileged access policy

First, connect to Exchange Management PowerShell with the credentials of a user configured as a Global Administrator in your test environment and attempt to create a new Journal rule. The [New-JournalRule](#) task is not currently defined in a privileged access policy for your organization.

1. On your local computer, open and sign into the the Exchange Online Remote PowerShell Module at [Microsoft Corporation > Microsoft Exchange Online Remote PowerShell Module](#) using the Global Admin account for your test environment.
2. In Exchange Management Powershell, create a new Journal rule for your organization:

```
New-JournalRule -Name "JournalRule1" -Recipient joe@contoso.onmicrosoft.com -JournalEmailAddress barbara@adatum.com -Scope Global -Enabled $true
```

4. View that the new Journal Rule was successfully created in Exchange Management PowerShell.

Create a new privileged access policy for the New-JournalRule task

NOTE

If you haven't already completed the Steps 1 and 2 from Phase 2 of this guide, be sure follow the steps to create an approver's group named "Privilege Access Approvers" and to enable privileged access in your test environment.

1. Sign into the [Microsoft 365 Admin Center](#) using credentials the Global Admin account for your test environment.
2. In the Admin Center, go to [Settings > Security & Privacy > Privileged access](#).
3. Select **Manage access policies and requests**.
4. Select **Configure policies** and select **Add a policy**.
5. From the drop-down fields, select or enter the following values:

Policy type: Task

Policy scope: Exchange

Policy name: New Journal Rule

Approval type: Manual

Approval group: Privileged Access Approvers

6. Select **Create** and then **Close**. It may take a few minutes for the policy to be fully configured and enabled. Be sure to allow time for the policy to be fully enabled before testing the approval requirement in the next step.

Test approval requirement for the New-JournalRule task defined in a privileged access policy

1. On your local computer, open and sign into the Exchange Online Remote PowerShell Module at **Microsoft Corporation > Microsoft Exchange Online Remote PowerShell Module** using an Global Admin account for your test environment.
2. In Exchange Management Powershell, create a new Journal rule for your organization:

```
New-JournalRule -Name "JournalRule2" -Recipient user1@<your subscription domain> -JournalEmailAddress user1@<your subscription domain> -Scope Global -Enabled $true
```

3. View "Insufficient permissions" error in Exchange Management PowerShell:

```
Insufficient permissions. Please raise an elevated access request for this task.  
+ CategoryInfo          : NotSpecified: (:) [], LocalizedException  
+ FullyQualifiedErrorId : [Server=CY1PR00MB0220,RequestId=7b8c7470-ddd0-4528-a01e-  
5e20ecc9bd54,TimeStamp=9/19/2018  
    7:38:34 PM] [FailureCategory=Cmdlet-LocalizedException] 882BD051  
+ PSComputerName         : outlook.office365.com
```

Request access to create a new Journal Rule using the New-JournalRule task

1. Sign into the [Microsoft 365 Admin Center](#) using the Global Admin account for your test environment.
2. In the Admin Center, go to **Settings > Security & Privacy > Privileged access**.
3. Select **Manage access policies and requests**.
4. Select **New request**. From the drop-down fields, select the appropriate values for your organization:

Request type: Task

Request scope: Exchange

Request for: New Journal Rule

Duration (hours): 2

Comments: Request permission to create a new Journal Rule

5. Select **Save** and then **Close**. Your request will be sent to the approver's group via email.

Approve privileged access request for the creation of a new Journal Rule

1. Sign into the [Microsoft 365 Admin Center](#) using the credentials for User 3 in your test environment (member of the "Privileged Access Approvers" security group in your test environment).
2. In the Admin Center, go to **Settings > Security & Privacy > Privileged access**.
3. Select **Manage access policies and requests**.
4. Select the pending request and select **Approve** to grant access to the Global Admin account to create a new Journal Rule. An notification email confirming that approval has been granted will be sent to the Global Admin account (the requesting user).

Test creating a new Journal Rule with privileged access approved for the New-JournalRule task

1. On your local computer, open and sign into the Exchange Online Remote PowerShell Module at **Microsoft Corporation > Microsoft Exchange Online Remote PowerShell Module** using an Global Admin account for your test environment.
2. In Exchange Management Powershell, create a new Journal rule for your organization:

```
New-JournalRule -Name "JournalRule2" -Recipient user1@<your subscription domain> -JournalEmailAddress  
user1@<your subscription domain> -Scope Global -Enabled $true
```

3. View that the new Journal Rule was successfully created in Exchange Management PowerShell.

Next step

Explore additional [information protection](#) features and capabilities in your test environment.

See also

[Microsoft 365 Enterprise Test Lab Guides](#)

[Deploy Microsoft 365 Enterprise](#)

[Microsoft 365 Enterprise documentation](#)

Microsoft 365 Enterprise for the Contoso Corporation

12/5/2018 • 2 minutes to read • [Edit Online](#)

Summary: How a fictional but representative global organization has adopted Microsoft 365 Enterprise.

Microsoft 365 Enterprise is Microsoft's premier cloud offering that combines Office 365, Windows 10 Enterprise, and Enterprise Mobility + Security (EMS) into a complete, intelligent solution that empowers everyone to be creative and work together, securely.

The Contoso Corporation is a fictional but representative global manufacturing conglomerate with its headquarters in Paris, France. Contoso has deployed Microsoft 365 Enterprise and addressed major design decisions and implementation details for networking, identity, Windows 10 Enterprise, Office 365 ProPlus, mobile device management, information protection, and security.

The overall goal of Contoso for Microsoft 365 Enterprise is to accelerate their digital transformation by using cloud services to bring together its employees, partners, data, and processes to create customer value and maintain its competitive advantage in a digital-first world.

See these articles for the details:

- [Overview](#)

Contoso is a global conglomerate manufacturing, sales, and support organization with over 100,000 products.

- [Contoso's IT infrastructure and needs](#)

Contoso has been transitioning from an on-premises, centralized IT infrastructure to a cloud-inclusive one that incorporates cloud-based personal productivity workloads, applications, and hybrid scenarios.

- [Networking](#)

Contoso's network engineers have optimized traffic to their intranet edge and to the closest Microsoft network location on the Internet.

- [Identity](#)

Contoso's identity in the cloud solution leverages their on-premises identity provider and includes federated authentication with their existing trusted, third-party identity providers.

- [Windows 10 Enterprise](#)

Contoso's Windows 10 Enterprise infrastructure deploys and automatically installs updates for their primary PC and device operating system.

- [Office 365 ProPlus](#)

Contoso Office 365 ProPlus infrastructure deploys and automatically installs updates for the Microsoft Office suite of productivity software.

- [Mobile device management](#)

With many roaming employees and both company and personal smart phones and tablets, Contoso uses mobile device management to enroll and secure the devices and their data.

- [Information protection](#)

To ensure that both common and high-value data is identified, labeled, and subject to layers of security, Contoso enforces its data security policies with Microsoft 365 Enterprise information protection.

- [Summary of Microsoft 365 Enterprise security](#)

Contoso uses the full spectrum of Microsoft 365 Enterprise security features for identity and access management, threat protection, information protection, and security management.

- [SharePoint Online site for highly confidential digital assets](#)

To protect the intellectual property and allow its research teams to more easily collaborate, Contoso used a SharePoint Online site for sites for highly regulated data.

Next step

[Learn](#) about the Contoso Corporation, their worldwide offices, and the design considerations that were addressed when they deployed Microsoft 365 Enterprise.

See also

[Deployment guide](#)

[Test lab guides](#)

Overview of the Contoso Corporation

12/5/2018 • 2 minutes to read • [Edit Online](#)

Summary: Understand the Contoso Corporation as a business and the tiered structure of its worldwide offices.

The Contoso Corporation is a multi-national business with headquarters in Paris, France. It is a conglomerate manufacturing, sales, and support organization with over 100,000 products.



Contoso around the world

Figure 1 shows the headquarters office in Paris and regional hub and satellite offices in various continents.

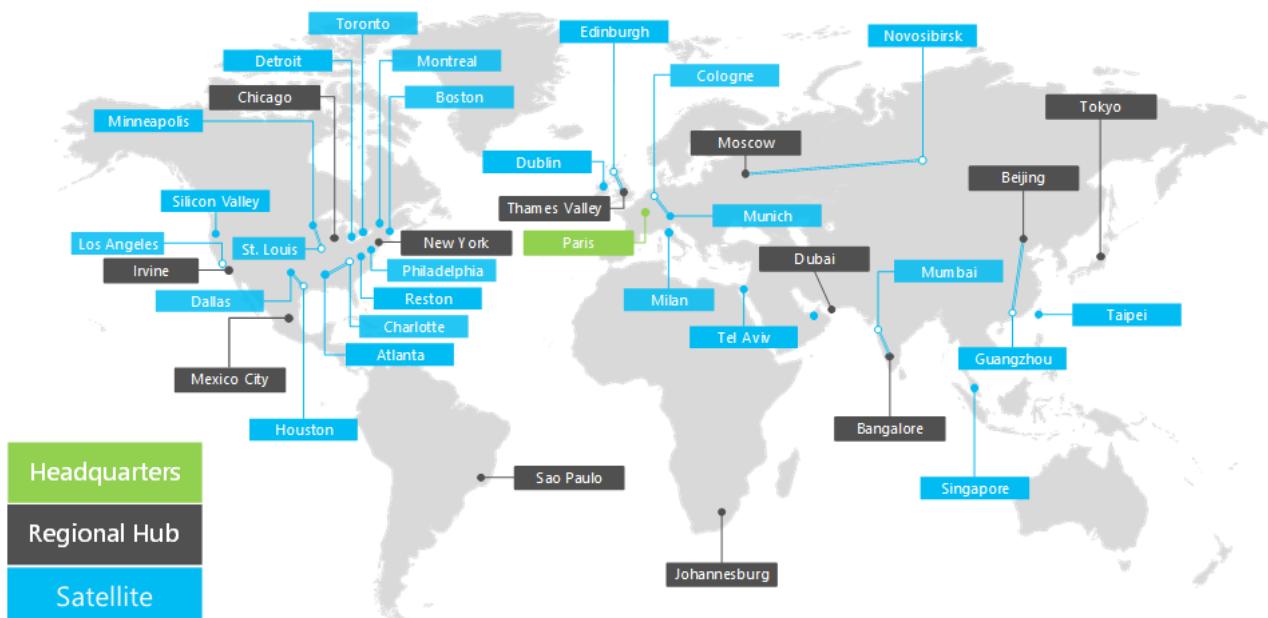


Figure 1: Contoso's offices around the world

Contoso's offices around the world follow a three-tier design.

- Headquarters

The Contoso Corporation headquarters is a large corporate campus on the outskirts of Paris with dozens of buildings for administrative, engineering, and manufacturing facilities. All of Contoso's datacenters and its Internet presence are housed in the Paris headquarters.

The headquarters has 25,000 workers.

- Regional hubs

Regional hub offices serve a specific region of the world with 60% sales and support staff. Each regional hub is connected to the Paris headquarters with a high-bandwidth WAN link.

Each regional hub has an average of 2,000 workers.

- Satellite offices

Satellite offices contain 80% sales and support staff and provide an on-site presence for Contoso

customers in key cities or sub-regions. Each satellite office is connected to a regional hub with a high-bandwidth WAN link.

Each satellite office has an average of 250 workers.

25% of Contoso's workforce is mobile-only, with a higher percentage of mobile-only workers in the regional hubs and satellite offices. Providing better support for mobile-only workers is an important business goal for Contoso.

Design considerations for Microsoft 365 Enterprise

Contoso's IT architects identified the following design considerations when deploying Microsoft 365 Enterprise:

- Multiple geographic locations with local regulations and compliance requirements
- A central intranet datacenter in the headquarters office and regional application servers that host internal line of business applications
- An existing System Center Configuration Manager infrastructure
- A mix of client computing devices, including Windows, Mac, and Linux
- A mix of personal and company-owned mobile devices, including iOS (iPhone and iPad) and Android smart phones and tablets
- Many remote and mobile workers
- Many business partners
- A large amount of customer and personally identifiable data
- A large amount of high-value intellectual property in the form of design specifications for products and manufacturing trade secrets

Next step

[Learn](#) about the Contoso Corporation's on-premises IT infrastructure and how their business needs can be addressed with Microsoft 365 Enterprise.

See also

[Deployment guide](#)

[Test lab guides](#)

Contoso's IT infrastructure and business needs

1/8/2019 • 3 minutes to read • [Edit Online](#)

Summary: Understand the basic structure of Contoso's on-premises IT infrastructure and how its business needs can be met by Microsoft 365 Enterprise.

Contoso has been transitioning from an on-premises, centralized IT infrastructure to a cloud-inclusive one that incorporates cloud-based personal productivity workloads and applications.

Contoso's existing IT infrastructure

Contoso uses a mostly centralized on-premises IT infrastructure, with application datacenters in the Paris headquarters.

Figure 1 shows a headquarters office with application datacenters, a DMZ, and the Internet.

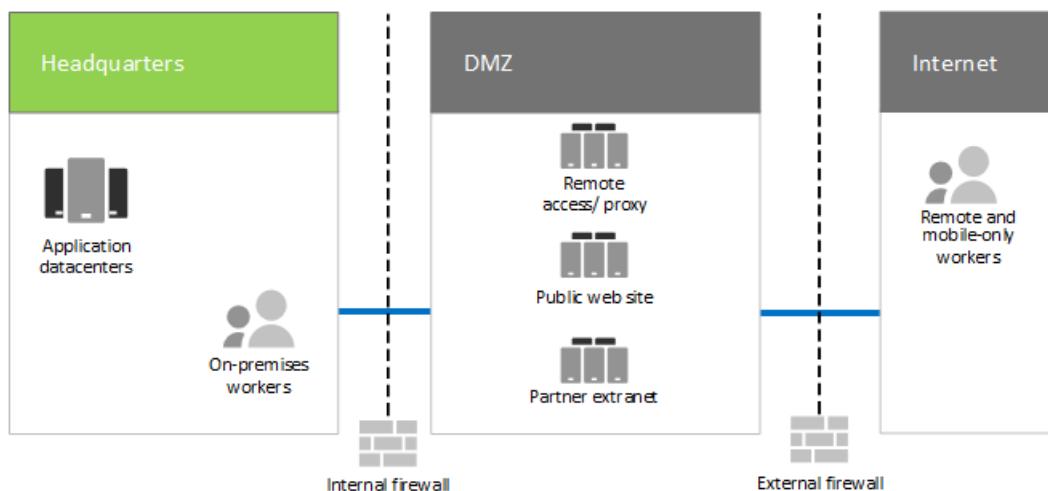


Figure 1: Contoso's existing IT infrastructure

The on-premises application datacenters host:

- Custom line of business applications that use SQL Server and other Linux databases.
- A set of legacy SharePoint servers.
- Organization and team-level servers for file storage.

Additionally, each regional hub office that supports a set of servers with a similar set of applications. These servers are under the control of regional IT departments.

Searchability across the applications and data of these separate multi-geographical datacenters continues to be a challenge.

In Contoso's headquarters DMZ, different sets of servers provide:

- VPN-based remote access to the Contoso intranet and web proxying for workers in the Paris headquarters.
- Hosting for the Contoso public web site, from which customers can order products, parts, supplies, or service.
- Hosting for the Contoso partner extranet for partner communication and collaboration.

Contoso's business needs

Contoso's business needs fall into five main categories.

Productivity:

- Make collaboration easier

Replace the email and file share-based collaboration with an online model that allows real-time changes on documents, easier online meetings, and captured conversation threads.

- Improve productivity for remote and mobile workers

With many employees working from homes or in the field, replace the bottlenecked VPN solution with performant access to Contoso data and resources in the cloud.

- Increase creativity and innovation

Take advantage of the latest visual learning and idea development methods, including inking and 3D visualization.

Security:

- Identity and access management

Enforce multi-factor and other forms of authentication and protect user and administrator account credentials.

- Threat protection

Protect against external security threats, including email and operating system-based malware.

- Information protection

Lock down access to and encrypt high-value digital assets, such as customer data, design specifications, and employee information.

- Security management

Monitor security posture and be able to detect and respond to threats in real time.

Remote and mobile access and business partners:

- Better security for remote and mobile workers

Institute Bring Your Own Device (BYOD) and company-owned device management to ensure secured access, correct application behavior, and company data protection.

- Reduce remote access infrastructure for employees

Reduce maintenance and support costs and improve performance for remote access solution by moving resources commonly accessed to the cloud.

- Provide better connectivity and lower overhead for Business-to-Business (B2B) transactions

Replace aging and expensive partner extranet with a cloud-based solution that uses federated authentication.

Compliance:

- Adhere to regional regulatory requirements

Become and remain compliant with industry and regional regulations for data storage, encryption, data privacy, and personal data regulations, such as the General Data Protection Regulation (GDPR) for the Europe Union.

Management:

- Lower the IT overhead for managing software running on client PCs and devices

Automate the installation of updates to the Windows operating system and Microsoft Office across the organization.

Mapping Contoso's business needs to Microsoft 365 Enterprise

Contoso's IT department determined the following mapping of business needs to Microsoft 365 Enterprise E5 features prior to deployment:

Category	Business need	Microsoft 365 Enterprise products or features
Productivity	Make collaboration easier	Teams, SharePoint Online, Skype for Business Online
	Improve productivity for remote and mobile workers	Office 365 workloads and cloud-based data
	Increase creativity and innovation	Windows Ink, Cortana at Work, PowerPoint
Security	Identity & access management	Dedicated global administrator accounts with Multi-factor authentication (MFA) and Azure AD Privileged Identity Management (PIM) MFA for all user accounts Conditional access Windows Hello Windows Credential Guard
	Threat protection	Advanced Threat Analytics Windows Defender Advanced Threat Protection Office 365 Advanced Threat Protection Office 365 Threat Intelligence
	Information protection	Azure Information Protection Office 365 Data Loss Prevention (DLP) Windows Information Protection Microsoft Cloud App Security Office 365 Cloud App Security (CAS) Microsoft Intune
	Security management	Azure Security Center Windows Defender Security Center
Remote and mobile access and business partners		
	Better security for remote and mobile workers	Microsoft Intune

	Reduce remote access infrastructure for employees	Office 365 workloads and cloud-based data
	Provide better connectivity and lower overhead for B2B transactions	Federated authentication and cloud-based resources
Compliance		
	Adhere to regional regulatory requirements	GDPR features in Office 365
Management		
	Lower the IT overhead for installing client updates	Deployment rings Windows 10 upgrade in place and Autopilot Office 365 ProPlus

Next step

[Learn](#) about the Contoso Corporation's on-premises network and how it was optimized for access and latency to Microsoft 365 cloud-based resources across its organization.

See also

[Deployment guide](#)

[Test lab guides](#)

Networking for the Contoso Corporation

12/5/2018 • 4 minutes to read • [Edit Online](#)

Summary: Understand the Contoso networking infrastructure and how it uses its SD-WAN technology for optimal performance network connectivity to Microsoft 365 Enterprise cloud based services.

To adopt a cloud-inclusive infrastructure, Contoso's network engineers realized the fundamental shift in the way that network traffic to cloud-based services travels. Instead of a hub and spoke model that focusses network connectivity on the head office, they worked to map user locations to local Internet egress and local connections to Microsoft network locations on the Internet.

Contoso's networking infrastructure

The elements of Contoso's network that links their offices across the globe are the following:

- **MPLS WAN network**

An MPLS WAN network connects the Paris headquarters to regional offices and regional offices to satellite offices in a spoke and hub configuration. This is for users to access on-premises servers that make up line of business applications in the Paris office. It also routes any generic Internet traffic to the Paris office where network security devices scrub the requests. Within each office, routers deliver traffic to hosts or wireless access points on subnets, which use the private IP address space.

- **Local direct Internet access for Office 365 traffic**

Each office has an SD-WAN device with one of more local Internet ISP network circuits, with its own Internet connectivity through a proxy server. This is typically implemented as a WAN link to a local ISP that also provides public IP addresses and local DNS server IP addresses for the proxy server.

- **Internet presence**

Contoso owns the contoso.com public domain name. The Contoso public web site for ordering products is a set of servers in an Internet-connected datacenter in the Paris campus. Contoso uses a /24 public IP address range on the Internet.

Figure 1 shows Contoso's networking infrastructure and its connections to the Internet.

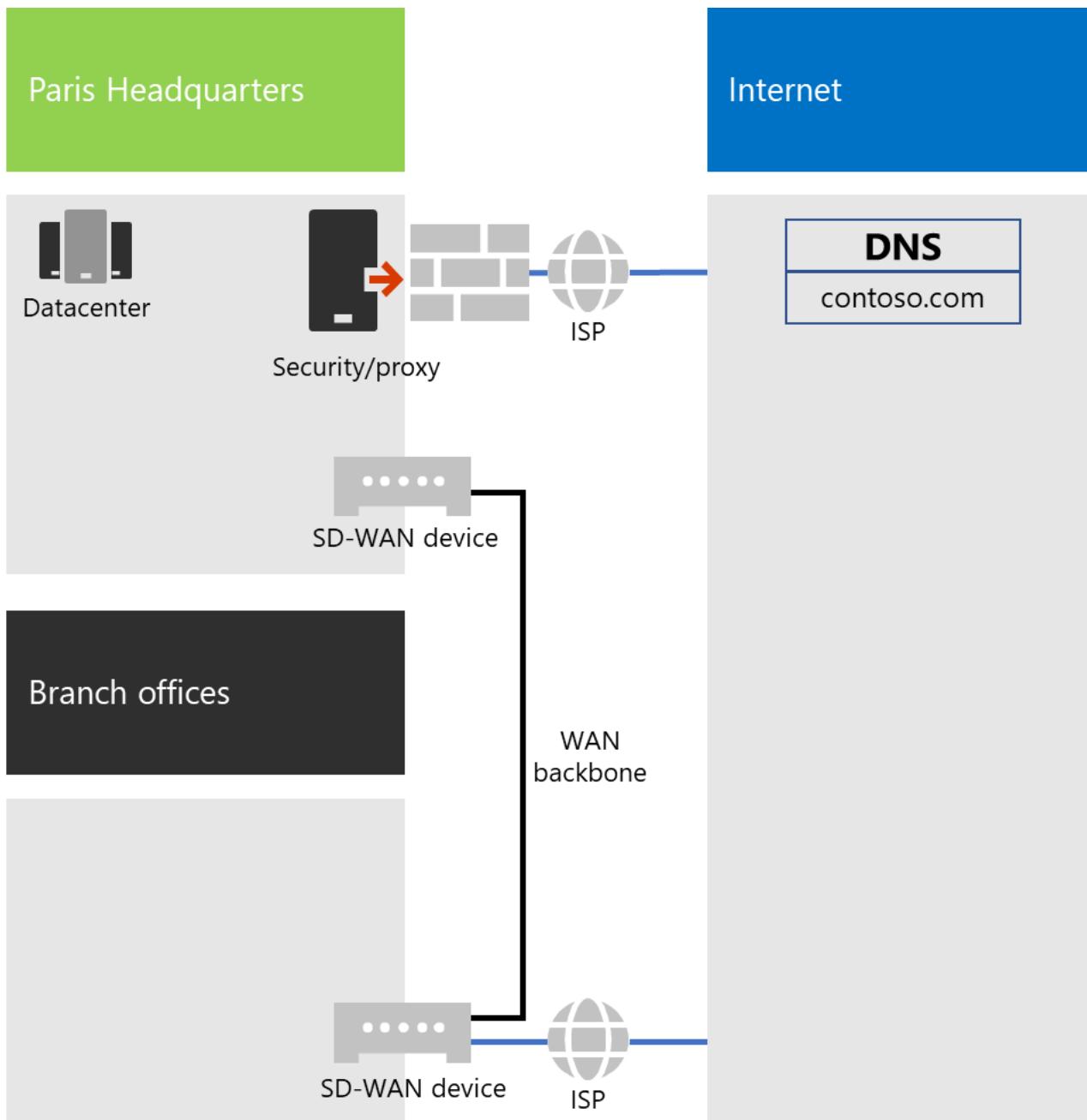


Figure 1: Contoso's network

Use of SD-WAN for optimal network connectivity to Microsoft

Contoso followed [Office 365 network connectivity principles](#):

1. Identify and differentiate Office 365 network traffic
2. Egress network connections locally
3. Avoid network hairpins
4. Bypass duplicate network security devices

There are three categories of network traffic for Office 365: Optimize, Allow, and Default. Optimize and Allow traffic is trusted network traffic that is encrypted and secured at the endpoints and is destined for Microsoft datacenters.

Contoso decided to use direct Internet egress for Optimize and Allow category traffic and to forward all Default category traffic to the Paris-based central Internet connection.

They decided to deploy SD-WAN devices at each of their office locations as a simple way to follow these principles and achieve optimal network performance for Microsoft 365 cloud-based services.

The SD-WAN devices have a LAN port for the local office network and multiple WAN ports. One WAN port connects to their MPLS network and other WAN ports connect to local ISP circuits. The SD-WAN device routes Optimize and Allow category network traffic to the ISP links.

Contoso's line of business app infrastructure

Contoso has architected its line of business application and server infrastructure for the following:

- Satellite offices use local caching servers to store frequently accessed documents and internal web sites.
- Regional hubs use regional application servers for the regional and satellite offices. These servers synchronize with servers in the Paris headquarters.
- The Paris campus has the datacenters that contain the centralized application servers that serve the entire organization.

Figure 2 shows the percentage of network traffic when accessing servers across Contoso's intranet.

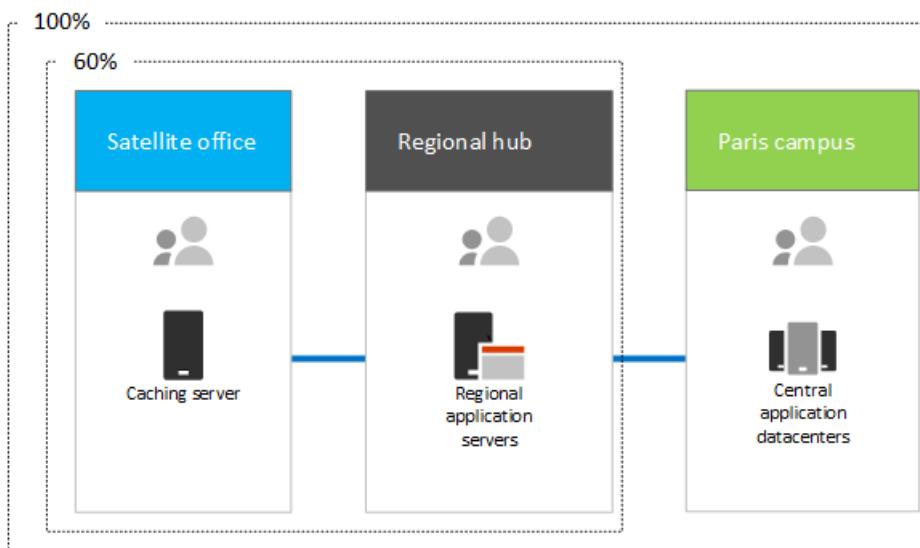


Figure 2: Contoso's infrastructure for internal applications

For users in satellite or regional hub offices, 60% of the resources needed by employees can be served by satellite and regional hub office servers. The additional 40% of resource requests must go over the WAN link to the Paris campus.

Contoso's network analysis and preparation of their network for Microsoft 365 Enterprise

Successful adoption of Microsoft 365 Enterprise services by Contoso's users depend on highly available and performant connectivity to the Internet, or directly to Microsoft cloud services. Contoso took these steps to plan for and implement optimized connectivity to Microsoft 365 Enterprise cloud services:

1. Created a company WAN network diagram to aid with planning

Contoso started their network planning by creating a diagram showing their locations, the existing network connectivity, their existing network perimeter devices and classes of service that are managed on the network. They used this diagram for each subsequent step in the planning and implementation of networking connectivity.

2. Created a plan for Microsoft 365 Enterprise network connectivity

Contoso used the [Office 365 network connectivity principles](#) and provided reference network architectures to determine SD-WAN as their preferred topology for Office 365 connectivity.

3. Analyzed Internet connection utilization and MPLS WAN bandwidth at each office and increased bandwidth as needed

Each office was analyzed for the current usage and circuits were increased so that predicted Microsoft 365 cloud-based traffic would be operating with an average of 20% of unused capacity.

4. Optimized performance to Microsoft network services

Contoso determined the set of Office 365, Intune, and Azure endpoints and configured firewalls, security devices, and other systems in the Internet path for optimal performance. Endpoints for Office 365 Optimize and Allow category traffic was configured into the SD-WAN devices that provided direct Internet access.

5. Configured internal DNS

DNS is required to be functional and to be looked up locally for Office 365 traffic.

6. Validated network endpoint and port connectivity

Contoso ran network connectivity test tools provided by Microsoft to validate connectivity for Microsoft 365 Enterprise cloud services.

7. Optimized employee computers for network connectivity

Individual computers were checked to ensure that the latest operating system updates were installed and that endpoint security monitoring is active on all clients.

Next step

[Learn](#) how Contoso is leveraging its on-premises identity provider in the cloud for employees and federating authentication for customers and business partners.

See also

[Networking for Microsoft 365 Enterprise](#)

[Deployment guide](#)

[Test lab guides](#)

Identity for the Contoso Corporation

2/13/2019 • 2 minutes to read • [Edit Online](#)

Summary: How Contoso takes advantage of Identity as a Service (IDaaS) and provides cloud-based authentication for its employees and federated authentication for its partners and customers.

Microsoft provides an Identity as a Service (IDaaS) across its cloud offerings with Azure Active Directory (Azure AD). To adopt Microsoft 365 Enterprise, Contoso's IDaaS solution had to leverage their on-premises identity provider and still include federated authentication with their existing trusted, third-party identity providers.

Contoso's Windows Server AD forest

Contoso uses a single Active Directory Domain Services (AD DS) forest for contoso.com with seven sub-domains, one for each region of the world. The headquarters, regional hub offices, and satellite offices contain domain controllers for local authentication and authorization.

Figure 1 shows the Contoso forest with regional domains for the different parts of the world that contain regional hubs.

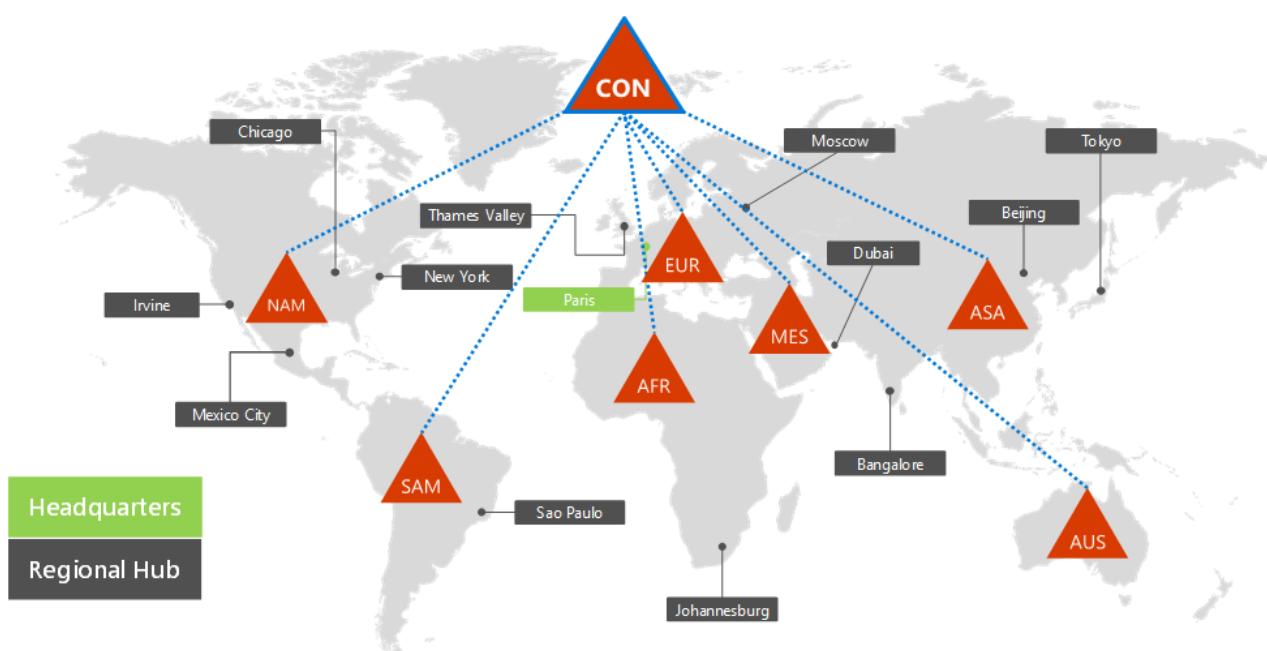


Figure 1: Contoso's forest and domains worldwide

Contoso wanted to use the accounts and groups in the contoso.com forest for authentication and authorization for its Microsoft 365 workloads and services.

Contoso's federated authentication infrastructure

Contoso allows:

- Customers to use their Microsoft, Facebook, or Google Mail accounts to sign in to their public web site.
- Vendors and partners to use their LinkedIn, Salesforce, or Google Mail accounts to sign in to the partner extranet.

Figure 2 shows the Contoso DMZ containing a public web site, a partner extranet, and a set of Active Directory Federation Services (AD FS) servers. The DMZ is connected to the Internet that contains customers, partners, and

Internet services.

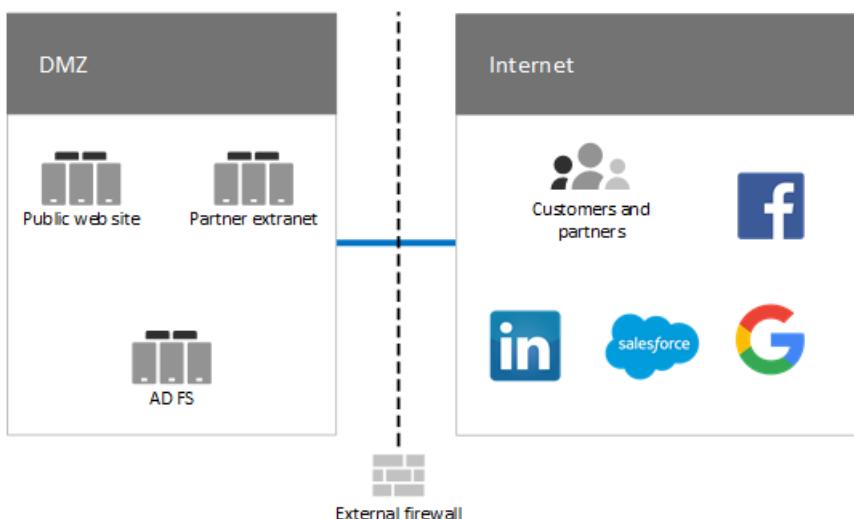


Figure 2: Contoso's support for federated authentication for customers and partners

AD FS servers in the DMZ authenticate customer credentials for access to the public web site and partner credentials for access to the partner extranet.

Contoso decided to keep this infrastructure and dedicate it to customer and partner authentications. Contoso identity engineers are investigating the conversion of this infrastructure to Azure AD [B2B](#) and [B2C](#) solutions.

Hybrid identity with password hash synchronization for cloud-based authentication

Contoso wanted to leverage its on-premises Windows Server AD forest for authentication to Microsoft 365 cloud resources. It decided on password hash synchronization (PHS).

PHS synchronizes the on-premises Windows Server AD forest with the Azure AD tenant of their Microsoft 365 Enterprise subscription, copying user and group accounts and a hashed version of user account passwords.

To perform the ongoing directory synchronization, Contoso has deployed the Azure AD Connect tool on a server in its Paris datacenter. Figure 3 shows the server running Azure AD Connect polling the Contoso Windows Server AD forest for changes and then synchronizing those changes with the Azure AD tenant.

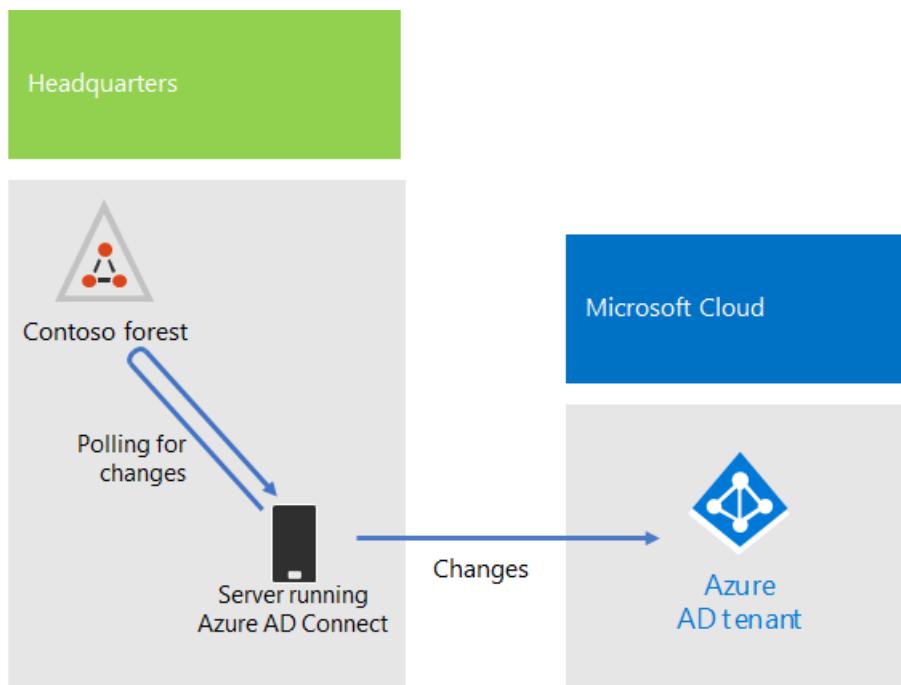


Figure 3: Contoso's PHS directory synchronization infrastructure

Conditional access policies for identity and device access

Contoso created a set of Azure AD and Intune [conditional access policies](#) for three protection levels:

- **Baseline** protections apply to all user accounts
- **Sensitive** protections apply to senior leadership and executive staff
- **Highly Regulated** protections apply to specific users in the finance, legal, and research departments that have access to highly regulated data

Figure 4 shows their resulting set of identity and device conditional access policies.

Protection level	Device type	Azure AD conditional access policies			Azure AD Identity Protection user risk policy	Intune device compliance policy	Intune app protection policies
Baseline: All user accounts	 	Require multi-factor authentication (MFA) when sign-in risk is medium or high	Require approved apps	Block clients that don't support modern authentication	Require compliant PCs	High risk users must change password	Compliance policies for Windows, iOS, and Android App protection policies for iOS and Android
Sensitive: Executive staff user accounts	 	Require MFA when sign-in risk is low, medium, or high			Require compliant PCs and mobile devices		
Highly regulated: Finance, legal, and research user accounts	 	Always require MFA					

Figure 4: Contoso's identity and device conditional access policies

Next step

[Learn](#) how Contoso is leveraging its System Center Configuration Manager infrastructure to deploy and keep current Windows 10 Enterprise across its organization.

See also

[Identity for Microsoft 365 Enterprise](#)

[Deployment guide](#)

[Test lab guides](#)

Windows 10 Enterprise deployment for Contoso

12/5/2018 • 3 minutes to read • [Edit Online](#)

Summary: Understand how Contoso used System Center Configuration Manager to deploy in-place upgrades for Windows 10 Enterprise.

Prior to the wide rollout of Microsoft 365 Enterprise, Contoso had Windows-compatible PCs and devices running a mixture of Windows 7 (10%), Windows 8.1 (65%), and Windows 10 (25%). Contoso wanted to upgrade their PCs for Windows 10 Enterprise take advantage of improved security and lowered IT overhead from automated deployments of updates.

After assessing their infrastructure and business needs, Contoso identified these key requirements for the deployment:

- As many PCs and devices as possible should run Windows 10 Enterprise
- Rollout of the in-place upgrades leverages existing System Center Configuration Manager infrastructure
- Control over which versions of Windows 10 Enterprise to deploy and updates are done through rings
- PCs and devices should stay up to date with minimal IT administrative costs and with minimal impact to end-users

Up to date is defined as the supported version of Windows 10 Enterprise that meets Contoso's business needs, which can be different from having all Windows-compatible PCs running the latest version of Windows 10 Enterprise.

Deployment tools

Prior to and during in-place upgrades of Windows 10 Enterprise, Contoso used the following solutions of Windows Analytics:

- Upgrade Readiness

Collects system, application, and driver data for analysis, and then identifies compatibility issues that can block an upgrade and suggested fixes the issues are known to Microsoft.

- Update Compliance

Collects system and diagnostics data including update installation progress, Windows Update for Business (WUfB) configuration data, Windows Defender Antivirus data, and other update-specific information, and then stores this data in the cloud analysis and usage.

- Device Health

Collects Windows 10 system and diagnostic data including update installation progress, Windows Update for Business (WUfB) configuration data, Windows Defender Antivirus data, and other update-specific information, and then stores this data in the cloud analysis and usage.

Contoso has an existing System Center Configuration Manager (Current Branch) infrastructure. Configuration Manager scales for large environments and provides extensive control over installation, updates, and settings. It also has built-in features to make it easier and more efficient to deploy and manage Windows 10 Enterprise.

Planning process

Prior to deployment, Contoso defined the following rings:

- Three rings for validation and deployment staging
 - One for preview builds
 - One for new release builds
 - One for a previous build
- One ring for broad deployment of Windows 10 Enterprise based on data from the validation rings

Contoso also used the Upgrade Readiness solution of Windows Analytics to determine the set of installed apps and their compatibility with Windows 10 Enterprise.

Deployment process

To complete the in-place upgrade deployment of Windows 10 Enterprise, Contoso implemented the following process, which includes best practice recommendations from Microsoft:

1. Enabled peer cache for Configuration Manager.
2. Created customized Windows packages based on images from the Volume Licensing Service Center.
3. Used Configuration Manager to deploy the Windows packages to distribution points across their network and deployed builds to the three validation and deployment staging rings.
4. Performed assessment of success for PCs and devices in the three validation and deployment staging rings using the Device Health and Update Compliance solutions of Windows Analytics.
5. Based on the Windows Analytics information, Contoso determined the version of Windows 10 Enterprise to deploy to the broad deployment ring.
6. Ran the Configuration Manager deployment task sequences to deploy the selected Windows package to the broad deployment ring.
7. Monitored PCs and devices in the broad deployment ring using the Device Health and Update Compliance solutions provided by Windows Analytics to address issues.

Figure 1 shows the in-place upgrade and ongoing updates deployment architecture.

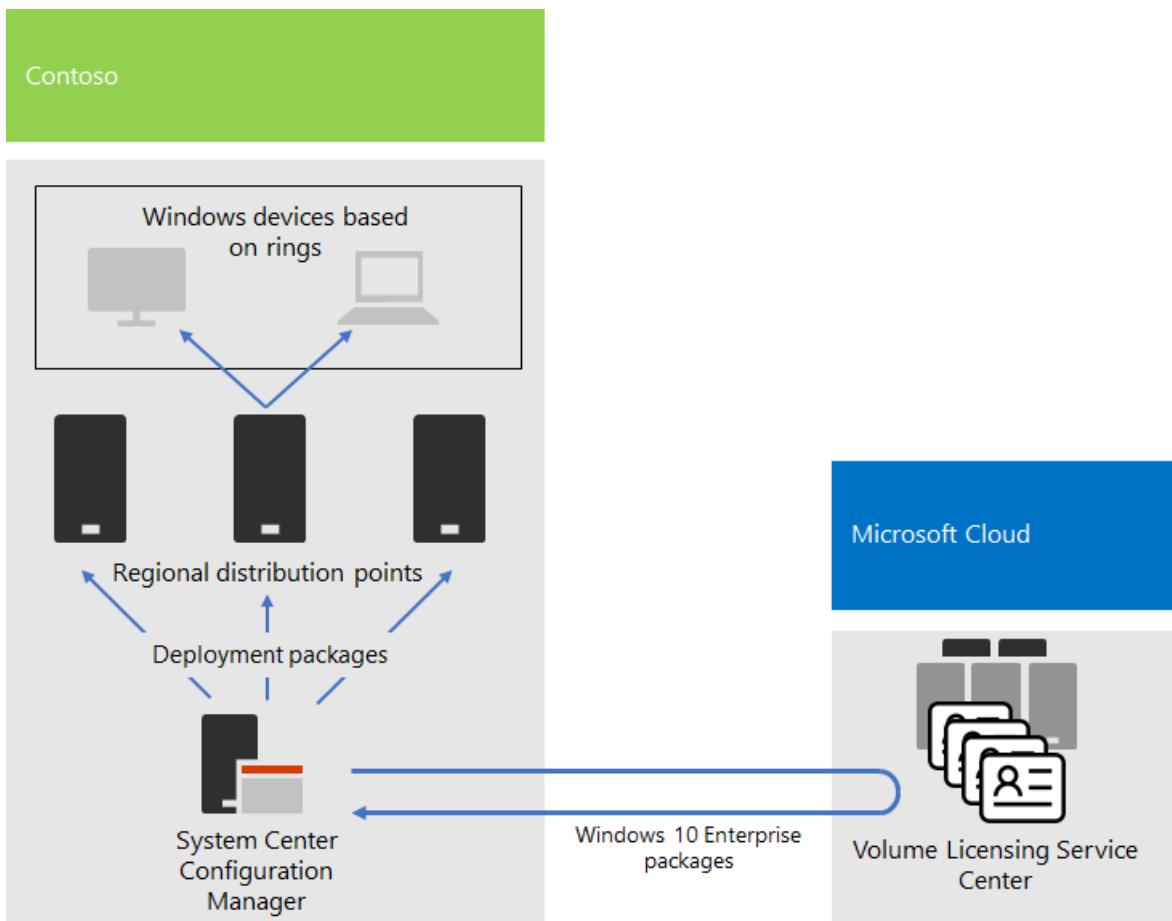


Figure 1: Contoso's Windows 10 Enterprise deployment infrastructure

This infrastructure consists of:

- System Center Configuration Manager, which:
 - Obtains images for Windows 10 Enterprise packages from the Microsoft Volume Licensing Center in the Microsoft Network.
 - Is the central administration point for deployment packages.
- Regional distribution points that are typically located in Contoso's satellite offices.
- Windows PCs and devices in various locations that receive and install the deployment packages for the in-place upgrade or ongoing updates based on ring membership.

Next step

[Learn](#) how Contoso is leveraging its System Center Configuration Manager infrastructure to deploy and keep current Office 365 ProPlus across its organization.

See also

[Windows 10 Enterprise for Microsoft 365 Enterprise](#)

[Deployment guide](#)

[Test lab guides](#)

Office 365 ProPlus deployment for Contoso

12/5/2018 • 4 minutes to read • [Edit Online](#)

Summary: Understand how Contoso uses System Center Configuration Manager to deploy Office 365 ProPlus.

Contoso upgraded their PCs to Windows 10 Enterprise and Office 365 ProPlus to enable more effective collaboration, better security, and a more modern desktop experience. After assessing their infrastructure and business needs, Contoso identified these key requirements for the deployment:

- All PCs should run Office 365 ProPlus
- Deployment should use existing management tools and infrastructure when possible
- Deployment must support multiple languages and existing architectures on end-user devices
- PCs should stay up-to-date and secure with minimal IT administrative costs and with minimal impact to end-users

Deployment tools

Based on their requirements, Contoso chose to deploy Windows and Office with System Center Configuration Manager (Current Branch). Configuration Manager scales for large environments and provides extensive control over installation, updates, and settings. It also has built-in features to make it easier and more efficient to deploy and manage Office, including:

- Peer cache, which can help with limited network capacity when deploying to devices in remote locations
- The Office Client Management dashboard, which makes it easy to deploy Office and monitor updates and gives administrators access to the latest deployment and management features
- Intelligent language pack deployment, including automatically deploying the same language as the operating system
- Fully supported and easy-to-use method of removing existing versions of Office from a client during deployment

In addition to Configuration Manager, Contoso used the [Readiness Toolkit](#), a free tool from Microsoft, to assess compatibility issues with their Office macros and add-ins.

Managing the deployment and updates

Office 365 ProPlus has a new release model: Office as a service. The service model makes it easy to stay up to date with new features, but often requires a change in approach for IT departments in how new releases are deployed and tested. To minimize any compatibility issues and to ensure their computers stayed up to date, Contoso deployed Windows and Office in two stages:

- For the first stage, they deployed Office 365 ProPlus to a small set of representative devices across the organization. This pilot group was used to test apps, add-ins, and hardware with Office 365 ProPlus
- Four months later, after addressing all critical issues with apps, add-ins, and hardware in the pilot group, Contoso deployed Office 365 ProPlus to the rest of the devices in the organization (the broad group).

Instead of managing updates to Office with Configuration Manager, Contoso enabled automatic updates from the cloud. Cloud-based updates reduced their administrative overhead while ensuring the devices stayed up to date.

Contoso followed the same two-stage approach for feature updates+ that they used for deploying Office: devices in the pilot group received feature updates four months earlier than devices in the rest of the organization (the broad group). To enable this for Office, Contoso used two recommended [update channels](#):

- Semi-Annual Channel (Targeted) for updates to the pilot group
- Semi-Annual Channel for updates to the broad group.

Because the Semi-Annual (Targeted) Channel releases a version of Office 365 ProPlus four months earlier than the Semi-Annual Channel, Contoso has time to validate the updates without having to manage them.

Deployment process

To complete the deployment of Office, Contoso implemented the following process, which includes best practice recommendations from Microsoft:

1. Before deploying, they used the Readiness Toolkit to test their apps and Office add-ins to assess their compatibility with Office 365 ProPlus.
2. In Configuration Manager, Contoso enabled peer cache on their client devices, which helped with limited network capacity when deploying to client devices in remote locations.
3. They defined two deployment groups as device collections in Configuration Manager: a pilot group and a broad group. The pilot group, which included a small set of representative devices across the organization, was used to do additional testing of apps, add-ins, and hardware with Windows 10 Enterprise and Office 365 ProPlus.
4. They created deployment packages for Office using the Office Client Management dashboard and the Office 365 Installer wizard, both of which are part of the Configuration Manager console. They built two Office 365 ProPlus packages, one for the pilot group on the Semi-Annual Channel (Targeted) and one for the broad group on the Semi-Annual Channel.
5. As part of each Office package, they included English, French, and German Language packs. If a device required a language not included in the Office package, it was automatically downloaded from the Office Content Delivery Network (CDN).
6. They used the built-in feature in the Office package to automatically remove all existing MSI versions of Office before installing Office 365 ProPlus.
7. In Configuration Manager, they deployed the Windows and Office packages to distribution points across their network, and then ran the Configuration Manager deployment task sequences to deploy the pilot Office 365 ProPlus package to the pilot group.
8. After addressing any compatibility issues with the pilot group, Contoso ran the task sequences to deploy the broad Office 365 ProPlus package to the broad group.

Because Contoso chose to automatically update devices from the cloud, there was no need to manage the process in Configuration Manager. Their devices are automatically updated directly from the cloud based on the update channel that was defined as part of the initial deployment.

Next step

[Learn](#) how Contoso is using Enterprise Mobility + Security (EMS) in Microsoft 365 Enterprise to manage its devices and the apps that run on them across its organization.

See also

[Office 365 ProPlus for Microsoft 365 Enterprise](#)

[Deployment guide](#)

[Test lab guides](#)

Mobile device management for Contoso

1/18/2019 • 2 minutes to read • [Edit Online](#)

Summary: Understand how Contoso uses EMS in Microsoft 365 Enterprise to manage its devices and the apps that run on them.

Enterprise Mobility + Security (EMS) in Microsoft 365 Enterprise consists of Microsoft Intune and a set of Azure services to support mobile device and application management and security.

Contoso has many mobile-enabled employees, some of which have offices in Contoso locations and some of which have no offices. Contoso needed a way to enable employee productivity but keep the devices, the Contoso data stored on those devices, and application behavior secure.

Plan

Early in the analysis of mobile device management for Microsoft 365 Enterprise, Contoso identified the following Intune use cases:

- Protect Exchange Online email and data so it can be safely accessed by mobile devices
- Implement a bring your own device (BYOD) program for Contoso employees
- Issue organization-owned phones and limited-use shared tablets to Contoso employees

Contoso is not using Intune to:

- Allow employees to securely access Office 365 from an unmanaged public kiosk
- Protect on-premises email and data so it can be safely accessed by mobile devices, because there are no longer on-premises Microsoft Exchange servers.

Deploy

This is how Contoso set up their mobile device management infrastructure:

- Set Intune as the Mobile Device Management (MDM) authority and are using Intune on Azure to administer content and manage the devices
- Created Azure AD groups for devices for enrollment and Intune settings and device-based conditional access policies

See [Contoso's conditional access policies](#) for more information.

- Enabled the Apple device platform to support employees with iPads, iMacs, iPhones, and for iPhone-based corporate-owned phones
- Created Contoso-specific terms and conditions policies, which are seen during the installation of the Company Portal for Contoso on mobile devices
- For devices that are not enrolled, a set of Mobile Application Management (MAM) policies to require authentication for access to Office 365 services
- Created Intune policies that enforce:
 - Allowed apps
 - Device encryption to help prevent unauthorized access
 - A six-digit PIN or password

- An inactivity timeout period
- Antivirus and malware protection, and signature updates with Windows Defender on Windows 10 devices
- Automatic updates on Windows 10 devices that include the latest security updates
- Pushing certificates to managed devices
- A clear separation of business and personal data. Users or admins can selectively wipe corporate data from the device, while leaving personal data such as pictures, personal email accounts, and personal files untouched.

Once deployed, Contoso enrolled PCs and company-owned smartphones and tablets by adding them to the appropriate Intune device groups and rolled out a BYOD program for employees to enroll their personal devices. Enrolled devices received Intune policies, resulting in managed and secured devices and their applications. Devices that are not enrolled have Mobile Application Management (MAM) policies that specify allowed applications.

Next step

[Learn](#) how Contoso uses the information protection capabilities of Microsoft 365 Enterprise to classify, identify, and protect crucial digital assets across its organization.

See also

[Mobile device management for Microsoft 365 Enterprise](#)

[Deployment guide](#)

[Test lab guides](#)

Information protection for the Contoso Corporation

1/8/2019 • 5 minutes to read • [Edit Online](#)

Summary: Understand how Contoso uses information protection features in Microsoft 365 Enterprise to secure their digital assets in the cloud.

Contoso is serious about their information security and protection. For example, leakage or destruction of their intellectual property describing product designs and proprietary manufacturing techniques would place them at a competitive disadvantage.

Before moving their sensitive and most valuable digital assets to the cloud, they made sure that their on-premises information classification and protection requirements were supported and implemented in the cloud-based services of Microsoft 365 Enterprise.

Contoso's data security classification

Contoso performed an analysis of their data and determined the following levels.

Level 1: Baseline	Level 2: Sensitive	Level 3: Highly regulated
<p>Data is encrypted and available only to authenticated users</p> <p>Provided for all data stored on premises and in cloud-based storage and workloads, such as Office 365. Data is encrypted while it resides in the service and in transit between the service and client devices.</p> <p>Examples of Level 1 data are normal business communications (email) and files for administrative, sales, and support workers.</p>	<p>Level 1 plus strong authentication and data loss protection:</p> <p>Strong authentication includes multi-factor authentication with SMS validation. Data loss prevention ensures that sensitive or critical information does not travel outside the on-premises network.</p> <p>Examples of Level 2 data are financial and legal information and research and development data for new products.</p>	<p>Level 2 plus the highest levels of encryption, authentication, and auditing.</p> <p>The highest levels of encryption for data at rest and in the cloud, compliant with regional regulations, combined with multi-factor authentication with smart cards and granular auditing and alerting.</p> <p>Examples of Level 3 data are customer and partner personally identifiable information, product engineering specifications, and proprietary manufacturing techniques.</p>

Contoso's information policies

The following table lists Contoso's information policies.

	Access	Data retention	Information protection
Level 1: Low business value (Baseline)	Allow access to all	6 months	Use encryption

Level 2: Medium business value (Sensitive)	Allow access to Contoso employees, subcontractors, and partners Use multi-factor authentication (MFA), Transport Layer Security (TLS), and Mobile Application Management (MAM)	2 years	Use hash values for data integrity
Level 3: High business value (Highly regulated)	Allow access to executives and leads in engineering and manufacturing Rights Management System (RMS) with managed network devices only	7 years	Use digital signatures for non-repudiation

Contoso's path to information protection with Microsoft 365 Enterprise

Contoso used the following steps to prepare Microsoft 365 Enterprise for their information protection requirements:

1. Identified what information to protect

Contoso did an extensive review of their existing digital assets located on on-premises SharePoint sites and file shares and classified each one.

2. Determined access, retention, and information protection policies for data levels

Based on the data levels, Contoso determined detailed policy requirements, which were used to protect existing digital assets as they were moved to the cloud.

3. Created Azure Information Protection labels and their settings for the different levels of information

Contoso modified the default Azure Information Protection labels with the titles that match their data levels and configured the Sensitive and Highly regulated labels to encrypt with Azure cloud key. They created sub-labels of the Highly regulated label for specific types of trade secret data and confined their access to specific research and development groups. Contoso also deployed the Azure Information Protection client to all Windows PCs and devices.

4. Created protected SharePoint Online sites for sensitive and highly regulated data with permissions that lock down access

Both sensitive and highly regulated sites were configured as [isolated sites](#), in which the default SharePoint Online team site permissions were customized to Azure AD groups. Sensitive and highly regulated SharePoint Online sites were also configured with a default Office 365 label. Files stored in highly regulated SharePoint Online sites are protected with an Azure Information Protection sub-label of a scoped policy. For more information, see the [Microsoft Teams and SharePoint Online sites for highly regulated data scenario](#).

5. Moved data from on-premises SharePoint sites and file shares to their new SharePoint Online sites

The files migrated to the new SharePoint Online sites inherited the default Office 365 labels assigned to the site.

- Trained employees on how to use Azure Information Protection labels for new documents, how to interact with Contoso IT when creating new SharePoint Online sites, and to always store digital assets on SharePoint Online sites

Considered the hardest part of the information protection transition for the cloud, Contoso IT and management needed to change the bad information storage habits of the organization's employees to always label their digital assets and never use on-premises file shares.

Conditional access policies for information protection

In conjunction with their identity and mobile device management infrastructure and as part of their rollout of Exchange Online and SharePoint Online, Contoso configured the following set of conditional access policies and applied them to the appropriate Azure AD groups:

- Managed and unmanaged application access on devices policies
- Exchange Online access policies
- SharePoint Online access policies

Figure 1 shows Contoso's resulting set of policies for information protection.

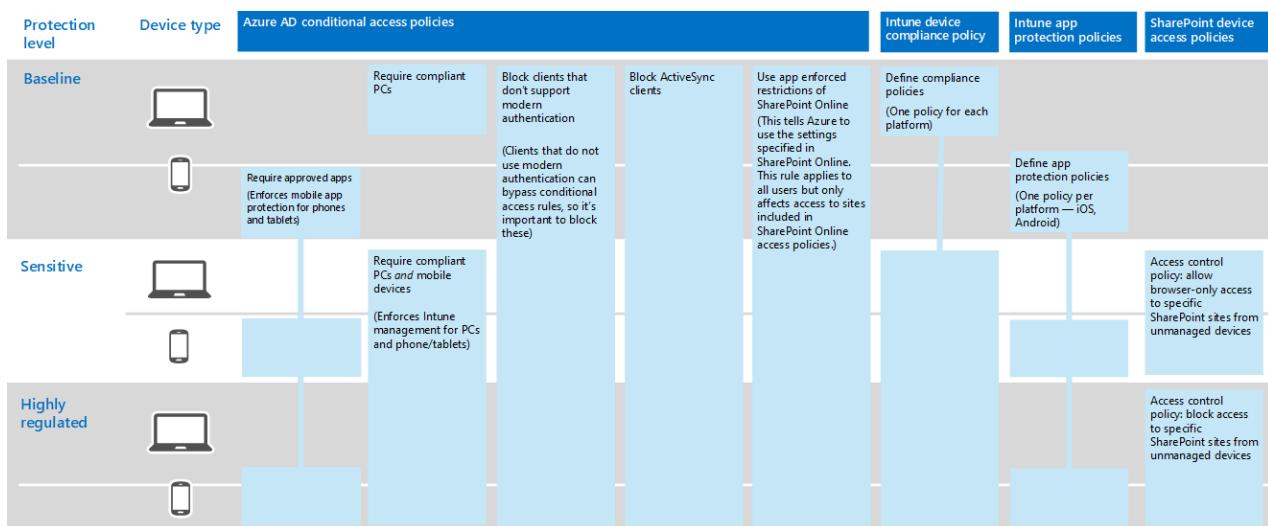


Figure 1: Device, Exchange Online, and SharePoint Online conditional access policies

NOTE

Contoso also configured additional conditional access policies for identity and sign-in. See [Identity for the Contoso Corporation](#).

These policies ensure that:

- App protection policies define which apps are allowed and the actions they can take with your organization data.
- PCs and mobile devices must be compliant.
- Exchange Online uses Office 365 message encryption for Exchange Online.
- SharePoint Online uses app enforced restrictions.
- SharePoint Online uses access control policies for browser-only access and to block access for unmanaged devices.

Mapping Microsoft 365 Enterprise features to Contoso's data levels

The following table shows the mapping the Contoso's data levels to information protection features in Microsoft

	Office 365	Windows 10 and Office 365 ProPlus	EMS
Level 1: Baseline	SharePoint Online and Exchange Online conditional access policies Permissions on SharePoint Online sites	Azure Information Protection client BitLocker Windows Information Protection	Device conditional access policies and Mobile Application Management policies
Level 2: Highly sensitive	Level 1: Baseline plus: Azure Information Protection labels Office 365 labels on SharePoint Online sites Office 365 Data Loss Prevention for SharePoint Online and Exchange Online Isolated SharePoint Online sites	Level 1: Baseline plus: Azure Information Protection labels on digital assets Office 365 Advanced Data Governance	Level 1: Baseline
Level 3: Highly regulated	Level 2: Highly sensitive plus: Bring Your Own Key (BYOK) encryption and protection for trade secret information Azure Key Vault for line of business applications that interact with Office 365 services	Level 2: Highly sensitive	Level 1: Baseline

Next step

[See](#) how Contoso has used the security features across Microsoft 365 Enterprise for identity and access management, threat protection, information protection, and security management.

See also

[Information protection for Microsoft 365 Enterprise](#)

[Deployment guide](#)

[Test lab guides](#)

Summary of Microsoft 365 Enterprise security for the Contoso Corporation

1/8/2019 • 6 minutes to read • [Edit Online](#)

Summary: How Contoso is using the security features across Microsoft 365 Enterprise.

To obtain the sign-off of the deployment of Microsoft 365 Enterprise by the IT security department, a thorough security review was conducted. Here are Contoso's security requirements for the cloud:

- Use the strongest methods of authentication for employee access to cloud resources
- Ensure that PCs and mobile devices connect and access applications in secure ways
- PCs and email are protected from malware
- Permissions on cloud-based digital assets define who can access what and what they can do and are designed for least privilege access
- Sensitive and highly regulated digital assets are labeled, encrypted, and stored in secure locations
- Highly regulated digital assets are protected with permissions
- IT security can monitor security posture from central dashboards and get notified of security events for quick response and mitigation

Contoso's path to Microsoft 365 security readiness

Contoso used the following steps to ready their security for their deployment of Microsoft 365 Enterprise:

1. Limited administrator accounts for the cloud

Contoso did an extensive review of the existing Windows Server AD administrator accounts and set up a series of cloud administrator accounts and groups.

2. Performed data classification analysis into three levels

Contoso performed a careful review and determined the three levels, which was used to determine the Microsoft 365 Enterprise features to protect Contoso's most valuable data.

3. Determined access, retention, and information protection policies for data levels

Based on the data levels, Contoso determined detailed requirements, which will be used to qualify future IT workloads being moved to the cloud.

In accordance with security best practices and Microsoft 365 Enterprise deployment requirements, Contoso's security administrators and IT department have deployed many security features and capabilities, as described in the following sections.

Identity & access management

- Dedicated global administrator accounts with MFA and PIM

Rather than assign the global admin role to everyday user accounts, Contoso created three, dedicated global administrator accounts with very strong passwords and protected them with multi-factor authentication (MFA) and Azure AD Privileged Identity Management (PIM).

Signing in with a global administrator account is only done for specific administrative tasks, the passwords are only known to designated staff, and can only be used within the time configured with Azure AD PIM.

Contoso's security administrators have assigned lesser admin roles to accounts that are appropriate to that IT person's job function and responsibility.

For more information, see [About Office 365 admin roles](#).

- MFA for all user accounts

MFA adds an additional layer of protection to the sign-in process by requiring users to acknowledge a phone call, text message, or an app notification on their smart phone after correctly entering their password. With MFA, Azure AD user accounts are protected against unauthorized sign-in even if an account password is compromised.

- To protect against a compromise of the Microsoft 365 subscription, Contoso requires MFA on all global administrator accounts.
- To protect against phishing attacks, in which an attacker compromises the credentials of a trusted person in the organization and sends malicious emails, Contoso enabled MFA on all user accounts, including manager and executive staff.

- Safer device and application access with conditional access policies

Contoso is using [conditional access policies](#) for identity, devices, Exchange Online, and SharePoint Online. Identity conditional access policies include requiring password changes for high-risk users and blocking clients from using apps that don't support modern authentication. Device conditional policies include the definition of approved apps and requiring compliant PCs and mobile devices. Exchange Online conditional access policies include blocking ActiveSync clients and setting up Office 365 message encryption. SharePoint Online conditional access policies include additional protection for sensitive and highly regulated sites.

- Windows Hello for Business

Contoso has deployed and requires [Windows Hello for Business](#) to eventually eliminate the need for passwords with strong two-factor authentication on PCs and mobile devices running Windows 10 Enterprise.

- Windows Defender Credential Guard

To block targeted attacks and malware running in the operating system with administrative privileges, Contoso has enabled [Windows Defender Credential Guard](#) through Windows Server AD group policy.

Threat protection

- Protection from malware with Windows Defender Antivirus

Contoso is using [Windows Defender Antivirus](#) for malware protection and anti-malware management for PCs and devices running Windows 10 Enterprise.

- Secure email flow and mailbox audit logging with Office 365 Advanced Threat Protection

Contoso is using Exchange Online Protection and [Office 365 Advanced Threat Protection \(ATP\)](#) to protect against unknown malware, viruses, and malicious URLs transmitted through emails.

Contoso has also enabled mailbox audit logging to determine who has logged into user mailboxes, sent messages, and other activities performed by the mailbox owner, a delegated user, or an administrator.

- Attack monitoring and prevention with Office 365 Threat Intelligence

Contoso uses [Office 365 Threat Intelligence](#) to protect their Office 365 users by making it easy to identify and address attacks, and to prevent future attacks.

- Protection from sophisticated attacks with Advanced Threat Analytics

Contoso is using [Advanced Threat Analytics \(ATA\)](#) to protect itself from advanced targeted attacks. ATA automatically analyzes, learns, and identifies normal and abnormal entity (user, devices, and resources) behavior.

Information protection

- Protect sensitive and highly regulated digital assets with Azure Information Protection

Contoso determined three levels of data protection and deployed [Azure Information Protection](#) labels that users apply to digital assets. For its trade secrets and other intellectual property, Contoso uses Azure Information Protection sub-labels in a scoped policy for highly regulated data that encrypts content and restricts access to specific security groups.

- Prevent intranet data leaks with Office 365 Data Loss Prevention

Contoso has configured [Data Loss Prevention](#) policies for Exchange Online, SharePoint Online, and OneDrive for Business to prevent users from accidentally or intentionally sharing sensitive data.

- Prevent device data leaks Windows Information Protection

Contoso is using [Windows Information Protection \(WIP\)](#) to protect against data leakage through Internet-based apps and services and enterprise apps and data on enterprise-owned devices and personal devices that employees bring to work.

- Cloud monitoring with Microsoft Cloud App Security

Contoso is using [Microsoft Cloud App Security](#) to map their cloud environment, monitor its usage, and detect security events and incidents.

- Office 365 security monitoring with Office 365 Cloud App Security

Contoso security administrators set up alerts with [Office 365 Cloud App Security \(CAS\)](#) to be notified of unusual or risky user activity, such as downloading large amounts of data from SharePoint Online or OneDrive for Business, multiple failed sign-in attempts, or sign-ins from unknown or dangerous IP addresses.

- Device management with Microsoft Intune

As part of the Enterprise Management + Security (EMS) suite, Contoso uses [Microsoft Intune](#) to enroll, manage, and configure access to mobile devices and the apps that run on them. Device-based conditional access policies also require approved apps and compliant PCs and mobile devices.

Security management

- Central security dashboard for IT with Azure Security Center

Contoso uses the [Azure Security Center](#) for a unified view of security and threat protection, to manage security policies across its workloads, and to respond to cyberattacks.

- Central security dashboard for users with Windows Defender Security Center

Contoso has deployed the [Windows Defender Security Center app](#) to its PCs and devices running Windows 10 Enterprise so that users can see their security posture at a glance and take action.

Next step

[Learn](#) how Contoso created a SharePoint Online site for highly regulated data to enable collaboration among its research teams.

SharePoint Online site for highly confidential digital assets of the Contoso Corporation

1/24/2019 • 3 minutes to read • [Edit Online](#)

Summary: How Contoso implemented a SharePoint Online site for highly regulated data for easier collaboration between its research teams.

Contoso's most valuable assets are its intellectual property in the form of trade secrets, such as proprietary manufacturing techniques, and design specifications for products that are in development. These assets are in digital form, originally stored as files on a SharePoint Server 2016 site. When Contoso deployed Microsoft 365 Enterprise, they wanted to transition their on-premises digital assets to the cloud for easier access and more open collaboration across research teams in Paris, Moscow, New York, Beijing, and Bangalore.

However, due to their sensitive nature, access to these files must be:

- Restricted to the set of people who are allowed to view or change them, with ongoing permissions for the site administered only by SharePoint admins.
- Protected with Data Loss Prevention (DLP) to prevent users from distributing them outside the site.
- Encrypted and protected with access control lists to prevent unauthorized users from accessing their contents, even if they are distributed outside the site.

Security and SharePoint administrators in Contoso's IT department decided to use a [SharePoint Online site for highly regulated data](#).

Contoso used these steps to create and secure a SharePoint Online team sites for their research teams.

Step 1: Reviewed and verified the members of research team groups

Contoso IT admins performed a review of the set of security groups for their research teams. They removed anyone who was not a researcher or did not need access to research assets.

They also and created these new security groups:

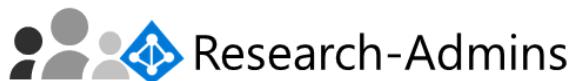
- **Research-Admins** The set of SharePoint admins that have full control over the site, including the ability to modify permissions.
- **Research Members** The set of security groups for the research teams around the world.
- **Research-Viewers** The set of management users, such as executives in the research organization, that can view the assets on the site.

Step 2: Created an isolated SharePoint Online team site

Contoso SharePoint admins first created a new team site named **Research**. They then configured:

- The Full Control permission level to use the Research Owners SharePoint group, which has the **Research-Admins** security group as a member
- The Edit permission level to use the Research Members SharePoint group, which has the **Research Members** security group as a member
- The Read permission level to use the Research Visitors SharePoint group, which has the **Research-Viewers** security group as a member

Here are the resulting SharePoint permission levels, SharePoint groups, and their members.



• • •



Next, they configured additional restrictions for the site.

For the configuration details, see [Deploy an isolated SharePoint Online team site](#).

Step 3: Configured the site for a restrictive DLP policy

First, Contoso admins applied the **Highly Confidential** Office 365 retention label to the **Research** site.

Next, they created a new Office 365 DLP policy named **Research** that:

- Uses the **Highly Confidential** Office 365 retention label.
- Is applied to the **Research** site.
- Prevents users from sharing documents.

For the configuration details, see [Protect SharePoint Online files with Office 365 labels and DLP](#).

Step 4: Created an Azure Information Protection sub-label for the site

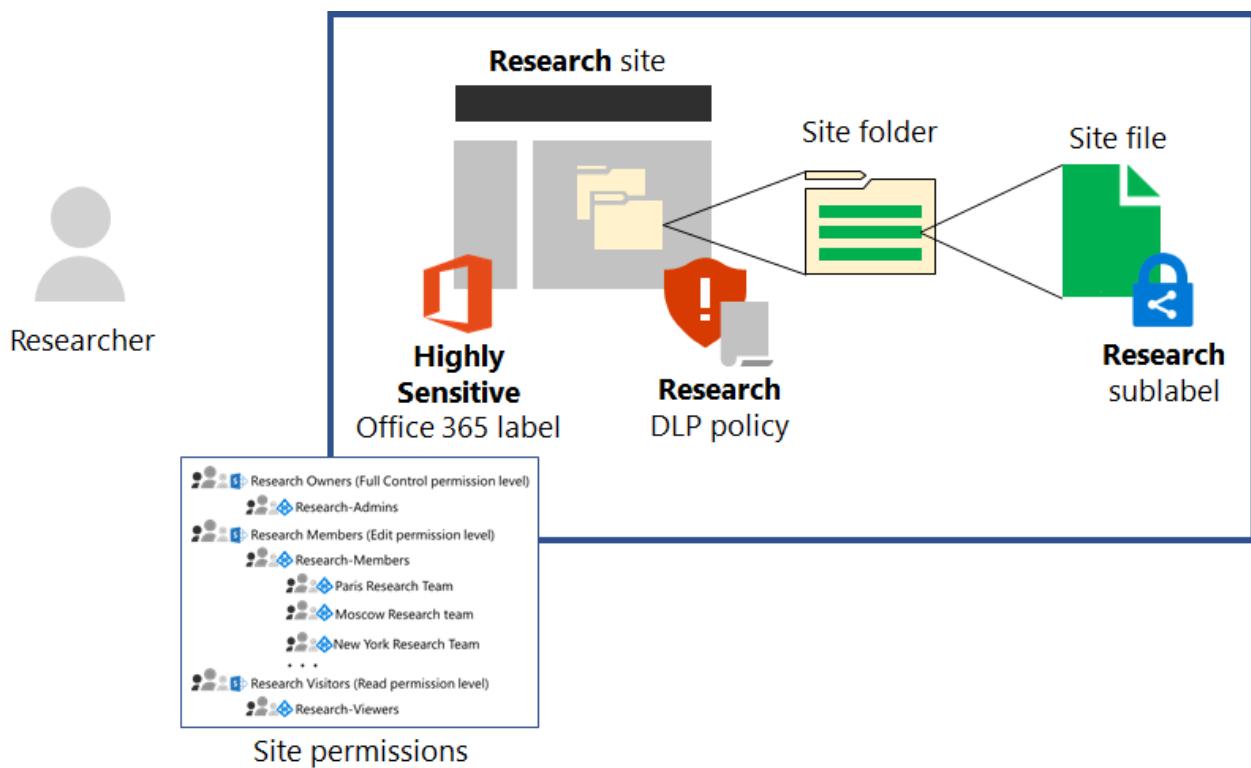
Contoso admins created a new Azure Information Protection sub-label named **Research** of the default **Highly Confidential** label in a scoped policy that:

- Requires encryption.
- Allows full access by members of the **Research Members** security group.
- Allows read access by members of the **Research Viewers** security group.

Next, they deployed the Azure Information Protection client to the devices of research team members.

For the configuration details, see [Protect SharePoint Online files with Azure Information Protection](#).

Here is the resulting configuration of the **Research** site for highly confidential assets.



Step 5: Migrated the on-premises SharePoint research data

Contoso admins moved all of the on-premises research files in the on-premises SharePoint Server 2016 site to folders in the new **Research** SharePoint Online site.

Step 6: Trained their users

Contoso security staff trained the research teams in a mandatory course that stepped them through:

- How to access the new **Research** SharePoint Online site and its existing files.
- How to create new files on the site and upload new files stored locally.
- A demonstration of how the DLP policy blocks files from being shared externally.
- How to use the Azure Information Protection client to label research files with the **Research** sub-label.
- A demonstration of how the **Research** sub-label protects a file even when it is leaked from the site.

The end result is a secure environment in which the researchers can collaborate across the organization in a secure environment.

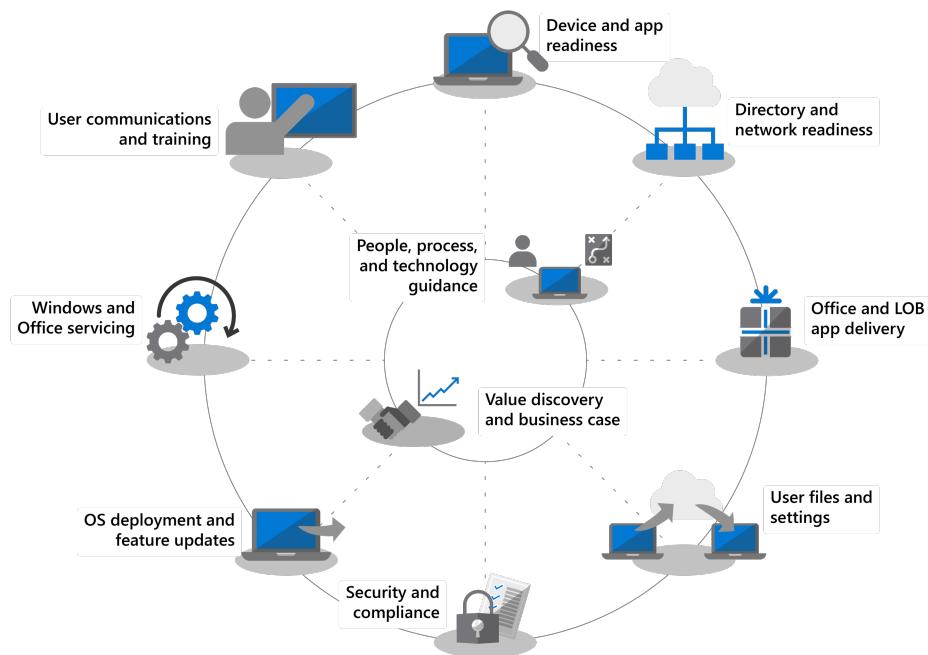
If a research document with the **Research** sub-label is leaked from the **Research** site, it is encrypted and accessible only to members of the **Research Members** and **Research Viewers** security groups with valid credentials.

Next step

[Deploy Microsoft 365 Enterprise in your organization.](#)

Modern Desktop Deployment Center

1/18/2019 • 2 minutes to read • [Edit Online](#)



Follow the steps below to plan and carry out your large-scale deployment of Windows 10 and Office 365 ProPlus. Each step below is part of the overall planning and deployment process with steps typically running in parallel to each other in a phased deployment. Download the free [Modern Desktop Deployment and Management Lab Kit](#) for hands-on training with the tools highlighted in the deployment process. You can also [find help](#) for your modern desktop deployment from Microsoft partners and FastTrack services.

	<h3>Getting Started: People, Process and Technology Guidance</h3> <p>Discover the benefits of a modern desktop, major changes and considerations versus previous deployments, and best practices to ensure a smooth transition to Windows 10 and Office 365 ProPlus.</p>	 <p>Modern Desktop Deployment Intro Aligning the people, process and technology to move to a modern desktop</p>
	<h3>Step 1: Device and App Readiness</h3> <p>Begin your desktop deployment project with an inventory of your devices and apps, prioritize what you need to move forward, test prioritized apps and devices, then remediate what's needed to get ready for deployment.</p>	 <p>Device & App Readiness Collecting data for compatibility and make data-driven decisions for upgrades</p>



Step 2: Directory and Network Readiness

Cloud connected services in Office 365 ProPlus and new deployment options like Windows Autopilot require Azure Active Directory. Your network and connectivity are also important areas to plan when moving Windows images, apps, drivers and related files to your PCs. Learn how new tools and deployment options reduce and streamline network traffic.

Directory & Network Readiness
Networking and bandwidth optimizations + implementing Azure AD



Step 3: Office and LOB App Delivery

Ensure your apps are packaged and ready for automated installation. Learn how Click-to-Run packaging with Office 365 ProPlus gives you new options to configure, deliver, and keep your Office apps up-to-date.

Office & LOB App Delivery
Click-to-Run and app configuration for automated distribution



Step 4: User Files and Settings

When refreshing or replacing PCs, save time by automating user state backup and restore. New options for cloud file sync allow you to enforce per user sync of Desktop, Documents, and Pictures folders to OneDrive for seamless file access from new Windows installs.

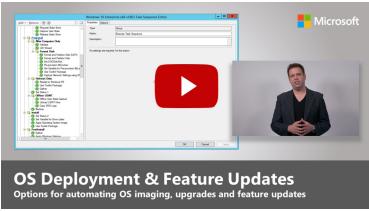
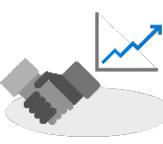
User Files & Settings
Options to move your files between PCs and sync them to the cloud



Step 5: Security and Compliance Considerations

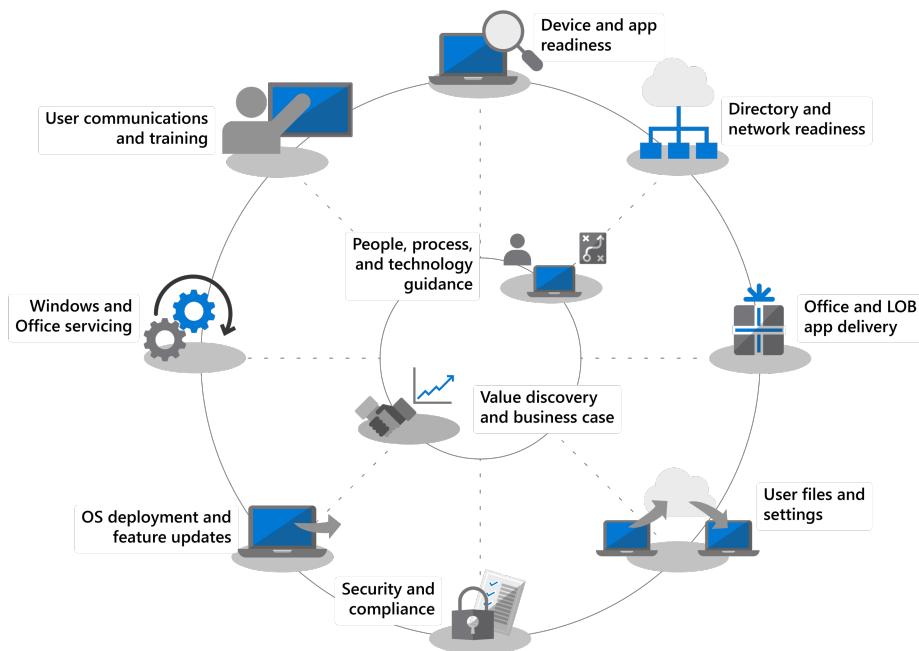
Windows 10 and Office 365 ProPlus provide new ways to protect your data, devices and users, and quickly detect and respond to threats. Also, learn how to deal with common problems associated with disk encryption, anti-malware apps, and policies when moving to Windows 10.

Security & Compliance
Assessing current security and compliance solutions + modern capabilities

	<h3>Step 6: OS Deployment and Feature Updates</h3> <p>Task sequence-based deployment is used to automate large scale, phased deployment for bare metal installs, PC refresh, and PC replacement. Upgrade task sequences will also help you stay current with major semi-annual updates. Windows Autopilot is a recent addition that modernizes imaging new and existing devices.</p>	 <p>OS Deployment & Feature Updates Options for automating OS imaging, upgrades and feature updates</p>
	<h3>Step 7: Windows and Office Servicing</h3> <p>Both Windows 10 and Office 365 ProPlus continually add new capabilities to keep bringing user experiences and security forward with the latest innovations. Learn how to stay current with semi-annual and monthly updates, how the new servicing model works, and the tools and options you have.</p>	 <p>Windows & Office-as-a-Service Options for delivering semi-annual updates</p>
	<h3>Step 8: User Communication and Training</h3> <p>Make sure your users are informed about new experiences and new ways of working as you shift your PCs to Windows 10 and Office 365 ProPlus. Learn how to take advantage of user adoption assistance with Microsoft FastTrack, training materials and communication templates, as well as new ways to monitor user acceptance and usage.</p>	 <p>User Comms & Training Planning your deployment and preparing users for change</p>
	<h3>Get your Leadership on Board: Value Discovery and Business Case</h3> <p>If you've done your deployment research, assessed app and device readiness, built your deployment plan and started piloting your deployment, but don't have the support or resources needed from your management team to meet your deployment timelines, the Business Value Programs at Microsoft can help. Learn how to build a business case for a modern desktop and help get everyone on board.</p>	 <p>Value Discovery & Business Case Why shift to a modern desktop, including benefits and business case</p>

Getting Started - Modern Desktop Deployment

1/18/2019 • 9 minutes to read • [Edit Online](#)



Getting Started: People, Process and Technology Guidance

Discover the benefits of a modern desktop, major changes and considerations versus previous deployments, and best practices to ensure a smooth transition to Windows 10 and Office 365 ProPlus.



Modern Desktop Deployment Intro
Aligning the people, process and technology to move to a modern desktop

NOTE

In this series we will explain the best ways to use existing tools and introduce you to new technologies, services, and methods enabled by the Cloud. To see the full desktop deployment process, visit the [Modern Desktop Deployment Center](#).

Welcome to the Modern Desktop Deployment Center, our central place to learn how to help you plan and make the shift to the modern desktop. This will allow you to take advantage of a secure workspace, powered by the latest productivity, teamwork, and collaboration experiences.

If you haven't deployed a new desktop environment for a while, the good news is much about the deployment process has improved. Challenges of the past, such as application compatibility, are much less of an issue today. New tools, as well as insight delivered from the Cloud, enable you to move forward with confidence faster and more efficiently than ever before.

In this introduction we'll outline what has changed and go on a tour of the Desktop Deployment Wheel. This will guide you through the recommended steps for your shift to Windows 10 and Office 365 ProPlus, detailing how to leverage your existing tools and processes while adopting modern management technology and approaches along

the way.

Why upgrade?

In combination, Windows 10 and the Microsoft Intelligence Cloud enhance your ability to deliver the most empowering and secure workspace for your users while allowing you to simplify your supporting infrastructure.

One of the key tenants of modern management practices is devices that are always up-to-date. Through this series you will read about new capabilities that are being delivered to help you move to Windows 10 and Office 365 ProPlus while staying current with the semi-annual releases of both.

[Windows 10 for the IT Pro](#)

What has Changed

Let's start by taking a look at what has changed and improved since your last desktop deployment. If you haven't shifted your desktop environment in a while you're likely using Windows 7 and Office 2010 or Office 2013. If you are, you'll notice a few things have evolved since your last major upgrade. Here are some of the core changes:

Identity and Access Management The modern desktop, with its connectivity to cloud productivity, security, and management services, has a new Identity and Access Management service at its core: Azure Active Directory. This enables single sign-on and secure connectivity across your cloud services, meaning that you are going to need Azure AD in place. This will allow you take advantage of Microsoft 365 services such as Office 365, Intune, or Windows Autopilot.

[Microsoft 365](#)

Secure Pre-Boot Environment 64-bit UEFI firmware replaces BIOS. This not only speeds up boot times, it is required to enable many of the modern security capabilities in Windows 10. While Windows 10 will run on BIOS, UEFI is strongly recommended. If you have not switched from BIOS to UEFI and 64-bit, now is the time. There are tools to help you make this switch either during a Windows 10 upgrade, or after it.

[Convert from BIOS to UEFI with MBR2GPT](#)

Cloud-based device Management Services like Microsoft Intune help you manage your Windows 10 devices as you do other mobile devices, all from one place. What makes Microsoft Intune unique is the ability to co-manage your Windows 10 devices with System Center Configuration Manager. You can use System Center Configuration Manager to help you in your shift to Windows 10, and then add Microsoft Intune. Working together, System Center Configuration Manager becomes the intelligent edge within your organization, connected to the Microsoft intelligent cloud. This allows you to manage your users' devices securely wherever they are, whether connected on your organization's infrastructure or in the public cloud.

[Co-management for Windows 10 devices](#)

Cloud-based Deployment Service As you acquire new PCs we've introduced a new cloud service to help you deploy Microsoft 365 devices called the Windows Autopilot deployment service. Autopilot is integrated with your hardware providers and new PCs are automatically registered in Autopilot enabling the new PC to be shipped directly to the end-user. When the PC is powered on the first time it is quickly configured to your organization's desired configuration and customized for the specific needs of the user.

[Windows Autopilot](#)

Click-to-Run Deployments When provisioning Office desktop apps, Office 365 ProPlus is the preferred option. This gives you access to the newest innovations in Office as they are developed, so you won't need to wait years before getting new capabilities. You'll also use a new installation called Click-to-Run.

Click-to-Run is quite different from the MSI-based packages of the past. Click-to-Run is faster, lighter, and supports updates in the background to keep your users to be up and running. It is still a local copy of Office and you can

continue to use your existing deployment tools, like System Center Configuration Manager, to provision and configure the apps.

[Deployment guide for Office 365 ProPlus](#)

Semi-Annual Updates Once you have moved to Windows 10 and Office 365 ProPlus, updates are delivered semi-annually with new features. But with Microsoft able to deliver insights from the cloud to help, you can quickly and confidently roll out these updates to hundreds or thousands of devices. Like an in-place upgrade, the Feature Update preserves apps, data, and configurations from the previous release.

The Deployment Process Wheel

Before you get started, you'll want to create a high-level plan and get the necessary sponsors on board. Our deployment process wheel outlines critical steps to help you to identify core team members and resources to manage in the following deployment areas.

Step 1: Device and App readiness For a successful deployment you must first know what you have. That means taking an inventory of your devices and apps and verifying compatibility.

To help with this you can leverage the tools available in our cloud-based service, Windows Analytics. Windows Analytics allows you tap into compatibility intelligence and telemetry gathered from hundreds of millions of PCs, to assess the apps and drivers running on your device so you can establish the readiness of your desktop estate. You can even export a list of "PCs ready for deployment" from Windows Analytics to System Center Configuration Manager if you use it, allowing you to build data-driven collections of targeted PCs as they become ready.

[Get started with Upgrade Readiness](#)

Step 2: Directory and Network Readiness If you haven't already, you'll want to implement Azure Active Directory for identity and access management next. You will also want to prepare your network for the movement of system images, application packages, user files, and updates across it. That means a large amount of additional data; your network must have the capacity to handle this extra load without impact to the day-to-day work of your organization. We have a range of networking optimizations available from bandwidth throttling and peer-to-peer options to dynamic bandwidth scavenging and differential updating.

[BranchCache vs. Peer Cache](#)

Step 3: Office and Line of Business App Delivery While Windows continues to support MSI-based installations it also now supports newer installations mechanisms, optimized for automated deployment and continuous updates. Office 365 ProPlus and Office 2019 clients use Click-to-Run installation technology. You may want to make a range of UWP apps available, and you may increasingly find yourself deploying third-party apps and in-house developed Line of Business Apps that use the new MSIX-based packaging apps. This step ensures your apps are ready for automated deployments, and that you are set up for success whether your apps deploy using Click-to-Run, MSIX, conventional MSI-based, or are UWP apps deployed from a Microsoft Store from Business you set up.

[MSIX Intro](#)

Step 4: User Files and Settings Migration This is a critical step in any PC replacement or refresh cycle: you have to ensure users' files, data, and settings move successfully and are preserved over the migration. This step covers the options available for manual or automated migrations, including well-known and new options.

As in previous upgrades, the User State Migration Tool continues to be a valuable tool to automate this process and it remains an integral part of migrations orchestrated using System Center Configuration Manager or the Microsoft Deployment Toolkit. But moving all this data at migration can be a timing bottleneck for PC replacement due to the physics involved in transferring sometimes hundreds of gigabytes per PC twice – first from the existing desktop, then back down to the new desktop. A new option enabled by OneDrive is Known Folder Move used to sync user documents, pictures, and desktop files at scale, in the cloud, and ahead of deployment.

Redirect and move Windows known folders to OneDrive

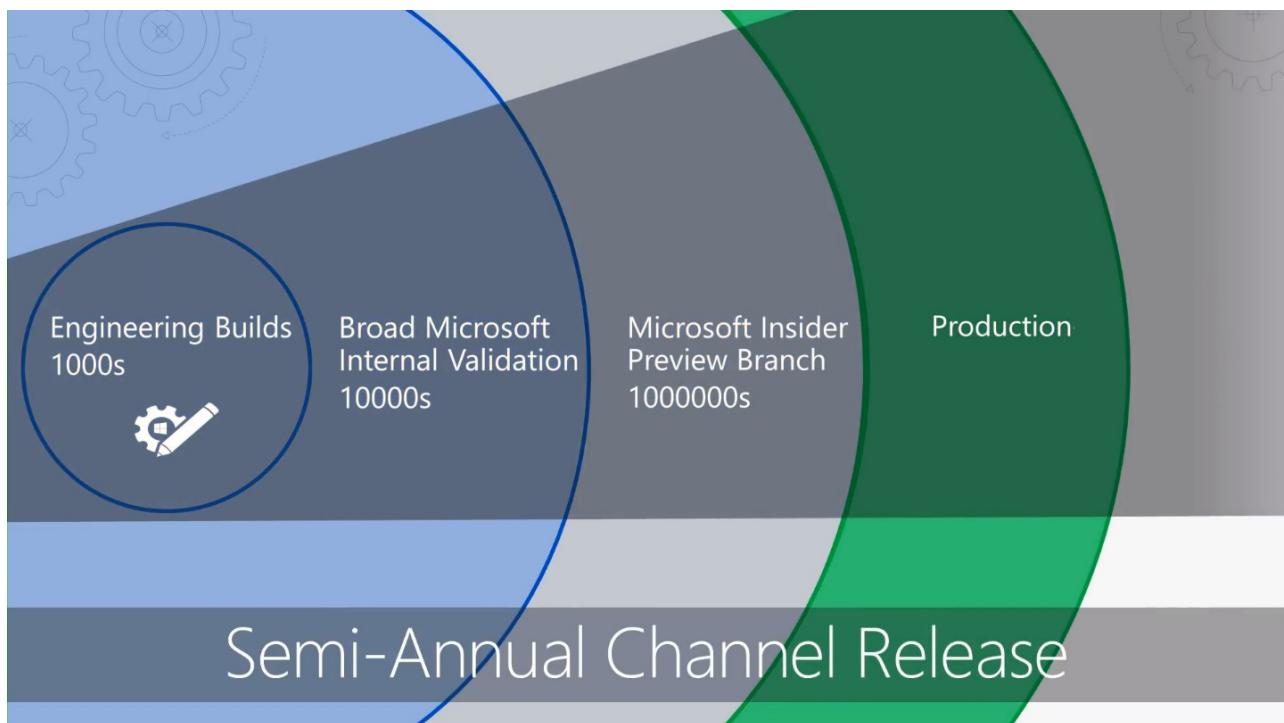
Step 5: Security and Compliance Security and Compliance is an area with a lot upside when moving to Windows 10 and Office 365 ProPlus. It is important you familiarize yourself with the new built-in capabilities and compare that with what you already have. For example, new capabilities in Windows 10 using virtualization-based security can prevent credential theft, protect against browser-based exploits and malicious code execution by isolating core processes and secrets from the operating system. In addition, cloud services like Advanced Threat Protection give you a unified platform for security hardening, post-breach detection, investigation, and response. Advanced Threat Protection can also safeguard you against malicious email attachments, unsafe hyperlinks and more.

[Microsoft Security](#)

Step 6: OS Deployment and Feature Updates With everything prepared, the next step is to deploy the OS images. A lot of the heavy lifting for can be done using System Center Configuration Manager task sequences and infrastructure. The recommended approach is to deploy in phases, first targeting and deploying to an "early adopter group" in your organization using a representative set of hardware and apps. You can then use the data from those devices and users to gradually target more and more PCs.

[Introduction to operating system deployment in System Center Configuration Manager](#)

Step 7: Windows and Office as a Service This represents a major shift in the way you maintain users' desktop real-estate. With this move to Windows 10 and Office 365 ProPlus you can move to managing Windows and Office as a service. In place of a massive shift in technology every few years, you will continually be bringing new capabilities, experiences, and protections to your user. Semi-annual feature updates deliver new capabilities in the Fall and Spring of each year, while monthly cumulative Quality Updates will contain security, reliability, and bug fixes. While you can opt to deploy the Office 2019 client, we strongly recommend you to move to Office 365 ProPlus. This follows a similar service plan to Windows so your users get updates to the Office apps on a regular basis too.



[Overview of Windows as a service](#) [Overview of Office as a service](#)

Step 8: User Communications and Training This last step is critical to driving usage of new capabilities for enhancing teamwork, communications, security, and more. Before broad deployment is targeted to users outside early adopter rings, we recommend you roll out user communication and training. This will help drive desired changes in how people use new capabilities in Office, Windows, or other line of business apps and services. To

assist, we provide free online training via Microsoft FastTrack. Plus, we've published free sample communication plans and timelines together with email, social, and intranet templates to help with your rollout of Windows 10. As a Microsoft 365 or Office 365 organization, your organization may also be eligible for and direct support.

Next Step

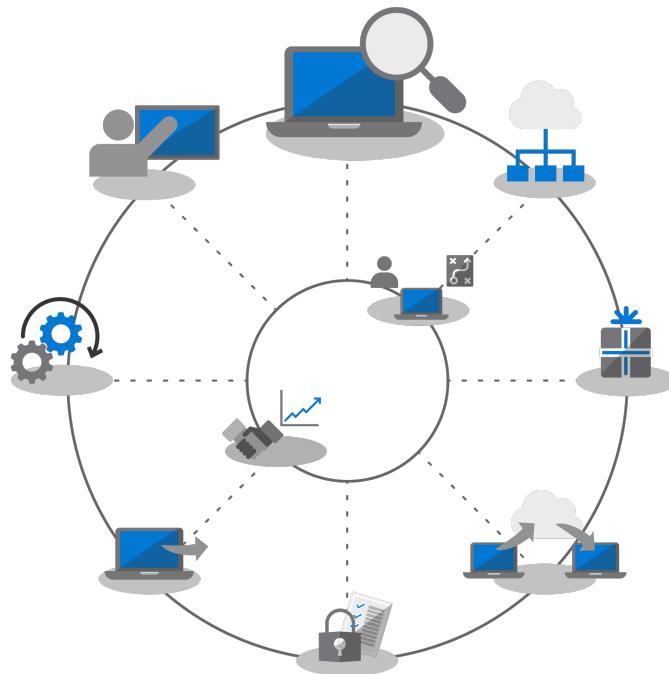
Now you know what's new and different, and we have walked through our recommended deployment process wheel. With this taste for the end-to-end guidance and tools available for you to make the shift a modern desktop, let's get started.

Step 1: Device and App Readiness

Step 1: Device and App Readiness

1/18/2019 • 5 minutes to read • [Edit Online](#)

Begin your desktop deployment project with an inventory of your devices and apps, prioritize what you need to move forward, test prioritized apps and devices, then remediate what's needed to get ready for deployment.



Step 1: Device and App Readiness

Begin your desktop deployment project with an inventory of your devices and apps, prioritize what you need to move forward, test prioritized apps and devices, then remediate what's needed to get ready for deployment.



NOTE

Device and App Readiness is the first step in our recommended deployment process wheel by covering the holistic aspects of application and hardware compatibility. To see the full desktop deployment process, visit the [Modern Desktop Deployment Center](#).

In the past, a major hurdle to upgrading the users' desktops is application and hardware compatibility. The good news as you plan your shift to Windows 10 and Office 365 ProPlus, is just about any application written in the last 10 years will run on Windows 10, and any COM add-ins and VBA macros your organization used on versions of Office dating back to Office 2010, will continue to work on the latest versions of Office, without modification.

That said, depending on the size and age of your organization, verifying application and hardware compatibility is likely still an essential initial step in our recommended 8-phase deployment process.

In this article we take you through that first phase – Device and App Readiness – using Microsoft readiness

assessment tools including the new Windows Analytics Upgrade Readiness tool, an intelligent cloud-based solution available with your Windows license.

Windows 10 Compatibility Scan

Before deploying Windows 10 Microsoft recommends checking the readiness of your existing devices running Windows 7 or 8/8.1. Windows 10 installation media supports a command line switch for the setup.exe to run the upgrade but only check for compatibility, not actually perform the upgrade. ScanOnly can be run as a scripted batch file or integrated into a System Center Configuration Manager task sequence, including the ability to run the ScanOnly directly from the network so the Windows 10 installation media isn't streamed down to the local device. When ScanOnly completes the results are returned via return codes in log files generated by Setup.EXE.

A sample ScanOnly command line that completes the compatibility scan silently would look like the below:

```
Setup.EXE /Auto Upgrade /Quiet /NoReboot /Compat ScanOnly
```

For more information on ScanOnly and other Windows setup command switches please review the [Windows Setup Command-line Options](#).

Recommended Tool: Windows Analytics Upgrade Readiness

Windows Analytics Upgrade Readiness offers many advantages over traditional desktop management systems and is our recommended tool. It is agentless and guides you through what needs to be done making use of application and driver compatibility information gathered through the upgrade of hundreds of millions of consumer PCs. This information gives you a detailed assessment, identifying compatibility issues that might block your upgrade, supported with links to suggested fixes known to Microsoft.

To set up Window Analytics Upgrade Readiness you'll first need to set up an Azure subscription and include an Azure Log Analytics workspace to that. Once you have the Windows Analytics Upgrade Readiness service running, you can then enroll any Internet-connected Windows 7 SP1 or newer device via Group Policy settings - it's that simple. There are no agents to deploy, and Windows Analytics Upgrade Readiness's visual workflow guides you from pilot to production deployment. If you wish, you can export data from Windows Analytics Upgrade Readiness to software deployment tools such as System Center Configuration Manager, to target PCs directly and build collections as they become ready for deployment.

If you don't currently have Windows Analytics set up for your environment or would like to sign up for a trial, go the [Windows Analytics page](#) and get started.

Device and App Readiness Process

Device and App Readiness is comprised of four steps: 1. Inventory, 2. Prioritize, 3. Test, 4. Remediate. Let's look at each of these in turn.

1. Inventory

Windows Analytics Upgrade Readiness service uses an agent-less process to inventory the computers, applications, and Office add-ins across your desktop estate.

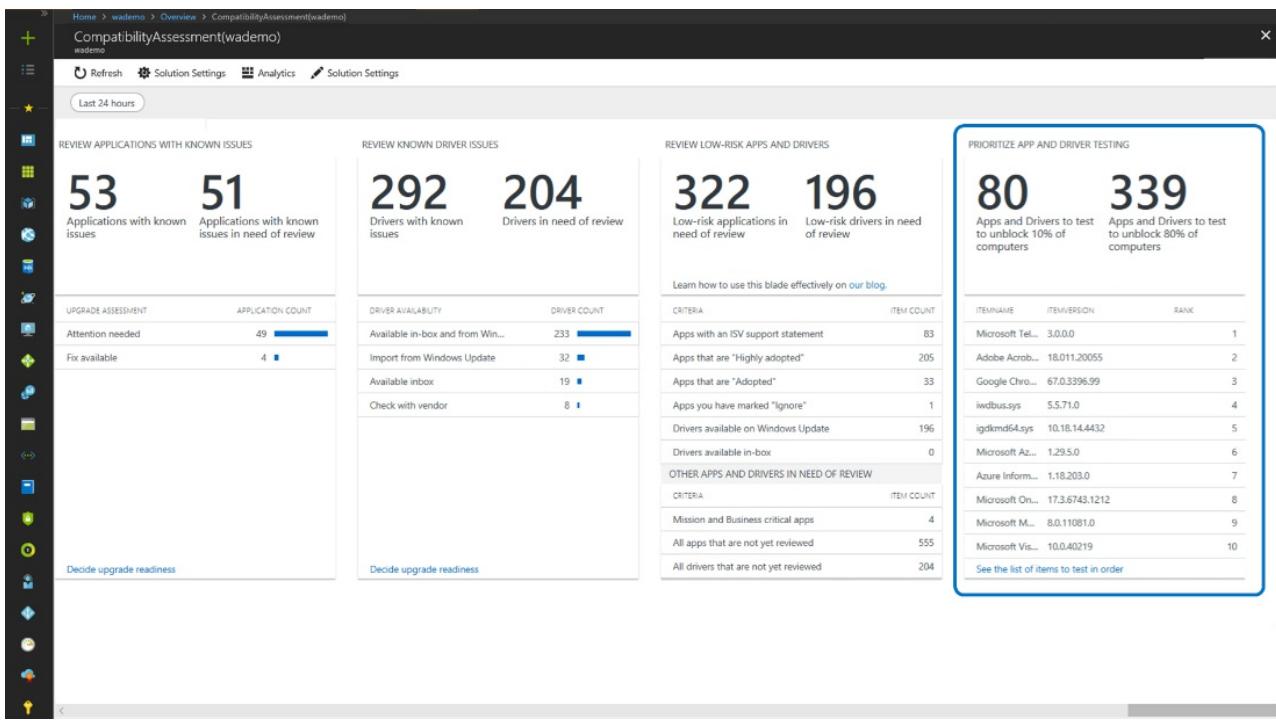
The screenshot shows the Windows Analytics Upgrade Readiness interface. The main title is "STEP 2: Resolve issues". Below it, there are three sections: "Review applications with known issues", "Review drivers with known issues", and "Review low-risk apps and drivers". Each section contains a brief description and a "More info" link. To the left, there's a sidebar titled "PRIORITIZE APPLICATIONS" with a summary of 22k total applications and 561 applications in need of review. It also includes a table for "Importance" and "APPLICATION COUNT" with categories like Low install count, Not reviewed, Review in progress, Business critical, Mission critical, and Ignore. A "Assign importance" button is at the bottom. To the right, there are two more sections: "REVIEW APPLICATIONS WITH KNOWN ISSUES" (53 known issues, 51 need review) and "REVIEW KNOWN DRIVER ISSUES" (292 known issues, 204 need review), each with a "Decide upgrade readiness" button.

It also provides reports on highly visited Internet sites, apps, and Intranet locations to help you with compatibility testing later.

The screenshot shows the "Site discovery" section of the Windows Analytics Upgrade Readiness interface. It includes four main components: "MOST ACTIVE SITES" (38 unique names, 47 unique URLs), "SITE ACTIVITY BY DOCUMENT MODE" (a pie chart showing 971.3K TOTAL visits across IE11 Document Mode (432.4K), IET Document Mode (352.7K), and IEB Enterprise Mode (185.6K)), "LIST OF COMMON BROWSER QUERIES" (a table of top queries like www.youtube.com, www.bing.com, www.google.com, outlook.office.com, etc.), and a "See all..." link. The interface has a similar layout with a sidebar for prioritizing sites and a "Decide upgrade readiness" button.

2. Prioritize

With inventory taken, Windows Analytics Upgrade Readiness helps you to identify and prioritize the most common apps and hardware used in your organization, as well as what to focus on to unblock as many PCs as possible for deployment.



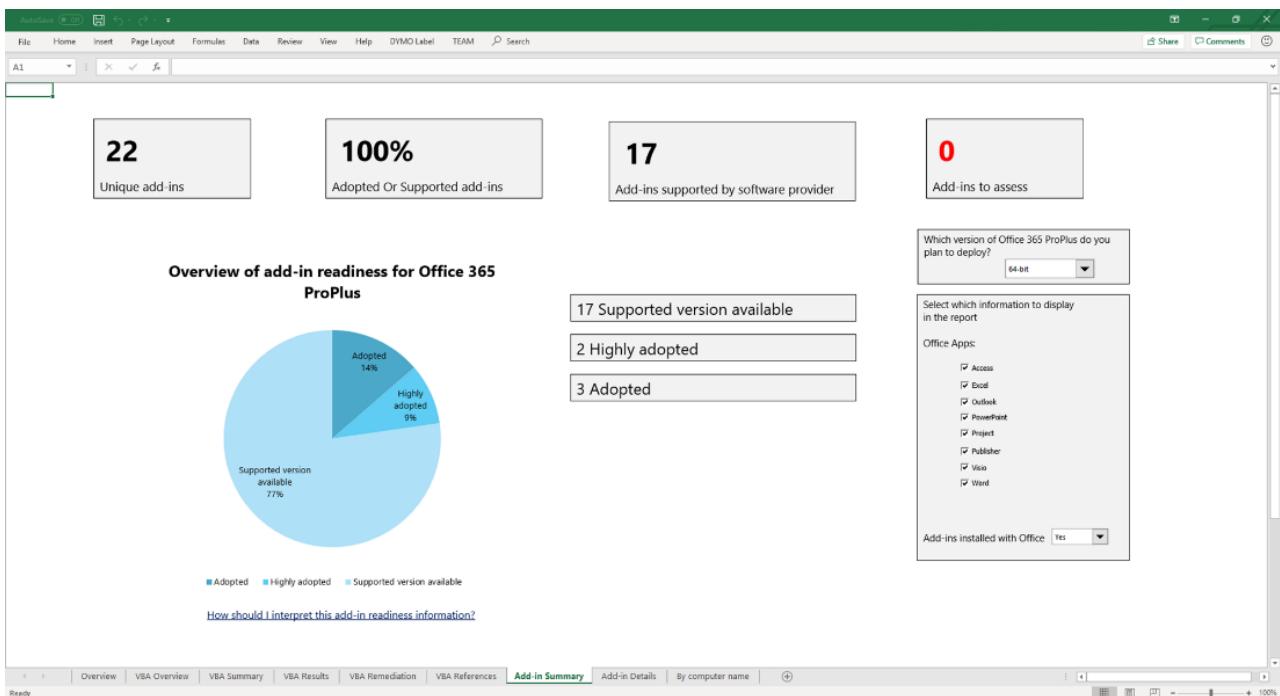
It also provides guidance to help you assess the updates necessary to resolve issues during the next step: testing.

3. Testing

You will find that most of the applications, drivers, and add-ins inventoried will work as-is. For items Windows Analytics Upgrade Readiness assesses to have issues, it provides you with known information including where to find version updates to resolve compatibility problems. Rather than devoting time and resource resolving complex issues in non-critical, sparsely deployed applications and older devices, you may choose instead to work with users to retire and replace these items.

You can use Windows Analytics Upgrade Readiness to assess browser-based compatibility issues too, identifying websites and web apps accessed by users still using ActiveX controls, Browser Helper Objects, VBScript, or other legacy technology not supported by the Microsoft Edge browser. Your users will still need to use Internet Explorer 11 for these sites, and you can add them to the [Enterprise Mode site list](#), using the Enterprise Mode Site List Manager.

Additionally, to assist in your move to Office 365 ProPlus, you may wish to make use of the [Readiness Toolkit for Office](#) to test the compatibility of your add-ins and Microsoft Visual Basic for Applications (VBA) macros.



4. Remediation

The final phase of device and app readiness is to 'remediate'. Here you'll want to collect the required software or driver packages; you are going to use these to supersede or update older versions as part of the deployment process.

STEP 3: Deploy

Deploy Eligible Computers

Now that you've resolved application and driver issues, you're ready to start upgrading computers to Microsoft Windows.

Select the list of computers that are ready to upgrade and export it to your software distribution solution.

Computer Groups

Use the CCM Computer Groups feature to organize your computers according to business area, geographic location, discipline, or any other factors you find relevant.

DEPLOY ELIGIBLE COMPUTERS

UPGRADE DECISION	COMPUTER COUNT
Review in progress	17
Won't upgrade	1
Ready to upgrade	2K

DEPLOY COMPUTERS BY GROUP

GROUP NAME	COMPUTER COUNT
Win 10 Computers	2K
Dell Devices	826
Win 7 Computers	115

As you work through the list remediating issues, you'll see that more and more PCs become "Ready for Deployment". This means that both the drivers and apps on the PCs are noted as compatible with the version of Windows 10 you are targeting for deployment.

Desktop App Assure

Another tool to help with Windows 10 and Office 365 ProPlus app compatibility is the [Desktop App Assure](#) program available through the FastTrack Center. Through Desktop App Assure in the event of valid application issues a Microsoft engineer will work with you at no additional cost to help remediate the application incompatibility.

Continued Use of Telemetry Tools

Windows Analytics Upgrade Readiness isn't just a tool to help you shift to Windows 10 and Office 365 ProPlus. Once you have desktops running on Windows 10 and Office 365 you can use it to help maintain your deployment and manage semi-annual Feature Updates so that you can stay current.

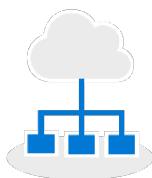
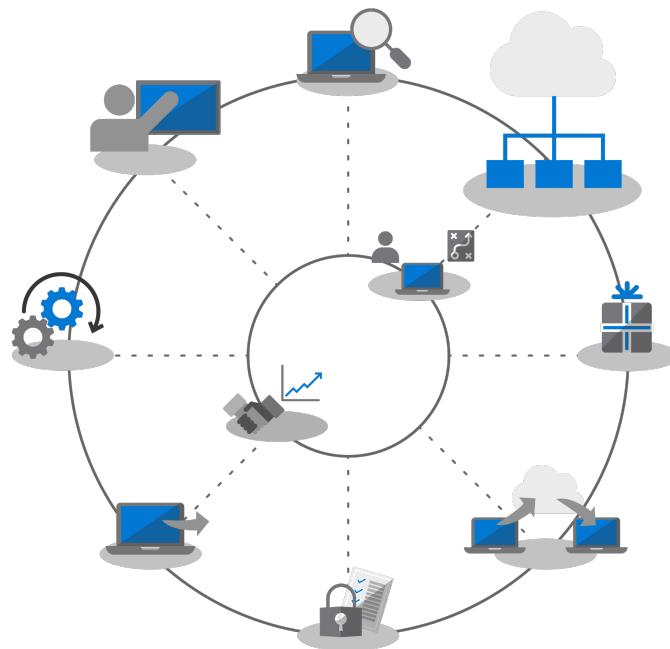
Next Step

Step 2: Directory and Network Readiness

Step 2: Directory and Network Readiness

1/18/2019 • 9 minutes to read • [Edit Online](#)

Ensure your directory and the network are configured and ready to support to your shift to Windows 10 and Office 365 ProPlus. This will require Azure Active Directory Services to be in place for users, and your network must have the capacity to handle both its regular traffic and the movement of potentially vast amounts of data as PCs are upgraded, and users' files, settings and applications are restored.



Step 2: Directory and Network Readiness

Cloud connected services in Office 365 ProPlus and new deployment options like Windows Autopilot require Azure Active Directory. Your network and connectivity are also important areas to plan when moving Windows images, apps, drivers and related files to your PCs. Learn how new tools and deployment options reduce and streamline network traffic.



Directory & Network Readiness
Networking and bandwidth optimizations + implementing Azure AD

NOTE

Directory and Network Readiness is the second step in our recommended deployment process wheel focusing on Azure Active Directory and optimizing the network. To see the full desktop deployment process, visit the [Modern Desktop Deployment Center](#).

Directory and Network readiness is fundamental to ensuring a smooth OS and desktop deployment. As with any automated deployment, it is important to ensure your file shares can be reached, and your network will need to be able to support the transfer of very large files, possibly to hundreds or even thousands of PCs at a time.

With your shift to Windows 10 and Office 365 ProPlus you also now need to make sure that cloud-based identity is set up with Azure Active Directory. This is key not only to activating Office 365 ProPlus, it also allows you to take advantage of modern provisioning solutions like Windows Autopilot.

In this article we'll explore the tools and options to prepare your directory services, and user and device permissions, ready for deployment to Windows 10 and Office 365 ProPlus.

Adding Azure Active Directory

If your organization already uses Office 365, Exchange Online, Microsoft Intune, or other Microsoft Online services, the good news is you are already using Azure Active Directory. If you are, you just need to ensure that the users you are targeting for desktop deployment are in your Azure Active Directory and that licenses have been assigned.

If you are not currently using Azure Active Directory, there are [numerous resources](#) to help you set it up. You may well qualify for personalized assistance via Microsoft FastTrack, as part of your Office 365 license. You can check out more about Microsoft Fastrack [here](#).

Once you have Azure Active Directory in place, your users can sign in to and activate their Office 365 ProPlus apps, and you can use Microsoft Intune or Windows Autopilot deployment for automated deployment of apps and policy.

Network Readiness

You must consider bandwidth requirements when planning your deployments. There are three main components in a deployment that will have an impact on your network – PC imaging, software updates, and user personalization. Between them, this can mean in excess of 20 GB per PC for the initial migration, and often 1 GB or more per month per PC to stay up-to-date.

Let's start by exploring the requirements of each of these three main components:

PC Imaging

For Windows Images with no customization you should plan typically for 3GB per PC, while for customized images with apps you may need to allow 6GB, or more. You may also need to consider Driver packages; these can be a few hundred megabytes per PC, sometimes up to 1GB.

Software Updates

You'll need to plan network bandwidth for software updates. Windows 10 and Office 365 ProPlus use a new servicing model delivering monthly and semi-annual updates. If you are new to this model, you can learn more about how this works [here](#).

The new servicing model includes Feature Updates for Windows twice a year, Office Semi-Annual Channel Updates, and monthly Quality Updates. Feature Updates are typically 2 – 4GB in size, and Office Semi-Annual Channel updates are 300 – 400 MB per update. Then there are the monthly Quality Updates. These may range from a few hundred megabytes to over a gigabyte. This is because monthly updates are cumulative, so these increase in size over the servicing lifetime for each Windows 10 version. That said, there are tools that can help reduce the amount of data that must pass over the network to implement updates. We will cover this in more detail below.

User Personalization

The third component to consider is user personalization. Here you need to plan network bandwidth to accommodate the restoring of user files, their settings, and their applications as part of the PC refresh or replacement process. Together, these items often exceed 20 GB per PC; for some users these may exceed 100 GB.

Limiting Bandwidth

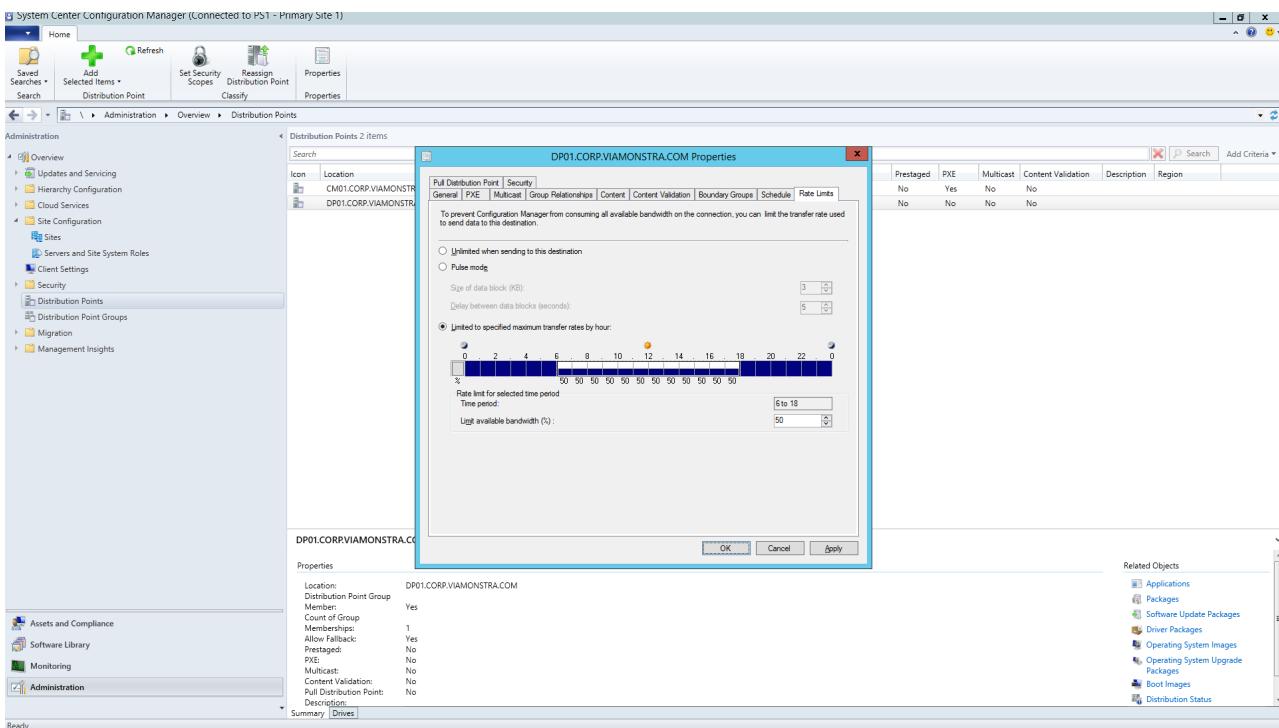
One way to limit the impact of deployment-related traffic on the network is to throttle it using the BITS (Background Intelligent Transfer Service) setting on clients. BITS uses an Adaptive Bit Rate (ABR) to adjust bandwidth available for deployment purposes; it can be configured on clients using Group Policy.

About BITS

If you use System Center Configuration Manager, you can also configure BITS-enabled Distribution Points or enable multicast with WDS.

Throttling specific traffic means that normal network traffic is less impacted by PCs downloading updates and applications. But carving out a certain percentage of bandwidth for these tasks helps ensure productivity isn't impacted by Windows or Office deployment and processes continue to run as needed, it can worsen deployment-related downtime, with users locked out of their PCs while a deployment runs.

Fortunately, there are new tools to make it easier for you to manage the network impact of a large-scale desktop deployment, including LEDBAT to optimize use of available bandwidth, and peer-to-peer (P2P) options to move deployment traffic away from the center of the network and out to the perimeter

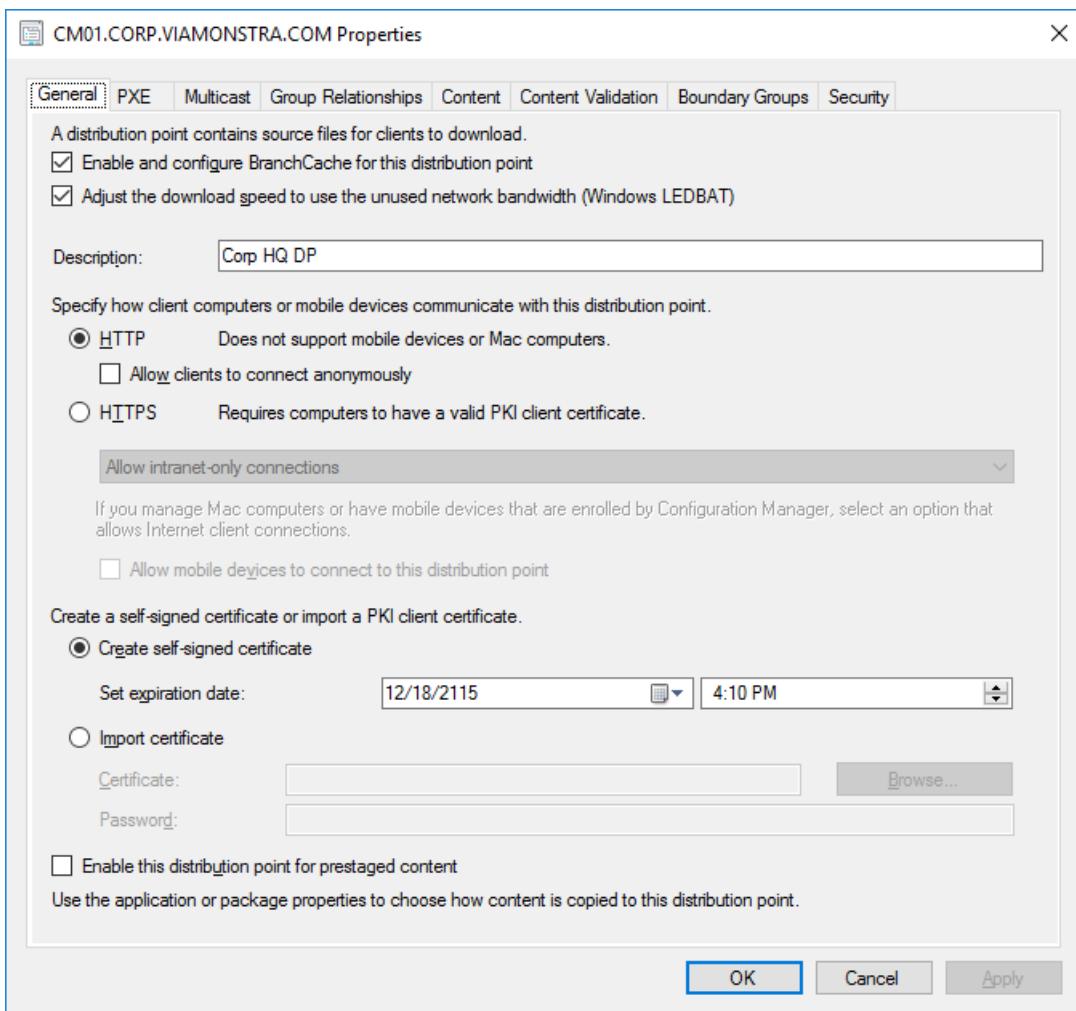


Scavenging Bandwidth

Low Extra Delay Background Transport (LEDBAT), supported in Windows Server 2019 and System Center Configuration Manager version 1806, is designed to optimize network traffic to Windows clients.

Top 10 Networking Features in Windows Server 2019: #9 LEDBAT – Latency Optimized Background Transport

Unlike traditional throttling, LEDBAT can use all available network bandwidth as a background task, instantly yielding bandwidth when other traffic requests it. Unlike BITS there is no delay; everything is automated – no manual tuning or scheduling required, and everything is setup server side. This affords potentially massive performance gains.



Peer-to-Peer options

Peer-to-Peer options are increasingly being used in Windows 10 migrations, for PC imaging, software updates and user personalization. They are also valuable in facilitating build-to-build upgrades after your initial Windows 10 deployment. Here we will cover several examples to help move Windows 10 and Office-related traffic away from the center of the network, reducing the need for classic throttling approaches, and allowing PCs to find the update files they need on peers in their local network rather than downloading them from a distribution point or the internet.

BranchCache can help you download content in distributed environments without saturating the network. It comes in two options: Hosted Cache Mode, which lets you use local servers to cache content, and Distributed Cache Mode (a mode supported in System Center Configuration Manager), which lets clients share already downloaded content with each other.

Peer Cache Clients supported by System Center Configuration Manager can also make use of Peer Cache. This allows PCs that are reliably available on the network to host source for content distribution. You won't want to enable this on all of your PCs – only target devices with reliable network connections as hosts (e.g. desktop, mini-tower, or tower PCs). Peer Cache can even work for deployment tasks running in Windows PE phases during setup.

Note: BranchCache and Peer Cache are complementary and can work together in the same environment.

BranchCache vs. Peer Cache

Delivery Optimization Delivery Optimization is another peer-to-peer caching technology, providing network-based controls for deployments. Windows 10 Delivery Optimization to update built-in UWP apps, also to install applications from the Microsoft Store, and for software updates using Express Updates. It has been available since early versions of Windows 10, though it has only recently integrated with System Center Configuration Manager. Since Windows 10 version 1803 new configuration options mean you can now independently set bandwidth limits

for background updates and foreground jobs such as an app install from the Store. Windows Delivery Optimization now also supports Office 365 ProPlus during client updates, available in all supported Office 365 client update channels. Support for Windows Delivery Optimization during Office 365 client initial installation will be coming soon.

← Settings

Advanced options

By default, we're dynamically optimizing the amount of bandwidth your device uses to both download and upload Windows and app updates, and other Microsoft products. But you can set a specific limit if you're worried about data usage.

Download settings

Limit how much bandwidth is used for downloading updates in the background

45%

Limit how much bandwidth is used for downloading updates in the foreground

90%

Upload settings

Limit how much bandwidth is used for uploading updates to other PCs on the Internet

50%

Monthly upload limit

500 GB

Note: when this limit is reached, your device will stop uploading to other PCs on the Internet.

Monthly upload to date
N/A

Amount left
500.0 GB

Additional Considerations for Office 365 ProPlus

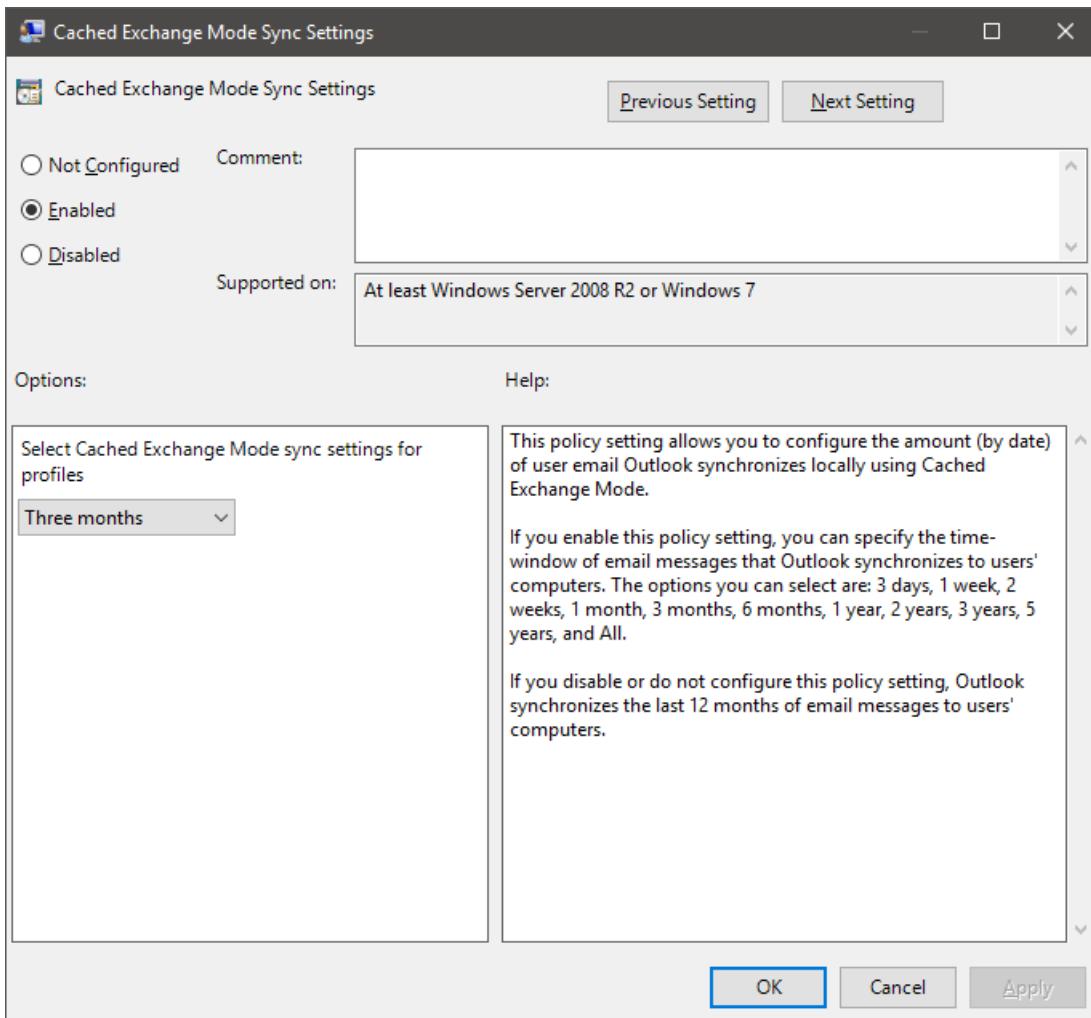
In addition to leveraging Delivery Optimization, here are three items that will help reduce your network load due to Office 365 ProPlus deployments.

Binary Delta Compression Office 365 ProPlus uses Binary Delta Compression to reduce bandwidth consumed by software updates when updating from the most recent release of Office 365 ProPlus to the next release. By only pulling the binary level changes from the previous release, the impact from month-over-month growth of cumulative updates is minimized. This has the potential of saving several hundred megabytes of data, per PC, each month. In order to use this capability though, you cannot skip releases. If you do, then the full cumulative update must be downloaded.

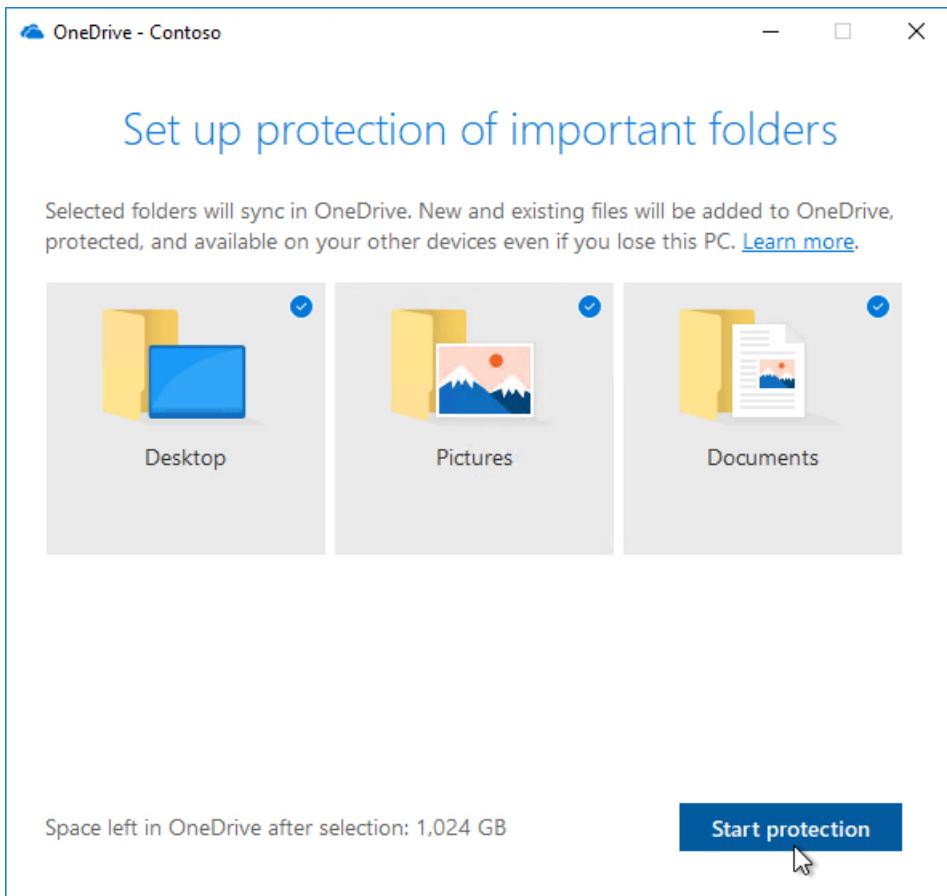
Downloading Updates for Office 365

Outlook Data Files Outlook is often configured to cache users' entire mailbox locally for use offline. In any Windows deployment, except an in-place upgrade, that requires the users' Outlook Data Files to rebuild themselves after the upgrade. This is an automated process, but with Outlook mailbox limits typically set to up to 100GB, re-caching the entire mailbox locally for all users means a lot of data transfer. To reduce the network load you may want to consider using Group Policy to reduce the "Mail to keep offline" setting. In Office 365 ProPlus or

Office 2016 the default value for Outlook is set to 12 months. In order to reduce network impact consider setting the offline cache to last between 1 to 6 months. Changing this setting does not affect the size of the online mailbox, and the entire mailbox can still be searched via Outlook when online.



OneDrive Files on Demand and Known Folder Move OneDrive is a great way to synchronize and protect user files from PCs and other devices in the cloud. With Known Folder Move, you can enforce file sync from a user's Desktop, Documents, and Pictures folders to OneDrive making those files available when signing into a new device or reimaged PC. Remember though, due to the sheer size and number of files kept in Desktop, Documents, and Pictures locations, you'll want to be planful with the rollout of policies enabling and enforcing OneDrive on your PCs. One option is to use Group Policy Network controls to throttle bandwidth used by the OneDrive sync service.



[Setup Known Folder Move](#)

[OneDrive Files on Demand](#)

If you haven't already rolled out OneDrive, the shift from Windows 7 to Windows 10 is a perfect opportunity to enable OneDrive and it integrates seamlessly Office 365 ProPlus. Consider starting this roll-out while working through your app and device readiness. This will give file sync a head start before you start moving Windows images and deploying apps over your network.

Next Step

[Step 3: Office and LOB App Delivery](#)

[Previous Step:](#)

[Step 1: Device and App Readiness](#)

Feedback

We'd love to hear your thoughts. Choose the type you'd like to provide:

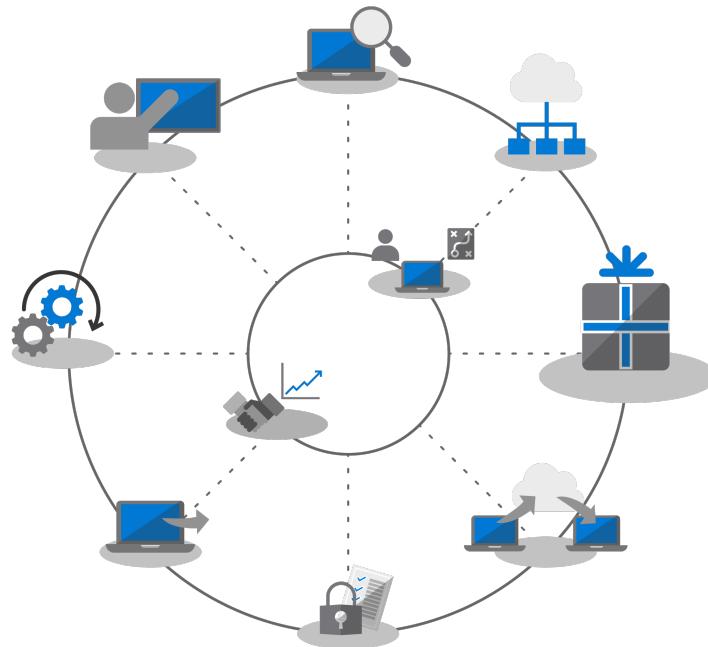
[Product feedback](#) [Sign in to give documentation feedback](#)

Our new feedback system is built on GitHub Issues. Read about this change in our blog post.

Step 3: Office and LOB App Delivery

1/18/2019 • 6 minutes to read • [Edit Online](#)

You are now ready to deliver Office and your Line of Business Apps. There are a number of ways to do this, including some exciting new options. Take some time to review and chose the best methods for your current needs.



Step 3: Office and LOB App Delivery

Ensure your apps are packaged and ready for automated installation. Learn how Click-to-Run packaging with Office 365 ProPlus gives you new options to configure, deliver and keep your Office apps up-to-date.



NOTE

Office and LOB App Delivery is the third step in our recommended deployment process wheel covering the options to install and manage Office and LOB. For successful deployment do not skip the first two steps. To see the full desktop deployment process, visit the [Modern Desktop Deployment Center](#).

While some applications are only available as either a 32-bit or 64-bit compiled version, others such as Office 365 ProPlus, offer both as 32-bit and 64-bit native compiled code, and one of biggest decisions you will make is which version to deploy. To take advantage of additional compute power and RAM on new devices Microsoft recommends using the 64-bit version when there are no 32-bit dependencies. To determine any add-in or file-related compatibility challenges you may have it is recommended to revisit Step 1 Device and App Readiness before you continue.

If nothing is blocking you, we recommend you deploy 64-bit versions of all apps, including Microsoft Office. 64-bit

native compiled apps offer the best performance and is the most future-proof choice.

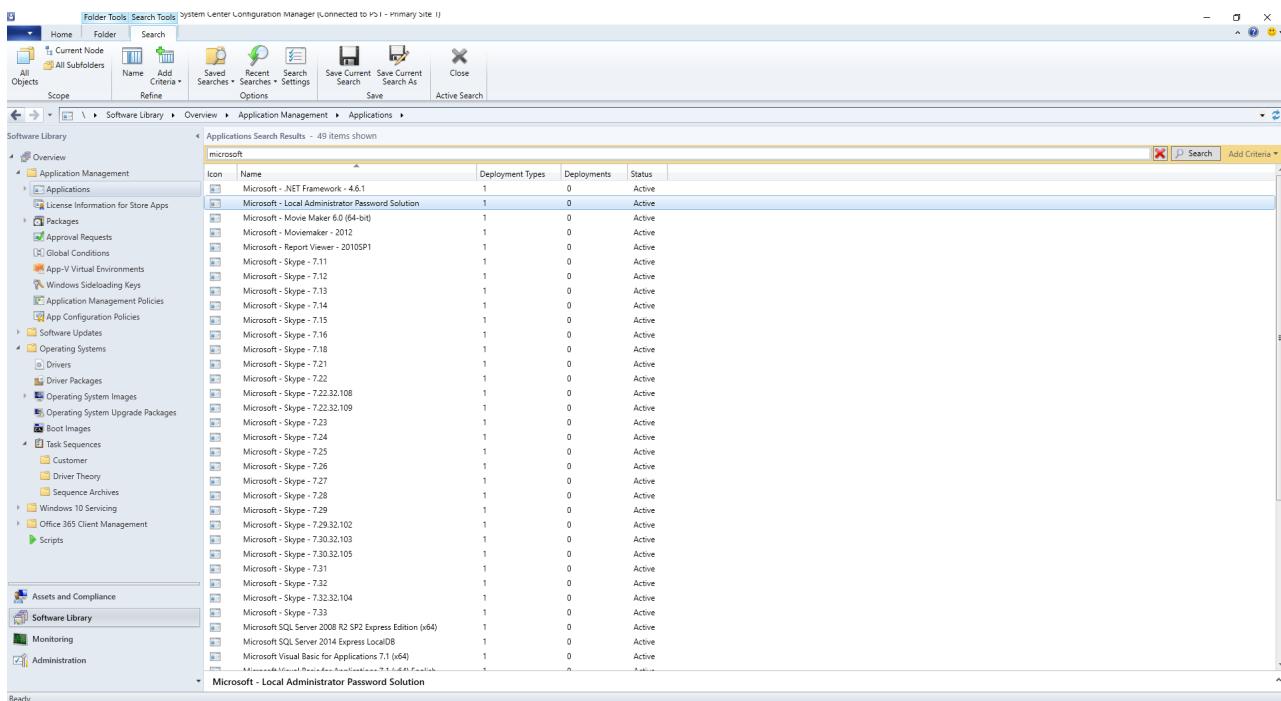
There are many methods and models for installing apps on Windows, so let's look at your delivery options.

Windows 10 application management

MSI-based Deployments

For your line of business apps, you'll probably use MSI-based packages or executable and install apps as part of an OS deployment task sequence. Windows 10 continues to work with these packages.

Software deployment tools like System Center Configuration Manager and Microsoft Intune are also optimized to deliver MSI-packaged apps. Once you have validated your apps on Windows 10, you can use System Center Configuration Manager (current branch) for app delivery. If you use the Company Portal in Microsoft Intune you can extend the choice of IT sanctioned apps available to your organization to include the latest applications, and users to self-select what they need.

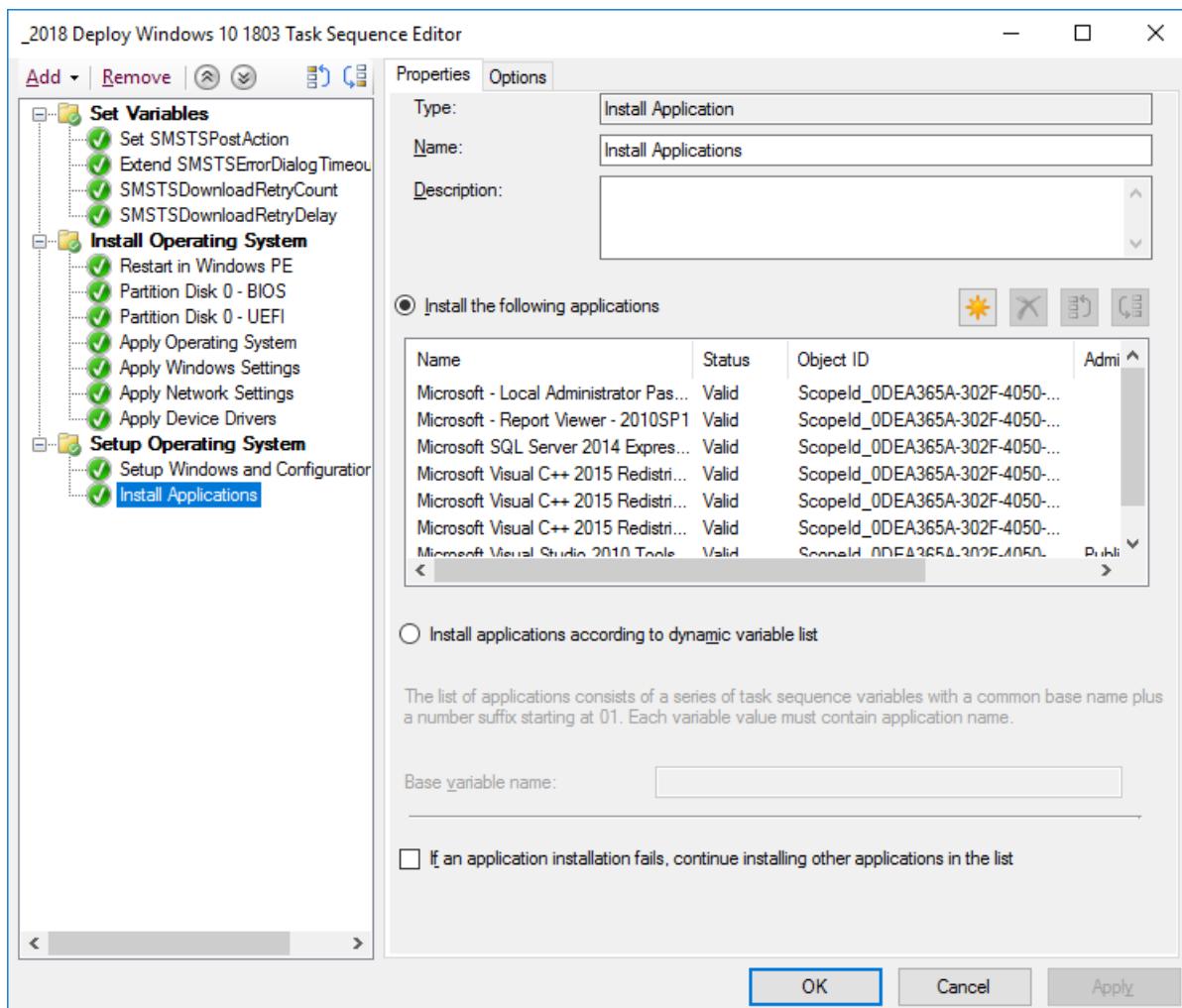


The screenshot shows the System Center Configuration Manager interface. The left navigation pane includes sections for Overview, Application Management (selected), License Information for Store Apps, Packages, Approval Requests, Global Conditions, App-V Virtual Environments, Windows Sideloaded Keys, Application Management Policies, App Configuration Policies, Software Updates, Operating Systems, Task Sequences, Assets and Compliance, Software Library (selected), Monitoring, and Administration. The right pane displays a table titled 'Applications Search Results - 49 items shown' under the 'microsoft' category. The table has columns for Icon, Name, Deployment Types, Deployments, and Status. Most items listed are Skype versions, with one entry for Microsoft - Local Administrator Password Solution and another for Microsoft SQL Server 2008 R2 SP2 Express Edition (x64). All items are marked as Active.

Icon	Name	Deployment Types	Deployments	Status
Microsoft - .NET Framework - 4.6.1	1	0	Active	
Microsoft - Local Administrator Password Solution	1	0	Active	
Microsoft - Movie Maker 6.0 (64-bit)	1	0	Active	
Microsoft - Movemaker - 2012	1	0	Active	
Microsoft - Report Viewer - 2010SP1	1	0	Active	
Microsoft - Skype - 7.11	1	0	Active	
Microsoft - Skype - 7.12	1	0	Active	
Microsoft - Skype - 7.13	1	0	Active	
Microsoft - Skype - 7.14	1	0	Active	
Microsoft - Skype - 7.15	1	0	Active	
Microsoft - Skype - 7.16	1	0	Active	
Microsoft - Skype - 7.18	1	0	Active	
Microsoft - Skype - 7.21	1	0	Active	
Microsoft - Skype - 7.22	1	0	Active	
Microsoft - Skype - 7.22.32.108	1	0	Active	
Microsoft - Skype - 7.22.32.109	1	0	Active	
Microsoft - Skype - 7.23	1	0	Active	
Microsoft - Skype - 7.24	1	0	Active	
Microsoft - Skype - 7.25	1	0	Active	
Microsoft - Skype - 7.26	1	0	Active	
Microsoft - Skype - 7.27	1	0	Active	
Microsoft - Skype - 7.28	1	0	Active	
Microsoft - Skype - 7.29	1	0	Active	
Microsoft - Skype - 7.29.32.102	1	0	Active	
Microsoft - Skype - 7.30.32.103	1	0	Active	
Microsoft - Skype - 7.30.32.105	1	0	Active	
Microsoft - Skype - 7.31	1	0	Active	
Microsoft - Skype - 7.32	1	0	Active	
Microsoft - Skype - 7.32.32.104	1	0	Active	
Microsoft - Skype - 7.33	1	0	Active	
Microsoft SQL Server 2008 R2 SP2 Express Edition (x64)	1	0	Active	
Microsoft SQL Server 2014 Express LocalDB	1	0	Active	
Microsoft Visual Basic for Applications 7.1 (x64)	1	0	Active	

PC Imaging

Another popular method of app delivery is PC imaging. In this case, applications are either installed via task sequence or manually on a sample PC, then a system image is captured with the required applications pre-installed. The imaging approach to build and capture can save time when provisioning new PCs but remember operating systems and apps within the image can become stale quickly. The Cumulative Update model in Windows 10 and Office 365 ProPlus help with this problem, but doesn't eliminate it completely. This is why we recommend a thin image approach, where your applications are installed from outside the image at deploy time.



If you do want to include Office 365 ProPlus in your image, remember that this uses a user-based activation; it cannot be pre-activated by the system admin. Use the Office Deployment Tool to pre-install Office on the device you are imaging and skip the user sign-in. Once the image is deployed end users can sign-in using their Office 365 credentials and activate Office 365 ProPlus.

Create a Task Sequence to Install an Operating System

[Deploy Office 365 ProPlus as part of an operating system image]<https://docs.microsoft.com/en-us/deployoffice/deploy-office-365-proplus-as-part-of-an-operating-system-image>

Office Click-to-Run

Office 365 ProPlus is installed using Click-to-Run, and Click-to-Run replaces MSI-based packaging in every version of the upcoming Office 2019 release for Windows. It brings with it a number of advantages, including faster installations, faster and more efficient updating, and cleaner uninstallation.

Programs delivered via Click-to-Run execute in a virtual application environment on your computer and so co-exist with other applications without conflict; they also take about half the disk space they would as an MSI-based package. Office applications are delivered and managed via the [Office Deployment Tool](#) which is the Office setup engine needed to download, configure, and customize your Office apps. The Office Deployment Tool reads a configuration XML file which provides the metadata instructions on how to configure and customization your Office installation.

Microsoft recommends using the [Office Customization Tool](#) to customize your deployment settings and create your configuration XML file. Through the Office Customization Tool you can set which applications and languages will be installed, how the applications will be updated, application preferences, and installation experience settings.

The screenshot shows the Microsoft Office Customization Tool interface. On the left, under 'Deployment settings', there's a section for 'Products and releases' with tabs for 'Architecture' and 'Products'. Under 'Architecture', the '64-bit' option is selected. Under 'Products', several products are listed in dropdown menus: 'Office Suites' (Office 365 ProPlus), 'Visio' (Visio Professional 2016 - Volume License), 'Project' (Project Professional 2016 - Volume License), and 'Additional Products' (Language Pack). On the right, under 'Configured settings', there are sections for 'General' and 'Products'. In 'General', there are fields for 'Organization name' and 'Description'. In 'Products', a table lists configurations for 'Office 365 ProPlus', including 'Excluded Applications' (OneDrive (Groove), OneNote 2016), 'Visio Professional 2016 - Volume License' (Excluded Applications: OneDrive (Groove)), 'Project Professional 2016 - Volume License' (Language Pack), and 'Architecture' (64-bit).

If you use System Center Configuration Manager, you can still use it for broad deployment of Office 365 ProPlus. System Center Configuration Manager (current branch) has native support for the updated Office Customization Tool, package customization for Click-to-Run at install time, and native support for software update management post installation.

The screenshot shows the System Center Configuration Manager interface. On the left, the 'Software Library' navigation pane is visible with categories like All Objects, Scope, Software Updates, Deployment Packages, and Office 365 Client Management. The 'Office 365 Client Management' node is expanded. On the right, a 'Deployment settings' window is open, titled 'Microsoft Office 365 Client Installation Wizard'. It contains sections for 'Products and releases' and 'Architecture'. Under 'Products and releases', there are dropdown menus for 'Office Suites' (Office 365 ProPlus), 'Visio' (Visio Professional 2019 - Volume License), 'Project' (Project Standard 2016 - Volume License), and 'Additional Products' (Select a suite or product). Under 'Architecture', the '64-bit' option is selected. There are also tabs for 'Application Settings' and 'Office Settings'.

Deployment Guide for Office 365 ProPlus

[Remove existing MSI versions of Office when upgrading to Office 365 ProPlus](#)

[Manage Office 365 ProPlus with Configuration Manager](#)

[Assign Office 365 apps to Windows 10 devices with Microsoft Intune](#)

Browser-based Apps

There are a few things to consider in order to make sure that your browser-based applications continue to work as expected. If you have specific web sites and apps that you know have compatibility problems with Microsoft Edge,

you can use the Enterprise Mode site list so that the web sites will automatically open using Internet Explorer 11.

Additionally, if you know that your intranet sites aren't going to work properly with Microsoft Edge, you can set all intranet sites to open using Internet Explorer 11 automatically. This process uses an XML file to govern whether IE11 is used for each site, using Group Policy to enforce settings.

[What is Enterprise Mode](#)

So far, we have covered well known deployment methods. But there are two new approaches to app deployment you may wish to consider.

Microsoft Store for Business

Microsoft Store for Business provides a flexible way discover, acquire, manage, and distribute free and paid apps to Windows 10 devices at scale. As an IT admin, you can publish selected Microsoft Store apps, along with your custom own apps, to your own private store while assigning and re-using licenses as needed. Your users are directed to this store only, and so can only find and install approved apps.

Store apps can be natively built as UWP apps or you can use the Desktop Bridge to repack your existing apps for the Store and add modern experiences for Windows 10. Aside from the code that you use to light up Windows 10 experiences, your app remains unchanged and continues to run in full-trust user mode.

MSIX Containerization

A new option for application packaging is MSIX. MSIX uses the containerization technology available in Windows, bringing together the best aspects of Click-to-Run, UWP and MSI packaging. With tools to migrate existing installers like EXE, MSI, APPV and APPX directly to MSIX we see MSIX Containerization provides a unified path for the many installation technologies in use today. MSIX support is included in current versions of Windows: any device running Windows 10 RS5 or newer includes everything you need to install and run MSIX packaged apps. Windows 10 dynamically integrates MSIX containers it receives, while keeping the applications separate from the operating system.

Containerization means clean uninstall and removal of packages, unlike a lot of MSI and EXE-based packages today that may leave items on the system. It also means only needing Standard User credentials to install applications – you do not have to have Administrator credentials to install MSIX containers. MSIX containers are more efficient to update too. When an update is published, use of block level differentials means only net new binaries are applied, reducing the update payload, for faster deployments consuming less network bandwidth.

You can find more information on MSIX via the [MSIX Tech Community site](#)

Next Step

[Step 4: User Files and Settings](#)

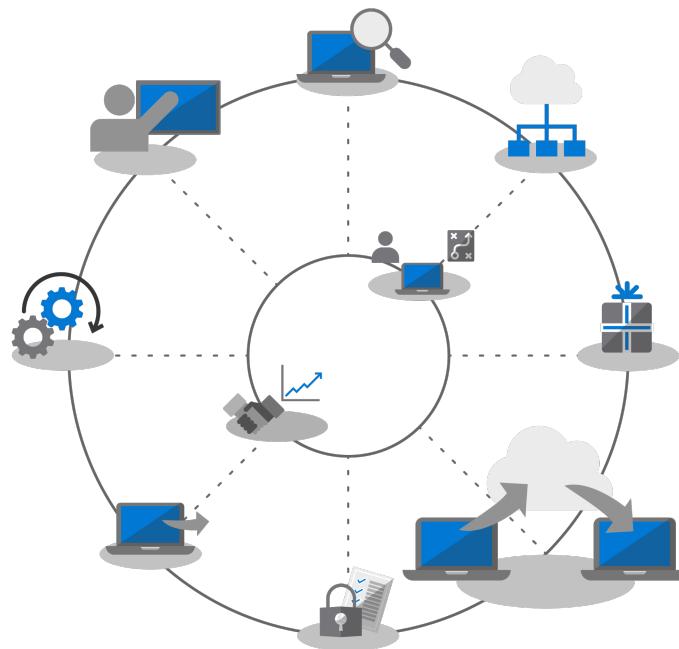
[Previous Step](#)

[Step 2: Directory and Network Readiness](#)

Step 4: User Files and Settings Migration

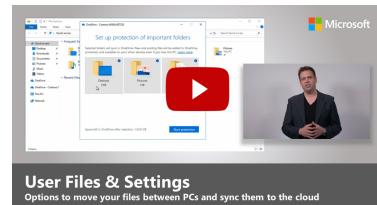
1/17/2019 • 6 minutes to read • [Edit Online](#)

Moving users' files and settings to their new or refreshed PCs is a critical process, failure is not an option. You can migrate each PC manually or you choose one of several ways to automate the process. Whichever migration method you choose there are three main considerations to be addressed – the transfer of users' files, their settings, and managing Windows 10 Start and taskbar layouts.



Step 4: User Files and Settings

When refreshing or replacing PCs, save time by automating user state backup and restore. New options for cloud file sync allow you to enforce per user sync of Desktop, Documents and Pictures folders to OneDrive for seamless file access from new Windows installs.



NOTE

While you can continue to use migration processes you have used in the past, with your shift to Office 365 ProPlus we recommend you use OneDrive 'Known Folder Move' (see below). To see the full desktop deployment process, visit the [Modern Desktop Deployment Center](#).

One of the trickiest and often most manual tasks of a large-scale deployment is the transferring of your users' files and settings. In this article we will cover the options available to you to migrate users to new, refreshed and re-imaged PCs.

Manual Migration

When it comes to deciding on what to keep when moving to a new PC or a new version of Windows some users may want to keep everything, others may want to take the opportunity to clean up their drives. Because of this, some IT departments choose to handle user file migration manually, sometimes by having support teams visit users; sometimes by setting up support centers for users to bring their PCs to the support team. Either way users can be involved in deciding what to transfer and what to discard.

Whether this is an option in your organization will depend on the scale of the migration you are planning. Clearly it is limited to the time and physics involved in working directly with users, understanding their needs, copying files across to their new, or freshly updated PC.

If you are opting for a manual migration, you may need to assess whether you will be able to complete the task by January 2020, when support for Windows 7 ends. If this looks doubtful, look into using one of the automated options below, or request more people to help.

Automated Migration using USMT

For large-scale deployments you can automate much of the process using task sequence-based deployment automation tools such as System Center Configuration Manager or the Microsoft Deployment Toolkit (MDT). Both these solutions make use User State Migration Tool (USMT) as part of their end-to-end deployment process.

USMT is part of the [Windows Assessment and Deployment Kit \(Windows ADK\)](#)

USMT captures user accounts, user files, operating system settings, and application settings, and them migrates them to a new Windows installation. It also gives you, the IT Admin, control of exactly what gets migrated and, optionally, can exclude unwanted file types – for example audio and video files, or executables.

During the migration process you will need to have sufficient server storage capacity available to act as your temporary migration store. Here USMT offers two important features. First, it can estimate, per PC, the amount of storage you will need. Second, it allows for migration stores to be encrypted, reducing the risk of data being compromised while being stored on file servers.

Where you are performing a PC refresh and not reformatting the primary Windows partition, you also have the option of using a hard-link migration store with USMT. This process preserves user state on the PC while the old operating system and apps are removed and refreshed. With the restore process coming from the same local partition, this option offers significant improvements on performance, and reduces network traffic.

[User State Migration Tool \(USMT\) Overview](#)

OneDrive Known Folder Move

If your users are on OneDrive or you are adding OneDrive in as part of this deployment, there is new option available to you. Using the cloud to synchronize user files, OneDrive "Known Folder Move" feature provides a level of flexibility not possible with local network-based file migration options. If enabled prior to migration, it provides secure access on new or refreshed PCs and, it eliminates the need to create temporary migration stores on your own servers. It is also has the potential to be completely transparent to the user.

[Redirect and move Windows known folders to OneDrive](#)

If you're already using OneDrive, you will know that users can select the folders and locations they would like to sync from OneDrive or SharePoint to their device, but that effectively puts the burden on the end user to set it up. With Known Folder Move, you can target the Documents, Desktop and Pictures folders within a user profile and protect it all on OneDrive. A user can do this themselves or, importantly for this scenario, you can [enforce this using Group Policy settings](#).

With Known Folder Move, users don't change their workflow – everything looks the same before, during and after synchronization with OneDrive is complete. Through Group Policy you can even choose whether or not to notify users that their documents, pictures and desktop are protected in OneDrive. If you choose not to, it all happens

silently in the background. The users will only be aware when they take delivery of a new PC or their PC is refreshed. As soon as they sign in to their OneDrive account, these files will be available again, and will be restored to their new PC. And of course, OneDrive means they will also store their files securely at any time from their phones and other devices.

Authentication for OneDrive is powered by Azure Active Directory, so for extra security, you can easily enable multi-factor authentication, and you can set policies to control the upload and download bandwidth OneDrive uses to limit network activity.

You don't have to migrate every user at the same time. You may want to phase the roll-out of the Group Policy settings, or [limit file sync to domain-joined PCs](#).

Start Menu and Task Bar Customization

OneDrive is designed to sync and protect files and folders; it does not sync application or Windows settings. To do this in the past you may have used the copy profile method to configure standard layouts for users' Start menus and taskbar settings. In Windows 10 Pro, Enterprise, and Education, you can use Group Policy, MDM, PowerShell, or provisioning packages, to deploy [customized Start and taskbar layouts](#). No reimaging is required, and the layout can be updated simply by overwriting the .xml file that contains the layout.

To create a new layout simply configure a sample system, and use the PowerShell [Export-StartLayout](#) cmdlet to generate an XML file, then place this file on a network share, or cache it locally as part of your deployment sequence; it just needs to be reachable as Read-only file once the user signs in. You can then use policy or the [Import-StartLayout](#) cmdlet to reference this file.

Removing unwanted in-box apps

Windows 10 includes many useful built-in apps as part of the standard installation, but you may want to remove some of these from your managed PCs, and even configure your installation to prevent those apps from returning, for example, XBOX or Zune Music. You can retrieve a list of these apps using the [PowerShell Get-AppxPackage](#) commands, and remove those you do not want using the [Remove-AppxPackage](#) command. Alternatively, you can mount the Windows Image (.img) file offline before deployment, and extract packages you do not want using the [Deployment Image Servicing and Management \(DISM\)](#) command line tool and the [Remove-AppxProvisionedPackage](#) command.

Next Step

[Step 5: Security and Compliance Considerations](#)

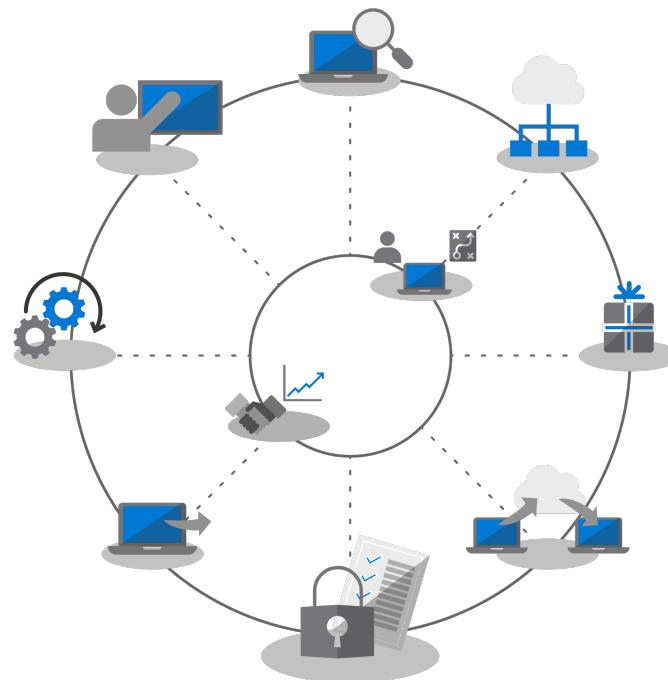
Previous Step

[Step 3: Office and LOB App Delivery](#)

Step 5: Security and Compliance Considerations

1/17/2019 • 7 minutes to read • [Edit Online](#)

Review your options for targeting new security and compliance capabilities as part of your Modern Desktop Deployment along with the considerations and common blockers when moving from previous versions of Windows and Office.



Step 5: Security and Compliance Considerations

Windows 10 and Office 365 ProPlus provide new ways to protect your data, devices and users and quickly detect and respond to threats. Also, learn how to deal with common problems associated with disk encryption, anti-malware apps and policies when moving to Windows 10.



NOTE

Security and Compliance is the fifth step in our recommended deployment process wheel covering Windows 10 and Office 365 ProPlus security and compliance considerations. To see the full desktop deployment process, visit the [Modern Desktop Deployment Center](#).

Many of the security-related capabilities in Windows 10 alone are driving the shift to the newer platform. Also, integration with cloud services in Office 365 and identity options using Azure Active Directory brings access to new and continually updated protections for your data, devices and users.

Overcoming Potential Security-Related Deployment Blockers

Before explaining new capabilities that you can add as you move to Windows 10 and Office 365 ProPlus and connect those experiences to the cloud, let's start with a few trends we're seeing that can often interrupt deployment progress.

Disk Encryption

First one of the initial challenges you might encounter is hard disk encryption. Many solutions for hard disk encryption cannot easily be upgraded from a previous version of Windows to a newer version of Windows.

Some disk encryption solutions allow you to perform the upgrades when using the '/reflectdrivers' option with Windows Setup on certain versions of their platforms, but others may require you to unencrypt the drive prior to deployment, then re-encrypt after Windows 10 is installed. Some solutions also do not allow you to move from Master Boot Record (MBR), using legacy BIOS, to GUID Partition Table (GPT), required for UEFI. This is important because a 64-bit version of Windows 10 with UEFI is required for the new virtualization-based security capabilities in Windows 10 and those are explained below.

One option to resolve these issues is using BitLocker in Windows 10, which is included in Windows 10 Pro and higher editions. BitLocker allows you to suspend protection for OS upgrades and Feature Updates as part of the process.

[Bitlocker basic deployment](#)

Antivirus and Antimalware Application Compatibility

Second, while we've seen that more than [99% of Windows applications are compatible](#) between Windows 7 and Windows 10, the exceptions are often anti-virus (AV) apps or Virtual Private Network (VPN) clients. These applications often implement non-standard development practices and APIs, using often undocumented ways to protect your system or connect you to network resources.

As a result, these apps by nature can be fragile to changes when shifting to a new version of Windows. If your AV or VPN software doesn't work in Windows 10 or after upgrading, the fix is typically to replace the app you're using with something supported and tested on Windows 10.

Security Policies

Your Active Directory Group Policy settings used for older versions of Windows and Office may not translate directly to Windows 10 and Office 365 ProPlus, and there are different considerations with newer security and compliance capabilities. It's a good idea to use the Microsoft Security Compliance Toolkit to get a baseline of the security policies for current versions of Windows and Office. Additionally, it's worth looking into Mobile Device Management policies as part of Microsoft Intune.

PROFILE NAME	PLATFORM	PROFILE TYPE	ASSIGNED	LAST MODIFIED
Automatic Redeployment (Enable)	Windows 10 a...	Device restrictions	Yes	2/05/18 12:18 AM
Conference Room PCs	Windows 10 a...	Custom	No	1/30/18 9:59 AM
Custom Word 2016	Windows 10 a...	Custom	No	5/04/18 3:29 PM
MMS 2018 Demo 1 - Remote Assistance Warnings	Windows 10 a...	Custom	No	5/04/18 10:53 AM
Manage Edge Favorites and Security	Windows 10 a...	Endpoint protection	No	4/19/18 12:02 AM
Ransomware Protection	Windows 10 a...	Endpoint protection	Yes	5/31/18 1:42 PM
Remote Assistance Messages	Windows 10 a...	Custom	No	5/04/18 3:16 PM
Windows Defender ATP	Windows 10 a...	Custom	Yes	4/04/18 10:48 AM
Word Custom AC for Caps	Windows 10 a...	Custom	Yes	5/04/18 4:02 PM

New Security and Compliance Capabilities in Microsoft 365

Now, those were considerations for moving your current protections forward and things to be aware of before your shift. Now let's take a look at new capabilities that you can take advantage of when moving to Windows 10, Office 365 ProPlus and cloud-based options from EMS and beyond.

Identity and Access Management

Starting with identity and access management. Azure Active Directory is the identity control plane for apps, devices and Cloud services and is the modern way to connect to Office 365 and other Cloud services. Conditional access allows you to define different authentication requirements based on where you are logging in from, which device you're using, as well as things like anomalous behaviors.

At the device level, biometrics can provide unique identifiers for simpler and more secure access to your devices and apps - as you move toward the goal of eliminating passwords. Windows Hello offers device-based, multi-factor authentication. It relies on the device itself, your PIN, or unique biometric identifier such as your face or fingerprint, which you can enforce via policy.

[Fundamentals of Azure identity management](#)

[Understand Azure identity solutions](#)

[Azure Active Directory Conditional Access](#)

[Windows Hello for Business](#)

Virtualization-based security

Now beyond identity, you can also enable continuous protection against both known and unknown threats and to do this Windows 10 uses virtualization-based security at the core to ensure boot integrity and code integrity using Secure Boot. We can help also stop credential theft with Credential Guard by maintaining user secrets in isolation from Windows. And, Application Guard can isolate and mitigate browser-based threats by running the browser in an isolated container. All of these technologies use virtualization-based security in Windows 10 and are foundational changes that cannot be replicated on a Windows 7 system – note that these also require UEFI, 64-bit Windows and virtualization extension support with SLAT – at the hardware level.

[More on Virtualization-based Security](#)

[Security enhancements from cloud services](#)

Cloud services provide another layer of optional protection to improve Windows and Office security. These can give you a new level of often real-time control that can instantly detect, resist and respond to new attacks and attack types – especially compared to traditional software updating and AV signature files – where response and update deployment times are inherently slower.

Along with the Microsoft Intelligent Security Graph, you have faster access to both information and protections from emerging threats. Here are a few examples of what you can take advantage of, starting with Office.

Data Loss Prevention built into Office 365 ProPlus, helps inform users of security policies when high risk content like credit card or identification numbers are detected. Policies can inform or block sending and sharing after notifying users.

Azure Information Protection is a complementary service that can be used with Office, allowing users to easily classify and label their Office files. It can trigger automatic action on labeled files, such as encryption or locking down sharing.

We've also introduced **Safe Links** protection across Office apps to protect you against a dynamic list of known malicious websites.

Additionally, **Safe Attachments** in Outlook and as part of Exchange Online goes beyond email filtering to inspect attachments. If a high-risk attachment is identified, Safe Attachments will inform the user of known malicious attachments and remove them from email.

Office 365 Message Encryption (OME) can also be used to safeguard email and attachments sent, ensuring only intended recipients can view email content. OME works seamlessly with Google, Yahoo, and Microsoft consumer account authentication, and one-time passcodes allow users of other email services to securely receive email as well.

Additional Windows 10 protections

Windows Defender Application Control in Windows 10 operates off an approved allow and deny list of applications that Microsoft has checked for safety and all that is managed by endpoint protection policies using Microsoft Intune.

Windows Defender Advanced Threat Protection is a unified platform for preventative protection, post-breach detection, automated investigation, and response. It protects endpoints from cyber threats; detects advanced attacks and data breaches, automates security incidents and improves security posture.

Exploit Guard helps reduce the attack surface for running applications by preventing malware from getting into Windows and blocking untrusted processes from accessing protected folders.

Microsoft Intune

Microsoft Intune serves as a Cloud based management service for mobile scenarios, including IOS, Android and Windows devices, and can now be configured for co-management to complement and extend controls for specific workloads managed by System Center Configuration Manager. One advantage here is that, devices accessing protected resources can be required to enroll into device management – even non-managed, non-domain joined or non-Azure AD joined devices. You can also take advantage of granular configuration and compliance policy enforcement at the operating system and application level. Application policies and settings can be configured centrally and enforced for Office 365 ProPlus and Store apps in Windows 10 using Microsoft Intune.

Next Step

Step 6: OS Deployment and Feature Updates

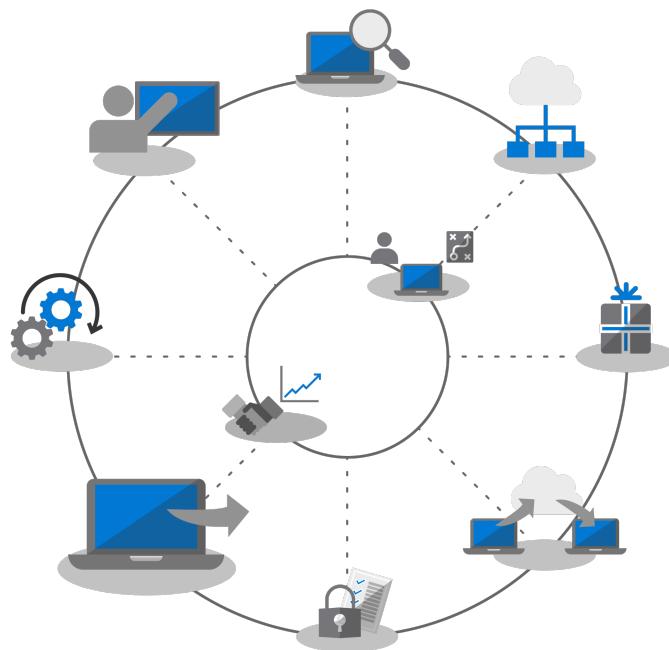
Previous Step

Step 4: User Files and Settings

Step 6: OS Deployment and Feature Updates

1/18/2019 • 7 minutes to read • [Edit Online](#)

Learn the options and get ready for operating system deployment using upgrade and imaging approaches with System Center Configuration Manager or the Microsoft Deployment Toolkit.



Step 6: OS Deployment and Feature Updates

Task sequence-based deployment is used to automate large scale, phased deployment for bare metal installs, PC refresh and PC replacement. Upgrade task sequences will also help you stay current with major semi-annual updates. And Windows Autopilot is a recent addition that modernizes the new PC acquisition process.



NOTE

OS Deployment and Feature Updates is the sixth step in our recommended deployment process wheel covering Windows 10 OS deployment, upgrades and Feature Updates. To see the full desktop deployment process, visit the [Modern Desktop Deployment Center](#).

If you've been following the deployment process wheel till now, you've at least partially completed the steps for device and app readiness, prepared your infrastructure, configured and collected app packages, have a plan in place for migrating user files and configuring default settings as well as have plans for retaining your existing security controls and perhaps deploying new ones.

Now we've arrived at the stage where you're putting all these pieces together to automate as much as you can to

install Windows 10 and Office 365 ProPlus, along with the necessary drivers, apps and whatever else is needed.

Ultimately, the best measure of success with an OS deployment is meeting user expectations and avoiding disruptions in their work. And in this step, you'll start testing and deploying to pilot users as part of a phased deployment. And one tip here, before you broaden deployment, you'll need to skip ahead to step 8 on our deployment process wheel – [User Communications and Training](#) to make sure users are informed and prepared for changes coming their way and that you can measure your roll-out pace with continuous validation using Phased Deployment.

Windows Imaging Process

Most organizations use the process of PC imaging to configure and capture a clone of Windows, including a base set of a few standard apps installed, or an even a thinner image with only application runtimes and updates. The best way to do this is using a virtual machine for this process to avoid any unexpected driver-related compatibility issues and for automation purposes.

If going the image capture route, it's best to automate as much as possible to ensure the best quality image and a repeatable process. For most deployments, it is also recommended to put as little customization and pre-installed apps as possible in the Windows image prior to capturing. This is what is called a 'thin image' approach, which can save overall bandwidth on the network by eliminating the number of apps within the image. By starting with a thin base image, you can layer on required apps, languages and configurations dynamically tailored to users.

During the build and capture process, tools like System Center Configuration Manager and the Microsoft Deployment Toolkit use the System Preparation Tool – or Sysprep – along with the "Generalize" command to reseal your image before they capture the Windows 10 installation as an image.

The captured image will have the Windows image – or WIM – format like standard Windows installation media. Once you have your custom WIM file, you can use another task sequence as part of your OS deployment in System Center Configuration Manager or Microsoft Deployment Toolkit to perform deployment-related tasks, to apply the image and run tasks before and after your Windows image is applied.

[Create a Windows 10 Reference Image](#)

[Create a Task Sequence to Install an Operating System](#)

Deployment Types

With your custom image ready, the installation or migration type will fall into the following categories:

- First, **bare metal deployment**. This is the scenario used to deploy an image to a clean disk, or to reimagine a computer where you don't intend to keep any of the data on the disk
- And second, similar to bare metal, is **Computer Refresh**, with the key difference that user state remains on the disk* or will be restored after the install is complete
- And last is **Computer Replacement**. Here as the name implies, you are replacing a PC with another PC. In this case, there is often a backup of user files from the first PC to a central location, then a restore of those files to the second PC.

All three of these scenarios have something in common, they use a task sequence to run, and a custom image can be applied each time.

[More About Windows 10 Deployment Scenarios](#)

In-place Upgrade using Task Sequence Automation

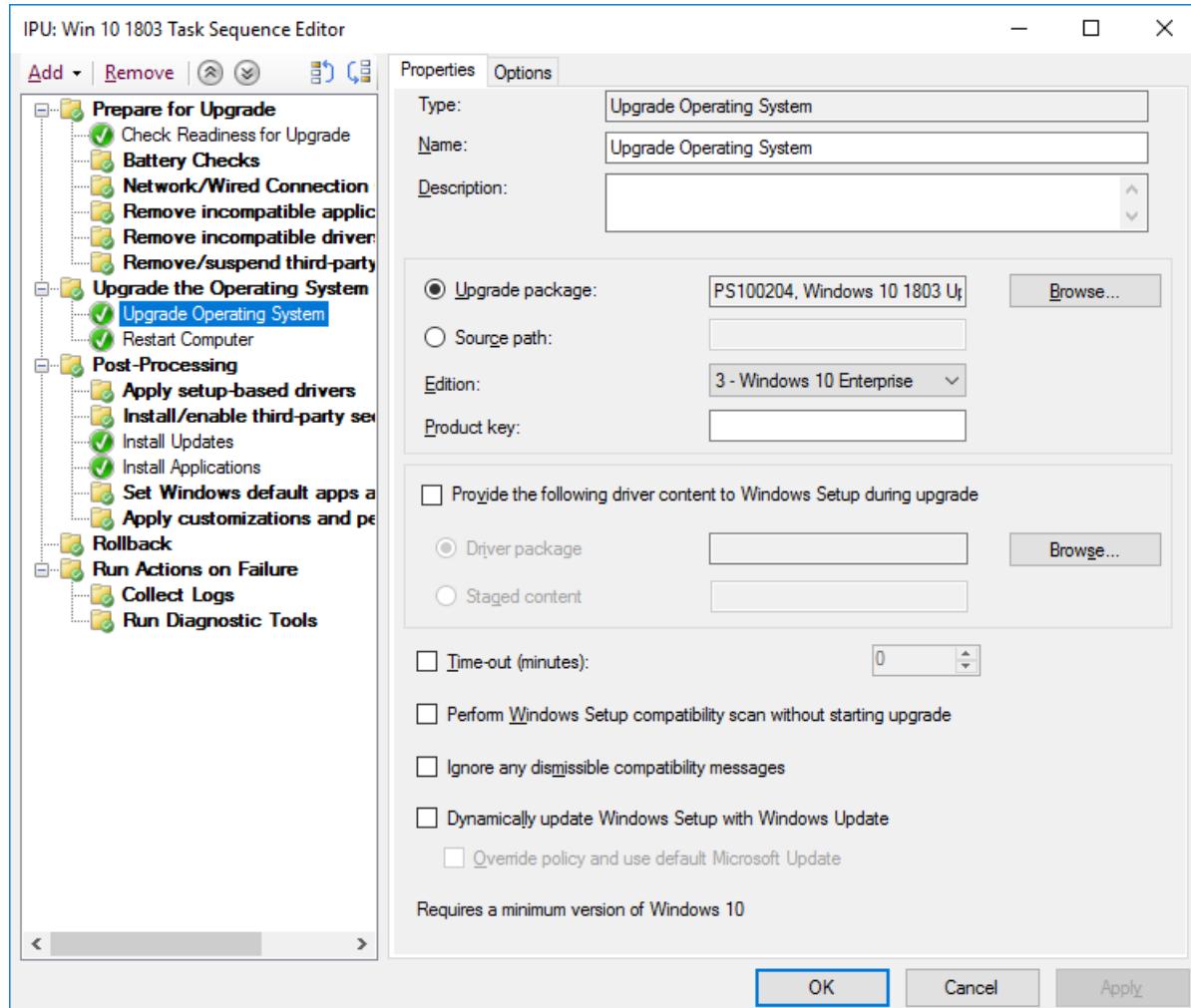
In addition to these deployment types, there is a new option available now as a System Center Configuration Manager Task Sequence with Windows 10 – and in-place upgrade using the Upgrade Task Sequence.

In-place upgrades from a previous version of Windows do not require a task sequence, but it is a recommended

approach when deploying at enterprise scale. An in-place upgrade does not allow you to apply a custom image with applications, but you can update the default install.wim using offline servicing. For example, you can make sure it has the latest Windows updates applied prior to performing upgrades.

In-place upgrade uses windows setup. The setup engine runs several small pre-installation checks looking for known compatibility issues. It also preserves the user state and applications and only removes what isn't compatible with the version of Windows 10 being installed. With this option, previously installed applications and user state are preserved. In-place upgrade also allows you to roll-back to the previous OS installed if needed for troubleshooting purposes.

Windows 10 Pre-Upgrade Validation Using setup.exe



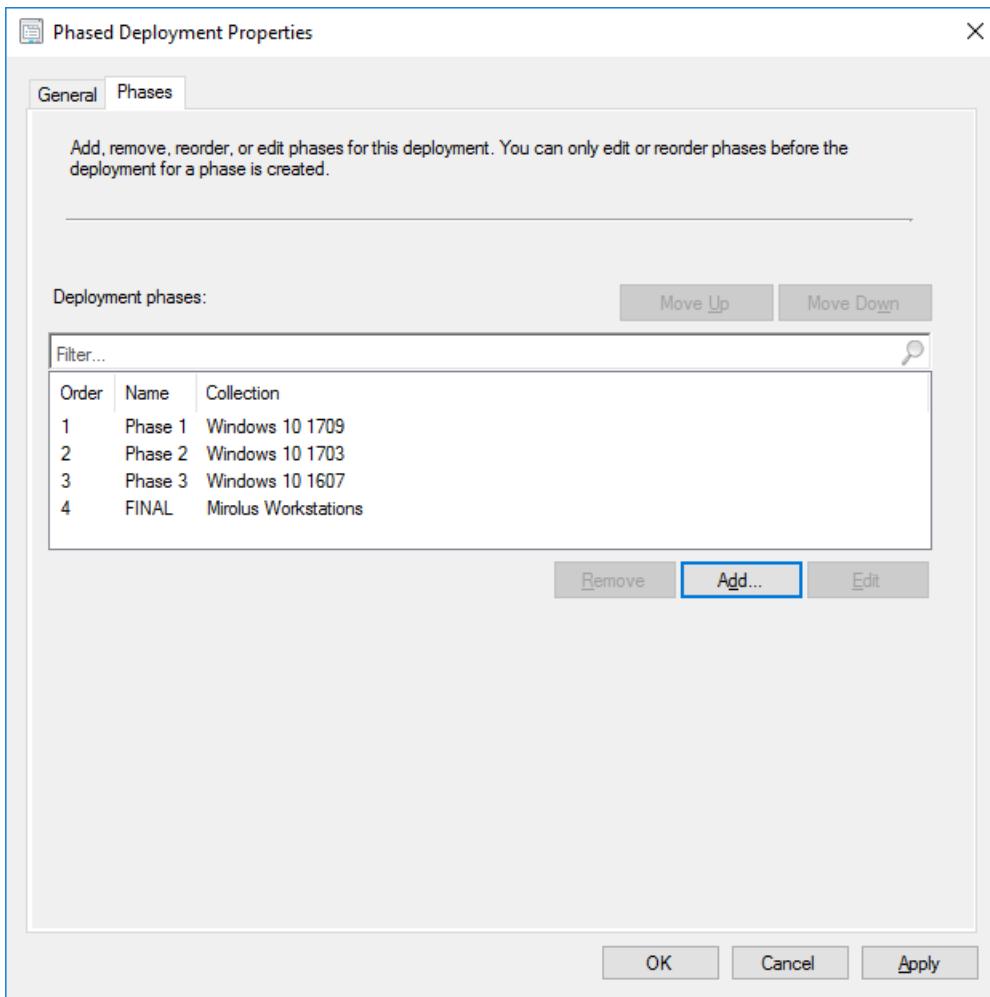
The in-place upgrade scenario can be used to migrate to Windows 10 from legacy versions of Windows, as well as upgrade from previous versions of Windows 10. After Windows Setup completes the upgrade, your task sequence can continue to run and upgrade applications like Office, replace drivers, and apply personalization settings. Likewise, you can use the Upgrade Task Sequence to perform pre-installation tasks or checks prior to carrying out the upgrade.

Perform an in-place upgrade to Windows 10 using Configuration Manager

Create a task sequence to upgrade an OS in Configuration Manager

Phased Deployment

As you're planning your deployment, you'll be targeting computers for bare metal, refresh, replace and upgrade paths. The recommended approach in this case is to use phased deployment to collections of similar machines. This way, you can validate compatibility, delivery and automation, user acceptance, network bandwidth consumption, and other factors before increasing the scale of your deployment.



Recommended Tools: System Center Configuration Manager and the Microsoft Deployment Toolkit

Regardless of the deployment type you choose, you'll want to make sure it's as automated as possible for predictability and repeatability. Microsoft offers two solutions to automate OS deployment using automated task sequences:

- **System Center Configuration Manager** (ConfigMgr) provides built-in operating system deployment capabilities to complement its capabilities for software distribution and software update management. ConfigMgr is widely used by organizations of all sizes and supports all four Windows deployment types. Optionally, you can integrate ConfigMgr with Microsoft Intune to add additional capabilities for deployment and device management.
- And one other popular deployment option is the free **Microsoft Deployment Toolkit** (MDT) which is typically used by small and medium sized organizations for OS deployment. This requires very little infrastructure. MDT integrates with Windows Deployment Services (WDS) for network boot. It supports all four deployment types as well as installation of applications, drivers, and settings. And of course, MDT can even be integrated with Configuration Manager.

Name	ID	Version	TaskSequence...	enable	guid
Convert BIOS to UEFI (OS)	CONVERTOS	1.0	Custom.xml	False	{560bbe5e-538...
Convert BIOS to UEFI (OS-PE-OS)	CONVERT	1.0	Custom.xml	False	{1b3fbf1c-3363...
Convert BIOS to UEFI (PE)	CONVERTMEDIA	1.0	Custom.xml	False	{975d4f7-8606...
Convert with Refresh to Windows 10 Enterprise x64 v1703	WIN10X64UEFI	1.0	Client.xml	False	{3aa10f97-afc9...
Convert with Upgrade to Windows 10 Enterprise x64 v1703	WIN10UPGUEFI	1.0	ClientUpgrade...	False	{1746f723-0bd...
Windows 10 Enterprise x64 v1607	W10-X64-003	1.0	Client.xml	False	{4906501f-454...
Windows 10 Enterprise x64 v1607 - Apps Removed	W10-X64-004	1.0	Client.xml	False	{4906501f-454...
Windows 10 Enterprise x64 v1607 - Credential Guard	W10-X64-006	1.0	Client.xml	False	{4906501f-454...
Windows 10 Enterprise x64 v1607 - Upgrade	W10-X64-004	1.0	ClientUpgrade...	False	{0fb35a3-341...
Windows 10 Enterprise x64 v1703 - Upgrade	W10-X64-009	1.0	Client.xml	False	{146837ba-52e...
Windows 10 Enterprise x64 v1709	W10-X64-011	1.0	ClientUpgrade...	False	{1746f723-0bd...
Windows 10 Enterprise x64 v1709 - BitLocker	W10-X64-013	1.0	Client.xml	True	{d999f96b-9a08...
Windows 10 Enterprise x64 v1709 - Move To OU	W10-X64-007	1.0	Client.xml	True	{d5097bf6-7325...
Windows 10 Enterprise x64 v1709 - Upgrade	W10-X64-005	1.0	Client.xml	False	{a7a146b-44f6...
Windows 10 Enterprise x64 v1709 - Upgrade	W10-X64-012	1.0	ClientUpgrade...	False	{c8fd2472-65ef...
Windows 10 Enterprise x64 v1709 - with Apps	W10-X64-014	1.0	Client.xml	False	{109abcc52-b2b...
Windows 10 Enterprise x64 v1803	W10-X64-001	1.0	Client.xml	False	{e4a13497-826...
Windows 10 Enterprise x64 v1803 - Upgrade	W10-X64-016	1.0	ClientUpgrade...	True	{febe998-80f...

Windows Autopilot

A new option with Windows 10 is to configure new PCs as part of your hardware refresh cycle using Windows Autopilot. Here you can work with supporting hardware vendors to customize the default Windows setup experience – for example by eliminating options presented to users, like Licensing Agreements or telemetry settings.

Then, when a user signs in to the PC during setup using their Azure AD credentials, the device enrolls into Microsoft Intune, which can then take over the deployment process and apply applications, software updates configurations and compliance policies. Windows Autopilot can also optionally prevent the user from accessing the first session until provisioning is complete.

Overview of Windows Autopilot

Windows Autopilot Prerequisites

Windows Update for Business for Feature Updates

Windows Update for Business is a free service that enables IT Pros to keep Windows 10 devices always up to date by directly connecting the devices to the Windows Update service. Windows Update for Business can be configured via Group Policy or through MDM solutions such as Microsoft Intune and allows IT Pros to create [deployment rings](#) to validate new builds. It is integrated into existing management tools such as Windows Server Update Services (WSUS), System Center Configuration Manager (current branch), and Microsoft Intune. Additionally, Windows Update for Business supports peer-to-peer delivery to help optimize bandwidth efficiency and reduce network congestion.

For more detailed information on Windows Update for Business please review the following documentation:

- [Deploy Updates Using Windows Update for Business](#)
- [Configure Windows Update for Business](#)
- [Integrate Windows Update for Business with Existing Management Tools](#)
- [Use Group Policy to configure Windows Update for Business](#)
- [Use Microsoft Intune to configure Windows Update for Business](#)

Next Step

[Step 7: Windows and Office Servicing](#)

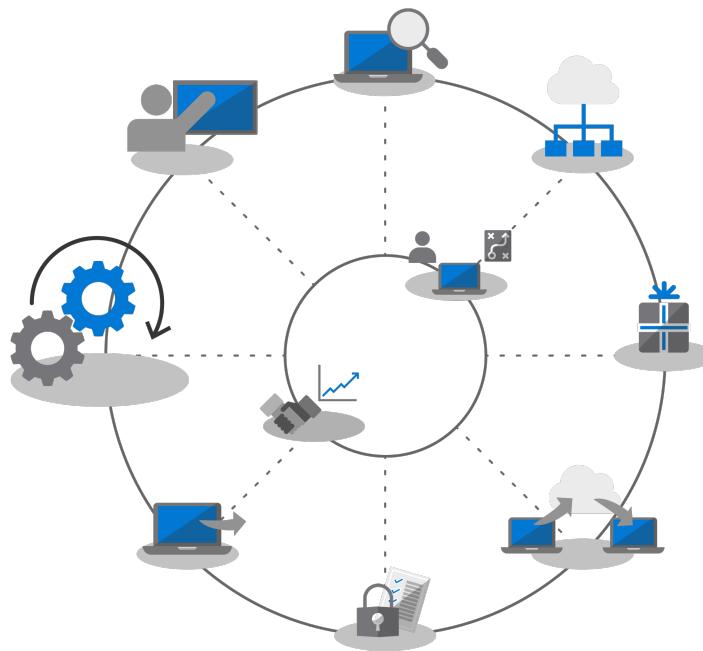
[Previous Step](#)

[Step 5: Security and Compliance Considerations](#)

Step 7: Windows and Office Servicing

1/18/2019 • 8 minutes to read • [Edit Online](#)

Prepare for semi-annual channel updates with new features and capabilities in Windows 10 and Office 365 ProPlus along with corresponding updates to management tools with System Center Configuration Manager Current Branch.



Step 7: Windows and Office Servicing

Both Windows 10 and Office 365 ProPlus continually add new capabilities to keep bringing user experiences and security forward with the latest innovations. Learn how to stay current with semi-annual and monthly updates, how the new servicing model works and the tools and options you have.



NOTE

Windows and Office Servicing is the seventh step in our recommended deployment process wheel covering the planning aspects of preparing for semi-annual updates to features. To see the full desktop deployment process, visit the [Modern Desktop Deployment Center](#).

Both Windows 10 and Office 365 ProPlus introduce new servicing options, support models and update timelines. These changes simplify the process for staying current on the latest features. Along with these updates are new configuration options to enable servicing plans that meet your needs.

[Helping customers shift to a modern desktop](#)

Update Types

Updates fall into two main categories, feature updates and then quality and security updates which contain cumulative security, reliability and bug fixes. In terms of cadence both Windows and Office deliver a semi-annual channel which delivers new features twice per year around March and September while quality and security Updates occur Monthly. Additionally, unique to Office 365 applications, we offer a fully-supported Monthly Channel option where updates contain both new features and quality updates.

If you're used to a longer cycle between desktop OS and app updates, you might be wondering;

- Will the updates be compatible?
- Will I need to keep retraining my users?
- And what are the risks?

To answer those questions and the rationale for delivering new capabilities more frequently, we'll some of the advantages of this approach

Feature Update Benefits

First, we've moved away from the model of the past that would introduce huge waves of change around every three years to now incremental smaller changes with feature updates twice per year. Why? With technology trends moving so fast in addition to rapidly evolving security threats, this keeps experiences and protections current. Some of the security related updates for example can't just be delivered by monthly security updates or antivirus signature files; they may be low-level changes platform, like virtualization-based security.

[Quick guide to Windows as a service](#)

[Mitigate threats by using Windows 10 security features](#)

Cumulative Update Model Benefits

Second delivering quality and security updates as a cumulative update package corrects many of the issues of the past. It used to be that you might pick and choose sometimes from a dozen updates or more each month for both Windows and Office. As you can imagine, this creates a nearly impossible set of test matrices for support. Also, if you install a version of Windows or Office that is a year or more old, it might take hours or sometimes days to apply all updates delivered since that version was released.

With the cumulative model, you're always one update away from being current and in doing so the number of monthly updates that you need to deploy is reduced. Each update builds upon updates from previous months and contains all of the fixes that you need to get current. Cumulative updates are especially helpful when PCs has been turned off for several months because they are in storage waiting to be reassigned to a different user.

Expanded Validation of Updates

Another advantage is that, before we roll out updates for broad deployment, we first release builds via the Insider programs for [Office](#) and [Windows](#), and this allows us to gather telemetry and feedback ahead of us releasing updates broadly. Now the Insider programs are open to everyone so that you can get ahead of understanding the updates. By the time we release updates we will have received telemetry from millions of configurations, so when we do roll out updates, quality is now inherently more predictable

AND one more thing, because Office 365 ProPlus Insider builds reflect monthly channel updates, if you are using semi-annual channel for Office to deliver feature updates twice per year aligned to Windows, you can validate those builds early as well using the semi-annual channel targeted releases.

Supporting Management Tools

We've also thought through how to make the deployment of updates seamless to you. System Center Configuration Manager Current Branch is updated frequently to support the roll-out of these updates to Windows and Office and any new capabilities.

[Deploy Windows 10 updates using System Center Configuration Manager](#)

[Manage Office 365 ProPlus with Configuration Manager](#)

Overview of Windows and Office Channels

Windows 10 offers three servicing channels:

- **Windows Insider Program** for organizations to test and provide feedback on features shipped in the next feature update
- **Semi-Annual Channel** provides new functionality with Feature Update releases twice per year
- **Long Term Servicing Channel** is designed only for specialized devices needing a longer servicing option

Office 365 offers four servicing channels:

- **Office Insider Program** for organizations to test and provide feedback on the newest Office features and functionalities still in development
- **Monthly Channel** to provide users with the newest Office features as soon as they're available
- **Semi-Annual Channel** provides new functionality with new features only twice per year
- **Semi-Annual Channel (Targeted)** is a fully supported build of Office that enables pilot users and application compatibility testers to test and validate the next Semi-Annual Channel

For detailed information about Windows and Office servicing channels please review the below documentation:

- [Overview of Windows as a Service](#)
- [Overview of Update Channels for Office 365 ProPlus](#)

Phased Deployment of Updates

Now let's shift gears to how you will roll out these updates. For any release, we recommend at least three deployment phases for IT – validation, piloting and broad production deployment. Once you're up and running on Windows 10 and Office 365 ProPlus, you'll use monthly servicing to stay current with critical security and quality updates, then you'll move to semi-annual servicing for new features.

Monthly Updating

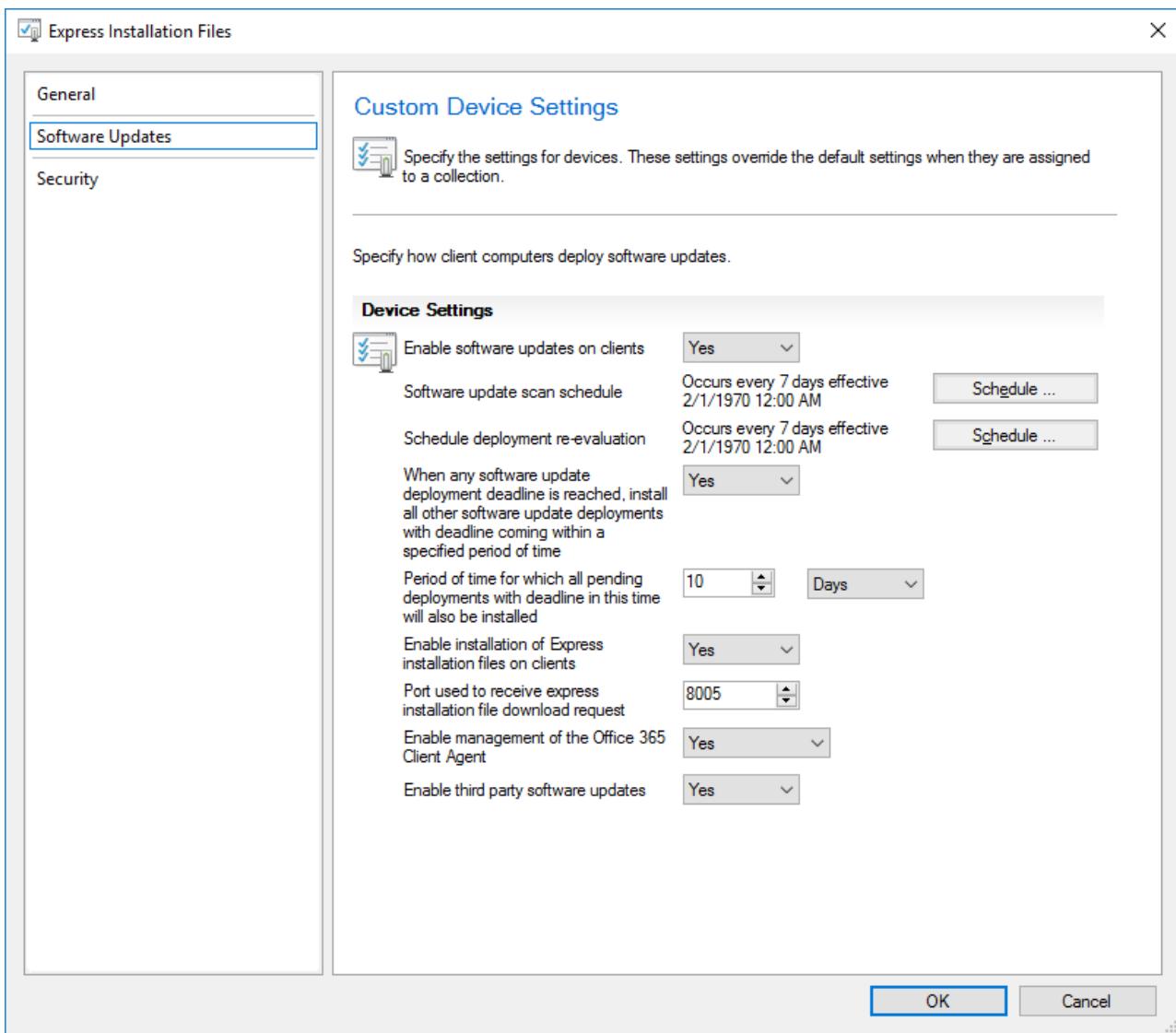
The service model is designed so you can choose to limit the roll-out of new features to twice per year, and if needed you can even skip a semi-annual update and continue receiving quality and security updates. As mentioned, the cumulative nature of monthly updates means each will increase in size per month.

Express Updates

Using a technology called "Express Updates" in Windows and Binary Delta Compression in Office, we can reduce the download size significantly. In both approaches, the update engines compare what's on the PC and finds only the differentials needed to update what's there.

[Windows 10 quality updates explained & the end of delta updates](#)

Windows Update for Business and Windows Server Update Services have supported express updates for a long time, but we've now extended that support to System Center Configuration Manager so that it can also use Express Updates.



Binary Delta Compression

Binary Delta Compression in Office is only used if you're updating from the most recent version of Office 365 ProPlus-- so to use this approach you need to be updating from the previous build and can't skip updates.

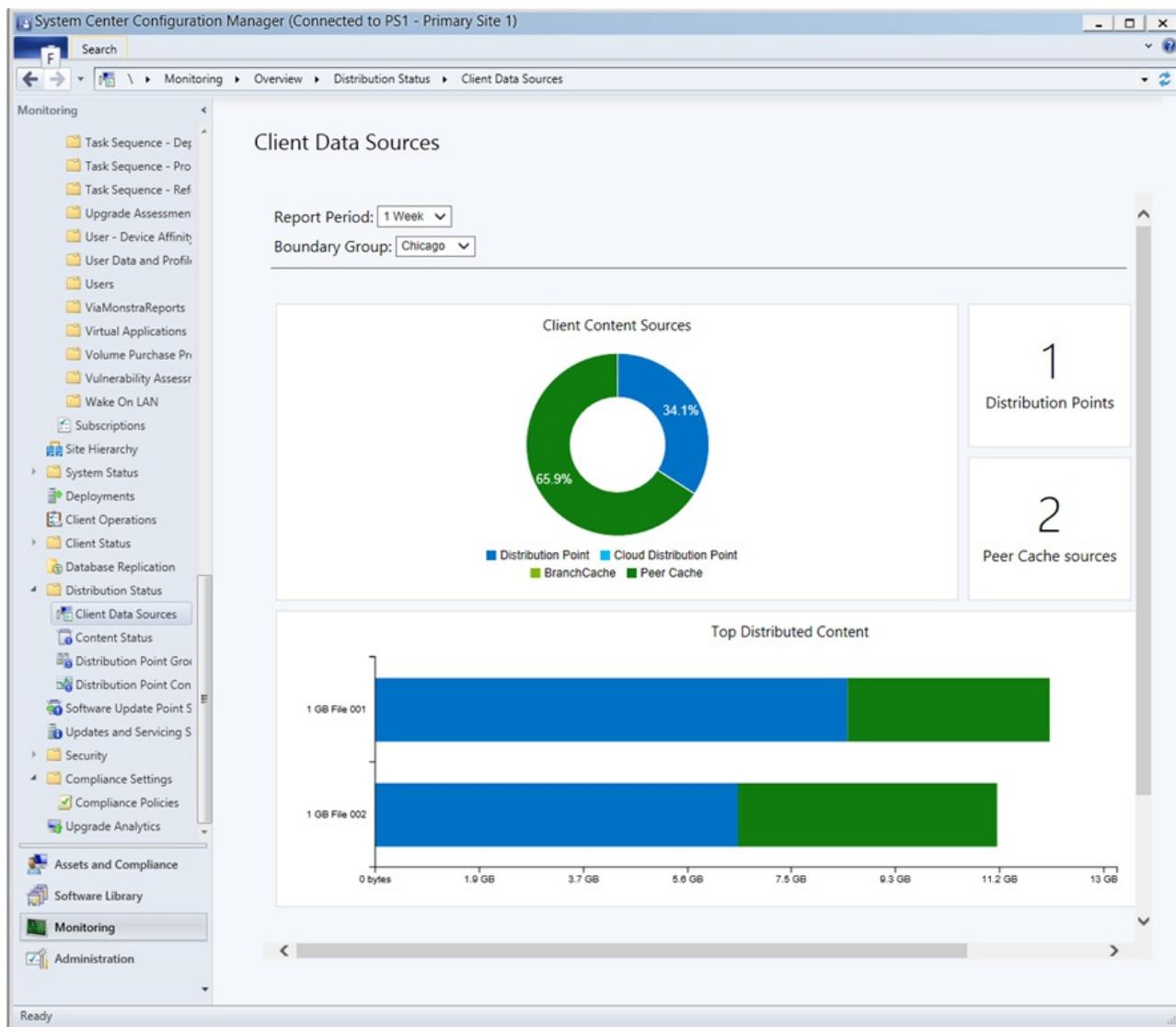
Windows and Office update channels can be managed via Configuration Manager using the standard approval and targeting process. Additionally, you can use policy settings in Office and Windows to enforce update channels used, as well as related settings.

Semi-Annual Updates

So those are your considerations for monthly updates, now let's move to the larger, semi-annual updates.

As we covered in Device and App Readiness, you'll want to begin your preparation for these larger updates using the same readiness tools we set up in Step 1 of the deployment process wheel.

As for tooling, you can use policy settings with Windows Update for Business, software update management via System Center Configuration Manager, Windows Server Update Services (WSUS), or update policies set by Microsoft Intune. If you are concerned about network bandwidth, see Step 2: Directory and Network Readiness, to learn about your options to reduce network traffic via Delivery Optimization and other peer to peer caching technologies.



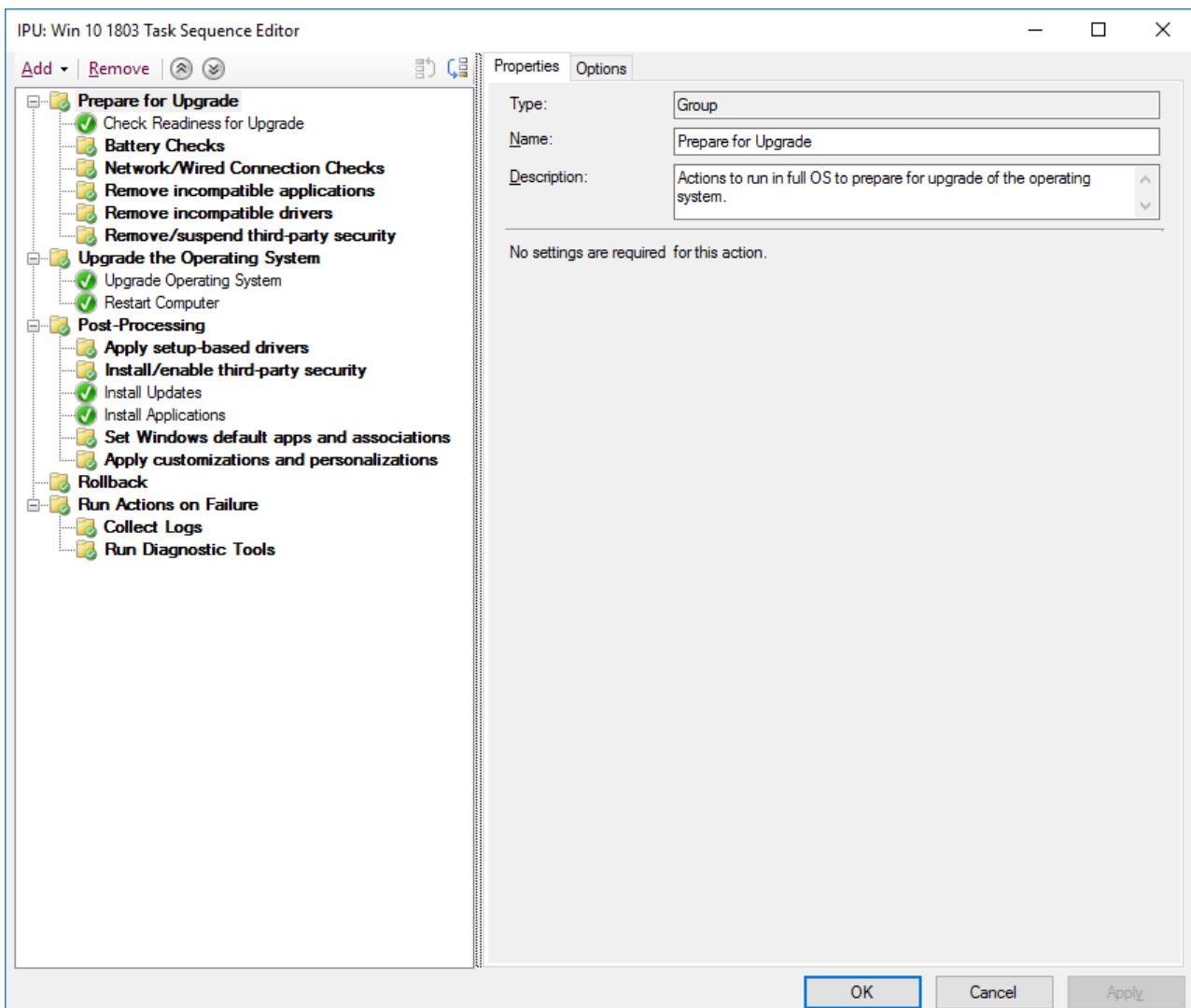
Windows Semi-Annual Channel

Semi-Annual Channel for Office 365 ProPlus

Upgrade Task Sequences

Installing the larger feature updates via standard software update management routines is a supported option, but many organizations will opt to use an Upgrade Task Sequence with System Center Configuration Manager or the Microsoft Deployment Toolkit.

A Task Sequence allows you to create custom checks or tasks BEFORE to the installing the Feature Update and allows you to perform custom tasks AFTER the update installation itself has completed – post-update tasks might include temporarily suspending services if needed during the update, driver installation and replacement, application upgrades or taskbar and Windows 10 Start personalization settings.



If you're already using task sequences to migrate your Windows 7 machines to Windows 10 and are well-versed with those tools, this is a great place to start and provides ultimate control. While you can use a single task sequence for the entire upgrade, it is quite common that organizations use two task sequences. One task sequence for making sure the machines are ready for the upgrade, that silently pre-stages all the required setup files on target computers, and one to do the actual upgrade. This approach ensures that your user productivity is less impacted.

[Create a task sequence to upgrade an OS in Configuration Manager](#)

Semi-annual channel support for feature updates

As announced in September 2018, support timeline for semi-annual channel updates will use the following model.

- All currently supported feature updates of Windows 10 Enterprise and Education, starting with version 1607, will be supported for 30 months from their original release date.
- All future feature updates, starting with 1809, with a targeting September will be supported for 30 months from their release date.
- Future feature updates targeting March and starting with 1903 will continue to be supported for 18 months from their release date.
- Office 365 ProPlus semi-annual updates continue to be supported for 18 months

Additional setup automation options outside of task sequences

If you don't use Upgrade Task Sequences, you can now run custom actions or apply driver files during feature updates in the Pre-install phase – before setup runs its compatibility checks – or in the pre-commit phase – before the upgrade is applied.

Next Step

[Step 8: User Communications and Training](#)

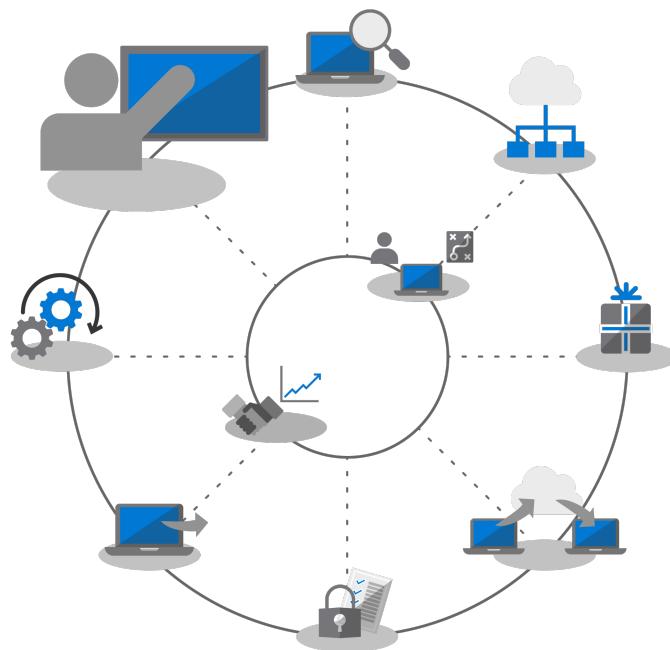
Previous Step

[Step 6 OS Deployment and Feature Updates](#)

Step 8: User Communications and Training

1/18/2019 • 7 minutes to read • [Edit Online](#)

Inform and prepare your users for modern workplace experiences spanning Office 365, Windows 10 and new security and compliance controls with Azure Active Directory and more.



Step 8: User Communication and Training

Make sure your users are informed about new experiences and new ways of working as you shift your PCs to Windows 10 and Office 365 ProPlus. Learn how to take advantage of user adoption assistance with Microsoft FastTrack, training materials and communication templates, as well as new ways to monitor user acceptance and usage.



NOTE

User Communications and Training is the eighth step in our recommended deployment process wheel by covering tips and recommendations to inform and prepare users. To see the full desktop deployment process, visit the [Modern Desktop Deployment Center](#).

The trick here is to figure out how to introduce updates -- when some users may fear disruptions to their productivity or changes in their workflow, or if they have to learn new things.

The good news is if you are moving from Windows 7 and Office 2010 or Office 2013, there will be a lot of people familiar with Windows 10 and newer versions of Office running on their personal devices, and all this will help

reduce the impact of change.

Getting ready for new experiences

Starting with Office, if you're deploying Office 365 ProPlus for the first time, this is when you can communicate the benefits of signing in to Office apps and saving files to OneDrive or SharePoint locations to enable easier sharing, reduce file branching and enable real-time co-authoring.

Detailed communication and training templates are available for these and other local or browser-based apps, like Teams and Planner.

Communicate through chat, meetings, and calls
Teams is a complete chat and online meetings solution. Host audio, video, and web conferences, and chat with anyone inside or outside your organization.
[LEARN MORE >](#)

Collaborate together with integrated Office 365 apps
Teams makes teamwork easy. Coauthor and share files with popular Office 365 apps like Word, Excel, PowerPoint, OneNote, SharePoint, and Power BI.
[START AN INTERACTIVE DEMO >](#)

We also give guidance for new in-app capabilities like attaching OneDrive linked files in Outlook or using the new Morph slide transitions and Designer features in PowerPoint.

For Windows 10, we help you to familiarize your users with optional and default capabilities like Windows Hello to log in securely using biometrics, Start updates to personalize your Windows experience, Timeline to easily get back to what you were working on, Cortana and more.

There are also visible security and compliance controls that your users may be exposed to. Enterprise Mobility + Security which comprises Azure AD and Microsoft Intune, integrates additional capabilities with Windows 10 and Office 365 that you can target for your desktop upgrade.

Microsoft Enterprise Mobility + Security

For example, if you've enabled Multi-factor Authentication, this uses Azure AD --and protects user sign-in to resources by leveraging a phone app or PIN to securely access services. And Azure Information Protection makes it easy for users to classify and label documents.

Set up multi-factor authentication for Office 365 users

These are just a handful of new capabilities that will be experienced by your users and some may catch them by surprise – either in a positive or less positive way. And these surprises – especially if they alter the normal work flow – can result in more calls and tickets for you or your helpdesk.

Proactive Preparation and Measured Roll-outs

To help minimize the risk associated with changes in the user experience, we recommend two complementary

approaches:

- Proactive communication to your users so they know what to expect
- Use of deployment rings to control the rate of deployment

Phased Deployment

Phased deployment using deployment rings is the concept of starting with small groups then broadened deployment scale in a measured way over time. Normally by the time a communication and training plan is drafted, these rings and their members should be formed. This way, you can reduce potential risk and validate your approach as you continually open the deployment valve, or pause activities if needed, for example, when you see more helpdesk calls come in than expected.

Deployment rings are best created in cooperation with business units and their managers. You'll want an understanding of critical dates and times to avoid when deploying or making changes. Without careful planning and buy-in from stakeholders, it will be difficult to get users on-board and comfortable with any changes coming their way.

The screenshot shows the SCCM console with the 'Assets and Compliance' navigation pane selected. In the center, under 'Upgrade Readiness', there is a table titled 'Upgrade Readiness 7 items'. The table has columns for Icon, Name, Limiting Collection, Member Count, Members Visible on Site, and Referenced Collections. One item is highlighted: 'Ready to upgrade in All Workstations' (Icon: blue gear, Name: Ready to upgrade in All Workstations, Limiting Collection: All Workstations, Member Count: 43, Members Visible on Site: 43, Referenced Collections: 0). Below this table, a summary for 'Ready to upgrade in All Workstations' is shown with details: Name: Ready to upgrade in All Workstations, Updated Time: 9/6/2018 9:31 PM, Member Count: 43, Members Visible on Site: 43, Referenced Collections: 0, and Comment: (empty).

Icon	Name	Limiting Collection	Member Count	Members Visible on Site	Referenced Collections
Cannot upgrade in All Workstations	All Workstations	23	23	0	
Incomplete data in All Workstations	All Workstations	3	3	0	
Ready to upgrade in All Workstations	All Workstations	43	43	0	
Ready to upgrade with Inbox driver in All Workstations	All Workstations	3	3	0	
Ready to upgrade with WU driver in All Workstations	All Workstations	3	3	0	
Unknown in All Workstations	All Workstations	2	2	0	
Upgraded in All Workstations	All Workstations	38	38	0	

Phase 1: The IT Team and Early Adopter Insiders

It's usually best to begin your deployment with the IT team and enthusiastic early adopters, who volunteer for early access. With these "insiders" you can test your communications, the impacts of change and the effectiveness of your communications and training. During this phase, IT runs small pilots, learns troubleshooting and automation techniques to help during broader deployment phases.

It's important to have engaged members in the initial pilot phase, to make sure they are documenting their observations and feeding back to the process. Also, it's good to have champions outside the IT team that help extend organic, word-of-mouth communication of new capabilities, and they'll often be first line of support when users in later phases need help.

Phase 2: Pilot

Once you feel good about the first phase, you can target a larger set of users for your second, pilot phase. This should comprise a representative mix of user roles, device types, Windows apps and Office add-ins. The data returning from these groups will be used via Analytics to target the initial waves for phase 3, the broader deployment.

Remember, all PCs in this phase and future phases should be logging up to the Analytics service, so you can collect

telemetry about device and app health as well as bandwidth savings from Delivery Optimization and use of Windows Hello login.

For this phase it is especially important to communicate changes and help users take advantage of new capabilities. Users can often de-prioritize or ignore email or other communications coming from IT – so it helps to meet with management to get their help in communicating change and drive adoption of new tools and technology.

You'll also need their input on timeframes to avoid, so you can minimize user disruption – for example the finance team may be particularly sensitive at the end of fiscal quarters or product development teams during a product launch.

In parallel to planning for devices, users, departments and timing, you can start to build your communication and training plans, as well as begin compiling content or engaging outside resources to help train users.

Microsoft FastTrack

To help your effort in pulling together training content, you can access a comprehensive set of short, video-based training with step-by-step instructional guidance on the Microsoft FastTrack Productivity Library.

[**Microsoft FastTrack Productivity Library**](#)

There are hundreds of topics, based on what's important to your organization, including: creating more impactful content, sharing sites and content, transforming teamwork and unlocking productivity with modern devices.

Also, if you are using Microsoft 365 or Office 365, there is good chance that you're eligible for help with driving user adoption via Microsoft's FastTrack service. Representatives guide you through adoption best practices as you go through the Microsoft 365 – Windows, Office and EMS – rollout process.

Microsoft IT Showcase

Microsoft's IT Showcase series is another great resource for Windows 10 deployment-related content. It includes timelines and schedules, digital promotion templates, email templates and Intranet content. These are based on materials used for Microsoft's own deployment of Windows 10 and has been modified for any organization to use.

[**Preparing your organization for a seamless Windows 10 deployment**](#)

These components and services together can be fine-tuned during the pilot phase. And as you start to realize what's resonating with users on the training side of things, which devices to target and via Analytics and which devices or user groups to avoid or delay, you can begin to broaden your deployment in later phases using a data- and experience-driven approach.

As your pilot expands, you'll want to document and publish frequently asked questions and self-service content to help proactively reduce support tickets and helpdesk activities.

Plan Deploy Support

Timelines and schedules

Microsoft IT mapped out timelines and work-back schedules to provide a solid framework for executing against key milestones. Plans covering readiness communications as well as the actual deployment effort ensured alignment and facilitated adjustments as challenges were encountered.

- > [Readiness communications schedule](#)
- > [Deployment timeline](#)



Digital promotions

Digital and video promotions on the Microsoft intranet, digital office signage, and internal social media channels were developed to excite employees and direct them to additional information about the upgrade experience.

- > [Digital display units](#)
- > [Intranet web banner units](#)
- > [Internal social media units](#)
- > [Windows 10 desktop backgrounds](#)



Step 3 of 7

Email

Microsoft IT sent a series of emails to set employee expectations and ensure successful device upgrades. The first was a company-wide announcement highlighting the deployment process and new features in the upcoming release. The second was personalized for each individual and included critical information about their device, dates for self-driven upgrades, and deadlines after which the device would perform an automatic mandatory upgrade.

- > [Overview email \(all company announcement\)](#)
- > [Personalized email \(details specific to individuals\)](#)

Intranet content

The Microsoft intranet hosted a series of webpages about Windows 10 to serve as the comprehensive source for information relevant to the employee upgrade, including:

- > [Getting started](#)
- > [New features](#)
- > [Application compatibility](#)
- > [Hardware compatibility](#)

Phase 3 and beyond: Broad Production deployment

By the time you reach broad deployment phases, you'll have refined your processes, communication, training and self-service tools. Now you can use data collected via telemetry to target more and more PCs.

Deploy at a rate that is manageable to your IT department, help desk, users and network capacity. You can always go back to Step 2 in the deployment process wheel to optimize your network even further using peer to peer cache, LEDBAT and other techniques to facilitate faster transfer of deployment-related data.

In addition to the telemetry that you monitor via the analytics tools, you can also monitor Office 365 and Microsoft 365 service usage in a granular way with detailed usage reports in by workload in the admin center and using the admin dashboards via Power BI. These are great tools to help set and track goals as you roll-out new tools for working together – like Microsoft Teams – or new ways to share files – like OneDrive.

New technology acceptance and adoption will go on long after every PC in your organization has Windows 10 and Office 365 ProPlus installed. And users won't necessarily change how they work – without taking the time to inform and train them of new capabilities. Finally, with the new servicing models providing new capabilities on an ongoing semi-annual schedule for Windows and optionally a monthly schedule for Office, communication will be continual.

Previous Step

Step 7: Windows and Office Servicing

Modern Desktop Deployment and Management Lab Kit

2/19/2019 • 3 minutes to read • [Edit Online](#)

These downloadable hands-on labs focus on Windows 10 deployment and Office 365 deployment along with the related configuration and management considerations post-deployment. This training is highly recommended for organizations preparing for Windows 7 end of life, but also applies if you're currently using Windows 10 and Office 365 Plus or Office 2019. Included are guides for Windows 10, Office 365 ProPlus, Enterprise Mobility + Security and related products and services.

These labs are designed to help you plan, test and validate your deployment and management of modern desktops running Windows 10 Enterprise and Office 365 ProPlus. The labs cover the steps and tools outlined in the Modern Desktop Deployment wheel, spanning System Center Configuration Manager, Windows Analytics, Office Customization Tool, OneDrive, Windows Autopilot and more.

As part of the [Modern Desktop Deployment](#) process for Windows 10 and Office 365 ProPlus, building a sandboxed or isolated lab environment is the recommended starting point when you begin to explore deployment tool updates and test your deployment-related automation.

The lab kit is free to download and uses trial software.

[Download the Modern Desktop Deployment and Management Lab Kit](#)

A complete lab environment

The lab provides you with an automatically provisioned virtual lab environment, including domain-joined desktop clients, domain controller, Internet gateway and a fully configured ConfigMgr instance. The lab contains Evaluation Versions of the following products:

- Windows 10 Enterprise, Version 1809
- Windows 7
- Office 365 ProPlus, Version 1901
- System Center Configuration Manager, Version 1802
- Windows Assessment and Deployment Kit for Windows 10, Version 1809
- Microsoft Deployment Toolkit
- Microsoft Application Virtualization (App-V) 5.1
- Microsoft BitLocker Administration and Monitoring 2.5 SP1
- Windows Server 2016
- Microsoft SQL Server 2014

PLUS, the lab is designed to be connected to trials for:

- Microsoft 365 Enterprise E5

Or

- Office 365 Enterprise E5
- Enterprise Mobility + Security

Step-by-step labs

Detailed lab guides take you through multiple deployment and management scenarios, including:

Device and App Readiness

- Windows Analytics
- Enterprise Mode and the Enterprise Mode Site List for Internet Explorer

Directory and Network Readiness

- Basic setup for Azure Active Directory and Microsoft 365
- Network optimization using Delivery Optimization, Peer Cache in ConfigMgr and LEDBAT
- ConfigMgr and Microsoft Intune Co-Management
- Remote Access (VPN)

Office and LOB App Delivery

- Office 365 ProPlus deployment using System Center Configuration Manager
- Office 365 ProPlus deployment using Microsoft Intune
- App deployment and management using Microsoft Intune
- App deployment and self-service installation using Microsoft Store for Business
- Desktop Bridge application conversion to UWP
- Windows App Certification Kit
- Browser compatibility remediation using Enterprise Mode for IE

User File and Settings Migration

- User State Migration Tool as part of PC Refresh and Replacement Task Sequences in ConfigMgr and MDT
- OneDrive Known Folder Move
- Enterprise State Roaming

Security and Compliance

- BitLocker device encryption
- Windows Defender Antivirus
- Windows Hello for Business
- BIOS to UEFI conversion as an enabler for virtualization-based security
- Windows Defender Credential Guard
- Windows Defender Application Guard
- Windows Defender Exploit Guard
- Windows Defender Application Control
- Windows Defender Advanced Threat Protection

OS Deployment and Feature Updates

- OS image creation
- OS Deployment Task Sequences in ConfigMgr
 - Bare Metal
 - Refresh
 - Replacement
 - Upgrade
- OS Deployment Task Sequences in MDT
- Feature Updates using Upgrade Task Sequences in ConfigMgr
- Windows Autopilot

Office and Windows as a Service

- Software update management using Configuration Manager

- Office 365 ProPlus update management in Configuration Manager
- Mobile Device Management applied to Windows 10 using Microsoft Intune

Download the Modern Desktop Deployment and Management Lab Kit

Please use a broad bandwidth to download this content to enhance your downloading experience and allow 30-45 minutes for automatic provisioning. The lab environment requires a minimum of 16 GB of available memory and 150 GB of free disk space. For optimal performance, 32 GB of available memory is recommended. The lab expires May 13, 2019. A new version will be published prior to expiration.

Additional guidance

- [Modern Desktop Deployment Center](#)
- [Modern Desktop Deployment series videos from Microsoft Mechanics](#)
- [System Center Configuration Manager OS Deployment](#)
- [Plan for Windows 10 deployment](#)
- [Deployment guide for Office 365 ProPlus](#)
- [Getting Started with Intune](#)

Related resources

- [Introducing Microsoft 365](#)
- [Office 365 for business](#)
- [Introducing Enterprise Mobility + Security](#)
- [Windows 10 for enterprise](#)
- [Windows 10 for small and medium business](#)

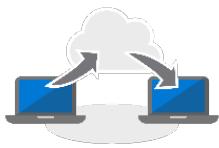
Find help for your Modern Desktop Deployment

12/5/2018 • 2 minutes to read • [Edit Online](#)

If you are planning your Windows 10 deployment with Office 365 ProPlus, there are several options to get additional help from certified Microsoft partners and [Microsoft FastTrack](#).

Below is a map of the available services aligned to the [Modern Desktop Deployment](#) process for Windows 10, Office 365 ProPlus and Enterprise Mobility + Security with existing partner and FastTrack offers. In many cases, these services are included with your qualifying subscription to Microsoft 365, Office 365 or Windows 10 Enterprise. For partner-led services like the Modern Desktop Assessment, as a qualifying organization, Microsoft provides a voucher for services performed by the partner. Details for each offer are found in the links below.

	<p>Device and App Readiness</p> <ul style="list-style-type: none">• Modern Desktop Assessment, where a qualified partner in your region provides your organization with an in-depth application and device compatibility and upgrade readiness assessment using the latest Microsoft tools and procedures.• Desktop App Assure, where Microsoft's FastTrack engineers provide advisory and remediation guidance if you encounter app compatibility issues as you deploy Windows 10 and Office 365 ProPlus or ongoing updates.
	<p>Directory and Network Readiness</p> <ul style="list-style-type: none">• Core onboarding, where Microsoft's FastTrack specialists provide identity integration between your current directory services and Azure Active Directory. This is required for Office 365 ProPlus, Microsoft Intune, OneDrive and other Office 365 and EMS cloud services as part of your desktop deployment.
	<p>Office and LOB App Delivery</p> <ul style="list-style-type: none">• Office 365 ProPlus configuration and deployment, where Microsoft's FastTrack specialists provide assistance with provisioning user licenses, configuring installation and update settings for Click-to-Run and creating packages if your organization uses System Center Configuration Manager.



User File and Settings Migration

- [OneDrive](#) configuration and implementation, where Microsoft's FastTrack specialists provide assistance with provisioning user licenses and configure OneDrive sync client settings. For organizations with eligible subscriptions [FastTrack will migrate data to OneDrive](#).



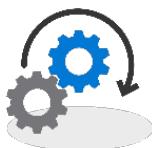
Security and Compliance Considerations

- [Azure AD Premium](#), where Microsoft's FastTrack specialists provide assistance with enabling services to enhance your security and information protection levels as you adopt Microsoft 365. Services include Azure Multi-Factor Authentication, Self Service Password Reset, Azure Active Directory Conditional Access and more. For device and endpoint security Microsoft FastTrack can also assist with [Microsoft Intune](#) provisioning and policies.



OS Deployment and Feature Updates

- [Microsoft Intune](#), where Microsoft's FastTrack specialists provide assistance with provisioning user licenses and configuring Windows Autopilot for new devices, MDM policies for your Windows 10 and other mobile devices, including app deployment; Wi-Fi and VPN profiles; co-management with System Center Configuration Manager and more.



Office and Windows as a Service

- [Microsoft Intune](#), where Microsoft's FastTrack specialists provide assistance with configuring update policies for Windows 10 and Office 365 ProPlus. [Office 365 ProPlus](#) where Microsoft FastTrack can also provide guidance on setting up deployment rings to stay current.



User Communications and Training

- [Productivity Library](#), a set of online resources from Microsoft for end user communication and training across Microsoft 365.
- [Office Training](#), a set of online resources from Microsoft end user training on Office 365 and Office 365 ProPlus.
- [Windows 10 Adoption Planning Kit](#), a set of online resources from Microsoft that includes user readiness assets.

Ask the Tech Community

For specific questions as you plan or start your deployment, join the [Microsoft Tech Community](#)

Related resources

- [Modern Desktop Deployment Center](#)
- [Modern Desktop Deployment series videos from Microsoft Mechanics](#)
- [Modern Desktop Deployment and Management Lab Kit](#)

Identity and device access configurations

12/5/2018 • 9 minutes to read • [Edit Online](#)

This series of articles describes how to configure secure access to cloud services through Enterprise Mobility + Security products by implementing a recommended environment and configuration, including a prescribed set of conditional access policies and related capabilities. You can use this guidance to protect access to all services that are integrated with Azure Active Directory, including Office 365 services, other SaaS services, and on-premises applications published with Azure AD Application Proxy.

These recommendations are aligned with Microsoft Secure Score as well as [identity score in Azure AD](#), and will increase these scores for your organization. These recommendations will also help you implement these [five steps to securing your identity infrastructure](#).

Microsoft understands that some organizations have unique environment requirements or complexities. If you are one of these organizations, use these recommendations as a starting point. However, most organizations can implement these recommendations as prescribed.

Intended audience

These recommendations are intended for enterprise architects and IT professionals who are familiar with [Office 365](#) and [Microsoft Enterprise Mobility + Security](#), which includes, among others, Azure Active Directory (identity), Microsoft Intune (device management), and Azure Information Protection (data protection).

Customer environment

The recommended policies are applicable to enterprise organizations operating both entirely within the Microsoft cloud and for customers with hybrid infrastructure (deployed both on-premises and the Microsoft cloud).

Many of the provided recommendations rely on services available only with Enterprise Mobility + Security (EMS) E5 licenses. Recommendations presented assume full EMS E5 license capabilities.

For those organizations who do not have Enterprise Mobility + Security E5 licenses, Microsoft recommends you at least implement Azure AD baseline protection capabilities that are included with all plans. More information can be found in the article, [What is baseline protection](#), in the Azure AD library.

Caveats

Your organization may be subject to regulatory or other compliance requirements, including specific recommendations that may require you to apply policies that diverge from these recommended configurations. These configurations recommend usage controls that have not historically been available. We recommend these controls, because we believe they represent a balance between security and productivity.

We have done our best to account for a wide variety of organizational protection requirements, but we're not able to account for all possible requirements or for all the unique aspects of your organization.

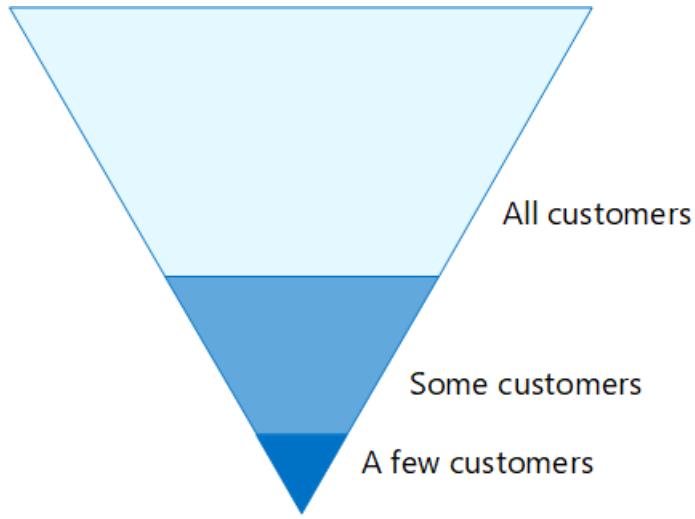
Three tiers of protection

Most organizations have specific requirements regarding security and data protection. These requirements vary by industry segment and by job functions within organizations. For example, your legal department and Office 365 administrators might require additional security and information protection controls around their email correspondence that are not required for other business unit users.

Each industry also has their own set of specialized regulations. Rather than providing a list of all possible security

options or a recommendation per industry segment or job function, recommendations have been provided for three different tiers of security and protection that can be applied based on the granularity of your needs.

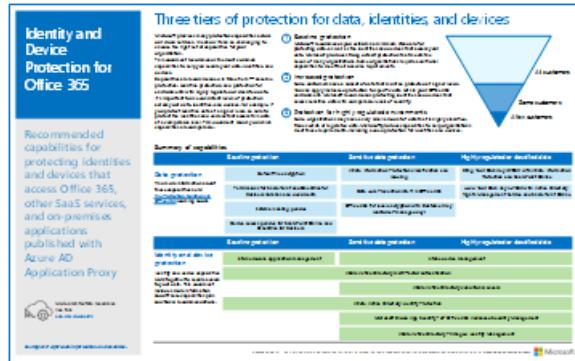
- **Baseline protection:** We recommend you establish a minimum standard for protecting data, as well as the identities and devices that access your data. You can follow these baseline recommendations to provide strong default protection that meets the needs of many organizations.
- **Sensitive protection:** Some customers have a subset of data that must be protected at higher levels, or they may require all data to be protected at a higher level. You can apply increased protection to all or specific data sets in your Office 365 environment. We recommend protecting identities and devices that access sensitive data with comparable levels of security.
- **Highly regulated:** Some organizations may have a small amount of data that is highly classified, constitutes trade secrets, or is regulated data. Microsoft provides capabilities to help organizations meet these requirements, including added protection for identities and devices.



This guidance shows you how to implement protection for identities and devices for each of these tiers of protection. Use this guidance as a starting point for your organization and adjust the policies to meet your organization's specific requirements.

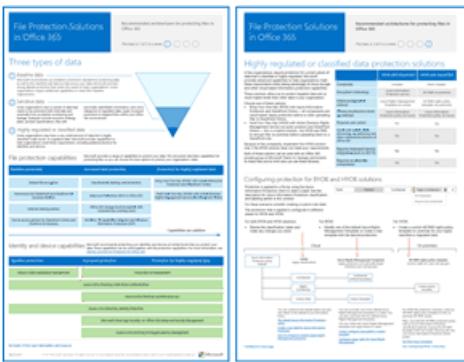
It's important to use consistent levels of protection across your data, identities, and devices. For example, if you implement this guidance, be sure to protect your data at comparable levels. These architecture models show you which capabilities are comparable.

Identity and device protection for Office 365



[PDF](#) | [Visio](#) | [More languages](#)

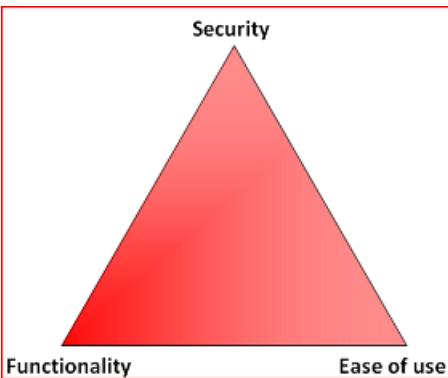
File Protection Solutions in Office 365



[PDF](#) | [Visio](#)

Security and productivity trade-offs

Implementing any security strategy requires trade-offs between security and productivity. It's helpful to evaluate how each decision affects the balance of security, functionality, and ease of use.



The recommendations provided are based on the following principles:

- Know your audience and be flexible to their security and functional requirements.
- Apply a security policy just in time and ensure it is meaningful.

Services and concepts for identity and device access protection

Microsoft 365 Enterprise is designed for large organizations and integrates Office 365 Enterprise, Windows 10 Enterprise, and Enterprise Mobility + Security (EMS), to empower everyone to be creative and work together securely.

This section provides an overview of the Microsoft 365 services and capabilities that are important for identity and device access.

Microsoft Azure Active Directory

Azure AD provides a full suite of identity management capabilities. For securing access we recommend using the following capabilities:

- **Self-service password reset (SSPR)**: Allow your users to reset their passwords securely and without helpdesk intervention, by providing verification of multiple authentication methods that the administrator can control.
- **Multi-factor authentication (MFA)**: MFA requires users to provide two forms of verification, such as a user password plus a notification from the Microsoft Authenticator app or a phone call. MFA greatly reduces the risk that a stolen identity can be used to access your Office 365 environment.
- **Conditional access**: Azure AD evaluates the conditions of the user login and uses conditional access policies you create to allow access. For example, in this guidance we show you how to create a conditional access policy to require device compliance for access to sensitive data. This greatly reduces the risk that a

hacker with a stolen identity can access your sensitive data. It also protects sensitive data on the devices, because the devices meet specific requirements for health and security.

- **Azure AD groups:** Conditional access rules, device management with Intune, and even permissions to files and sites in your organization, rely on assignment to user and/or Azure AD groups. We recommend you create Azure AD groups that correspond to the levels of protection you are implementing. For example, your executive staff are likely higher value targets for hackers. Therefore, it makes sense to assign these employees to an Azure AD group and assign this group to conditional access policies and other policies that enforce a higher level of protection for access.
- **Device registration:** You register a device into Azure AD to provide an identity to the device. This identity is used to authenticate the device when a user signs in and to apply conditional access rules that require domain-joined or compliant PCs. For this guidance, we use device registration to automatically register domain-joined Windows computers. Device registration is a prerequisite for managing devices with Intune.
- **Azure AD Identity Protection:** Azure AD Identity Protection enables you to detect potential vulnerabilities affecting your organization's identities and configure automated remediation policy to low, medium, and high sign-in risk and user risk. This guidance relies on this risk evaluation to apply conditional access policies for multi-factor authentication. This guidance also includes a conditional access policy that requires users to change their password if high-risk activity is detected for their account.

Microsoft Intune

[Intune](#) is Microsoft's cloud-based mobile device management service. This guidance recommends device management of Windows PCs with Intune and recommends device compliance policy configurations. Intune determines whether devices are compliant and sends this data to Azure AD to use when applying conditional access policies.

Intune app protection

[Intune app protection](#) policies can be used to protect your organization's data in mobile apps, with or without enrolling devices into management. Intune helps protect Office 365 information, making sure your employees can still be productive, and preventing data loss. By implementing app-level policies, you can restrict access to company resources and keep data within the control of your IT department.

This guidance shows you how to create recommended policies to enforce the use of approved apps and to determine how these apps can be used with your business data.

Office 365

This guidance shows you how to implement a set of policies to protect access to Office 365, including Exchange Online, SharePoint Online, and OneDrive for Business. In addition to implementing these policies, we recommend you also raise the level of protection for your Office 365 tenant using these resources:

- [Configure your Office 365 tenant for increased security](#): These recommendations apply to baseline security for your Office 365 tenant.
- [Office 365 security roadmap: Top priorities for the first 30 days, 90 days, and beyond](#): These recommendations include logging, data governance, admin access, and threat protection.
- [Secure SharePoint Online sites and files](#): This set of articles describes how to protect files and sites at appropriate levels for baseline, sensitive, and highly confidential protection.

Windows 10 and Office 365 ProPlus

Windows 10 and Office 365 ProPlus is the recommended client environment for PCs. We recommend Windows 10, as Azure is designed to provide the smoothest experience possible for both on-premises and Azure AD. Windows 10 also includes advanced security capabilities that can be managed through Intune. Office 365 ProPlus includes the latest versions of Office applications. These use modern authentication, which is more secure and a requirement for conditional access. These apps also include enhanced security and compliance

tools.

Applying these capabilities across the three tiers of protection

The following table summarizes our recommendations for using these capabilities across the three tiers of protection.

PROTECTION MECHANISM	BASELINE	SENSITIVE	HIGHLY REGULATED
Enforce MFA	On medium or above sign-in risk	On low or above sign-in risk	On all new sessions
Enforce password change	For high-risk users	For high-risk users	For high-risk users
Enforce Intune application protection	Yes	Yes	Yes
Enforce Intune enrollment (COD)	Require a compliant or domain-joined PC, but allow BYOD phones/tablets	Require a compliant or domain-joined device	Require a compliant or domain-joined device

Device ownership

The above table reflects the trend for many organizations to support a mix of corporate-owned devices, as well as personal or bring-your-own devices (BYODs) to enable mobile productivity across the workforce. Intune app protection policies ensure that email is protected from exfiltrating out of the Outlook mobile app and other Office mobile apps, on both corporate-owned devices and BYODs.

We recommend corporate-owned devices be managed by Intune or domain-joined to apply additional protections and control. Depending on data sensitivity, your organization may choose to not allow BYODs for specific user populations or specific apps.

Next steps

[Prerequisite work for implementing identity and device access policies](#)

Prerequisite work for implementing identity and device access policies

12/5/2018 • 6 minutes to read • [Edit Online](#)

This article describes prerequisites that need to be implemented before you can deploy the recommended identity and device access policies. This article also discusses the default platform client configurations we recommend to provide the best SSO experience to your users, as well as the technical prerequisites for conditional access.

Prerequisites

Before implementing the recommended identity and device access policies, there are several prerequisites that your organization must meet. The following table details the prerequisites that apply to your environment.

Configuration	Cloud Only	Active Directory with Password Hash Sync	Pass-Through Authentication	Federation with ADFS
Configure Password Hash Sync . This must be enabled to detect leaked credentials and to act on them for risk-based conditional access. Note: This is required regardless of whether your organization uses managed authentication, like pass-through authentication (PTA), or federated authentication.		Yes	Yes	Yes
Enable seamless single sign on to automatically sign users in when they are on their corporate devices connected to your corporate network.		Yes	Yes	

CONFIGURATION	CLOUD ONLY	ACTIVE DIRECTORY WITH PASSWORD HASH SYNC	PASS-THROUGH AUTHENTICATION	FEDERATION WITH AD FS
Configure named networks. Azure AD Identity Protection collects and analyzes all available session data to generate a risk score. We recommend you specify your organization's public IP ranges for your network in the Azure AD named networks configuration. Traffic coming from these ranges is given a reduced risk score, and traffic from outside the corporate environment is given a higher risk score.	Yes	Yes	Yes	Yes
Register all users for self-service password reset (SSPR) and multi-factor authentication (MFA). We recommend you register users for Azure MFA ahead of time. Azure AD Identity Protection makes use of Azure MFA to perform additional security verification. Additionally, for the best sign-in experience, we recommend users install the Microsoft Authenticator app and the Microsoft Company Portal app on their devices. These can be installed from the app store for each platform.	Yes	Yes	Yes	Yes

CONFIGURATION	CLOUD ONLY	ACTIVE DIRECTORY WITH PASSWORD HASH SYNC	PASS-THROUGH AUTHENTICATION	FEDERATION WITH AD FS
<p>Enable automatic device registration of domain-joined Windows computers. Conditional access will make sure devices connecting to apps are domain-joined or compliant. To support this on Windows computers, the device must be registered with Azure AD. This article discusses how to configure automatic device registration.</p>		Yes	Yes	Yes
<p>Prepare your support team. Have a plan in place for users that cannot complete MFA. This could be adding them to a policy exclusion group, or registering new MFA information for them. Before making either of these security-sensitive changes, you need to ensure that the actual user is making the request. Requiring users' managers to help with the approval is an effective step.</p>	Yes	Yes	Yes	Yes

Configuration	Cloud Only	Active Directory with Password Hash Sync	Pass-Through Authentication	Federation with AD FS
<p>Configure password writeback to on-premises AD.</p> <p>Password writeback allows Azure AD to require that users change their on-premises passwords when a high-risk account compromise is detected. You can enable this feature using Azure AD Connect in one of two ways: either enable Password Writeback in the optional features screen of the Azure AD Connect setup wizard, or enable it via Windows PowerShell.</p>		Yes	Yes	Yes
<p>Enable Azure Active Directory Identity Protection. Azure AD Identity Protection enables you to detect potential vulnerabilities affecting your organization's identities and configure an automated remediation policy to low, medium, and high sign-in risk and user risk.</p>	Yes	Yes	Yes	Yes
<p>Enable modern authentication for Exchange Online and for Skype for Business Online.</p> <p>Modern authentication is a prerequisite for using multi-factor authentication (MFA). Modern authentication is enabled by default for Office 2016 clients, SharePoint Online, and OneDrive for Business.</p>	Yes	Yes	Yes	Yes

Recommended client configurations

This section describes the default platform client configurations we recommend to provide the best SSO experience to your users, as well as the technical prerequisites for conditional access.

Windows devices

We recommend the Windows 10 (version 1703 or later), as Azure is designed to provide the smoothest SSO experience possible for both on-premises and Azure AD. Work or school-issued devices should be configured to join Azure AD directly or if the organization uses on-premises AD domain join, those devices should be [configured to automatically and silently register with Azure AD](#).

For BYOD Windows devices, users can use **Add work or school account**. Note that Chrome-browser users on Windows 10 need to [install an extension](#) to get the same smooth sign-in experience as Edge/IE users. Also, if your organization has domain-joined Windows 7 devices, you can install Microsoft Workplace Join for non-Windows 10 computers [Download the package to register](#) the devices with Azure AD.

iOS devices

We recommend installing the [Microsoft Authenticator app](#) on user devices before deploying conditional access or MFA policies. At a minimum, the app should be installed when users are asked to register their device with Azure AD by adding a work or school account, or when they install the Intune company portal app to enroll their device into management. This depends on the configured conditional access policy.

Android devices

We recommend users install the [Intune Company Portal app](#) and [Microsoft Authenticator app](#) before conditional access policies are deployed or when required during certain authentication attempts. After app installation, users may be asked to register with Azure AD or enroll their device with Intune. This depends on the configured conditional access policy.

We also recommend that corporate-owned devices (COD) are standardized on OEMs and versions that support Android for Work or Samsung Knox to allow mail accounts, be managed and protected by Intune MDM policy.

Recommended email clients

The following email clients support modern authentication and conditional access.

PLATFORM	CLIENT	VERSION/NOTES
Windows	Outlook	2016, 2013 Enable modern authentication , Required updates
iOS	Outlook for iOS	Latest
Android	Outlook for Android	Latest
macOS	Outlook	2016
Linux	Not supported	

Recommended client platforms when securing documents

The following clients are recommended when a secure documents policy has been applied.

Platform	Word/Excel/PowerPoint	OneNote	OneDrive App	SharePoint App	OneDrive Sync Client
Windows 7	Supported	Supported	N/A	N/A	Preview*
Windows 8.1	Supported	Supported	N/A	N/A	Preview*
Windows 10	Supported	Supported	N/A	N/A	Preview*
Windows Phone 10	Not supported	Not supported	Not Supported	Not Supported	Not Supported
Android	Supported	Supported	Supported	Supported	N/A
iOS	Supported	Supported	Supported	Supported	N/A
macOS	Public Preview	Public Preview	N/A	N/A	Not supported
Linux	Not supported	Not supported	Not supported	Not supported	Not supported

* Learn more about using conditional access with the [OneDrive sync client](#).

Office 365 client support

For more information about Office 365 client support, see the following articles:

- [Office 365 Client App Support - Conditional Access](#)
- [Office 365 Client App Support - Mobile Application Management](#)
- [Office 365 Client App Support - Modern Authentication](#)

Protecting administrator accounts

Azure AD provides a simple way for you to begin protecting administrator access with a preconfigured conditional access policy. In Azure AD, go to **Conditional access** and look for this policy — **Baseline policy: Require MFA for admins**. Select this policy and then select **Use policy immediately**.

This policy requires MFA for the following roles:

- Global administrators
- SharePoint administrators
- Exchange administrators
- Conditional access administrators
- Security administrators

For more information, see [Baseline security policy for Azure AD admin accounts](#).

Additional recommendations include the following:

- Use Azure AD Privileged Identity Management to reduce the number of persistent administrative accounts. See [Start using PIM](#).
- [Use privileged access management in Office 365](#) to protect your organization from breaches that may use existing privileged admin accounts with standing access to sensitive data or access to critical configuration settings.
- Use Office 365 administrator accounts only for administration. Admins should have a separate user account for regular non-administrative use and only use their administrative account when necessary to complete a task associated with their job function. [Office 365 administrator roles](#) have substantially more privileges than

Office 365 services.

- Follow best practices for securing privileged accounts in Azure AD as described in this [article](#).

Next steps

[Configure the common identity and device access policies](#)

Common identity and device access policies

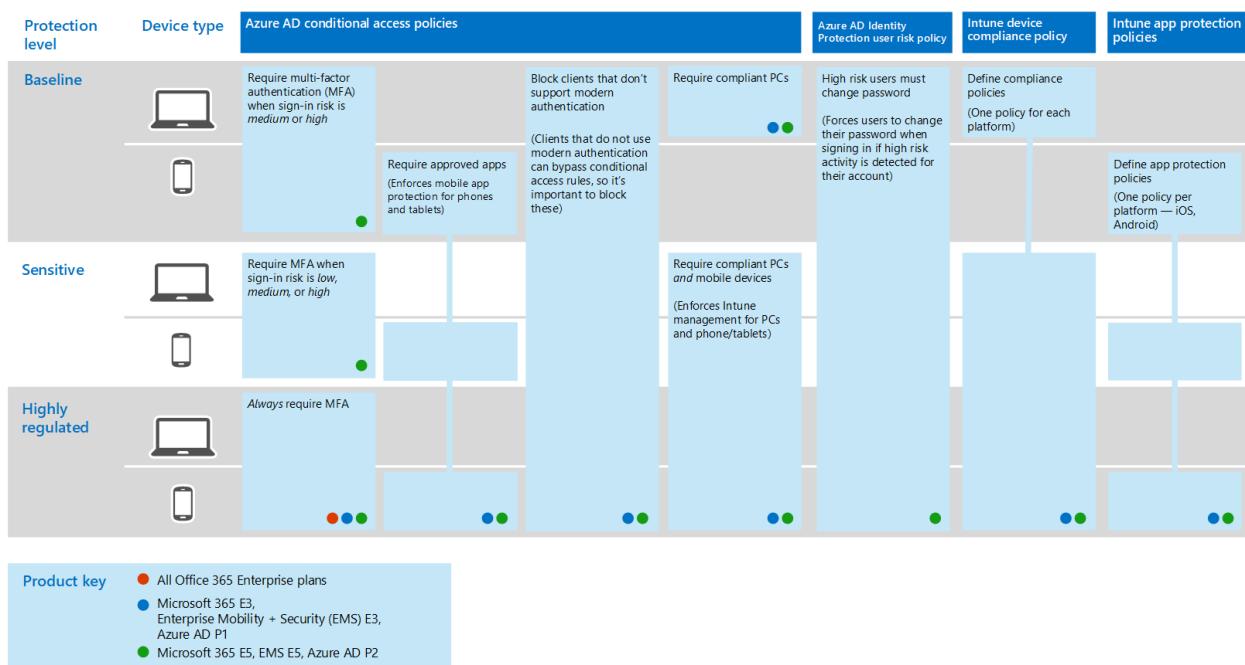
12/5/2018 • 19 minutes to read • [Edit Online](#)

This article describes the common recommended policies for securing access to cloud services, including on-premises applications published with Azure AD Application Proxy.

This guidance discusses how to deploy the recommended policies in a newly-provisioned environment. Setting up these policies in a separate lab environment allows you to understand and evaluate the recommended policies before staging the rollout to your preproduction and production environments. Your newly provisioned environment may be cloud-only or hybrid.

Policy set

The following diagram illustrates the recommended set of policies. It shows which tier of protections each policy applies to and whether the policies apply to PCs or phones and tablets, or both categories of devices. It also indicates where these policies are configured.



The rest of this article describes how to configure these policies.

Using multi-factor authentication is recommended before enrolling devices into Intune for assurance that the device is in the possession of the intended user. You must also enroll devices into Intune before enforcing device compliance policies.

To give you time to accomplish these tasks, we recommend implementing the baseline policies in the order listed in this table. However, the MFA policies for sensitive and highly regulated protection can be implemented at any time.

PROTECTION LEVEL	POLICIES	MORE INFORMATION
Baseline	Require MFA when sign-in risk is medium or high	

PROTECTION LEVEL	POLICIES	MORE INFORMATION
	Block clients that don't support modern authentication	Clients that do not use modern authentication can bypass conditional access rules, so it's important to block these
	High risk users must change password	Forces users to change their password when signing in if high-risk activity is detected for their account
	Define app protection policies	One policy per platform (iOS, Android, Windows).
	Require approved apps	Enforces mobile app protection for phones and tablets
	Define device compliance policies	One policy for each platform
	Require compliant PCs	Enforces Intune management of PCs
Sensitive	Require MFA when sign-in risk is <i>low, medium or high</i>	
	Require compliant PCs <i>and</i> mobile devices	Enforces Intune management for PCs and phone/tablets
Highly regulated	Always require MFA	

Assigning policies to users

Before configuring policies, identify the Azure AD groups you are using for each tier of protection. Typically, baseline protection applies to everybody in the organization. A user who is included for both baseline and sensitive protection will have all the baseline policies applied plus the sensitive policies. Protection is cumulative and the most restrictive policy is enforced.

A recommended practice is to create an Azure AD group for conditional access exclusion. Add this group to all of your conditional access rules under "Exclude". This gives you a method to provide access to a user while you troubleshoot access issues. This is recommended as a temporary solution only. Monitor this group for changes and be sure the exclusion group is being used only as intended.

The following diagram provides an example of user assignment and exclusions.

Protection level	Azure AD conditional access policies	Include	Exclude
Baseline	Require multi-factor authentication (MFA) when sign-in risk is <i>medium or high</i>	All users	Conditional access exclusion group
Sensitive	Require MFA when sign-in risk is <i>low, medium, or high</i>	Executive staff	Conditional access exclusion group
Highly regulated	Always require MFA	Top secret project X team	Conditional access exclusion group

In the illustration the "Top secret project X team" is assigned a conditional access policy that requires MFA *always*. Be judicious when applying higher levels of protection to users. Members of this project team will be required to provide two forms of authentication every time they log on, even if they are not viewing highly-regulated content.

All Azure AD groups created as part of these recommendations must be created as Office 365 groups. This is specifically important for the deployment of Azure Information Protection (AIP) when securing documents in SharePoint Online.

The screenshot shows the 'Group' creation interface. At the top, there's a title bar with 'Group' and close/cancel buttons. Below it, there are four input fields with validation stars:

- Group type:** A dropdown menu set to 'Office 365'.
- Group name:** A text input field with placeholder text 'Enter the name of the group'.
- Group description:** A text input field with placeholder text 'Enter a description for the group'.
- Membership type:** A dropdown menu.

Require MFA based on sign-in risk

Before requiring MFA, first use an Identity Protection MFA registration policy to register users for MFA. After users are registered you can enforce MFA for sign-in. The [prerequisite work](#) includes registering all users with MFA.

To create a new conditional access policy:

1. Go to the [Azure portal](#), and sign in with your credentials. After you've successfully signed in, you see the Azure dashboard.
2. Choose **Azure Active Directory** from the left menu.
3. Under the **Security** section, choose **Conditional access**.

4. Choose **New policy**.

The following tables describes the conditional access policy settings to implement for this policy.

Assignments

TYPE	PROPERTIES	VALUES	NOTES
Users and groups	Include	Select users and groups – Select specific security group containing targeted users	Start with security group including pilot users
	Exclude	Exception security group; service accounts (app identities)	Membership modified on an as-needed temporary basis
Cloud apps	Include	Select the apps you want this rule to apply to. For example, select Office 365 Exchange Online	
Conditions	Configured	Yes	Configure specific to your environment and needs
Sign-in risk	Risk level		See the guidance in the following table

Sign-in risk

Apply the settings based on the protection level you are targeting.

PROPERTY	LEVEL OF PROTECTION	VALUES	NOTES
Risk level	Baseline	High, medium	Check both
	Sensitive	High, medium, low	Check all three
	Highly regulated		Leave all options unchecked to always enforce MFA

Access controls

Type	Properties	Values	Notes
Grant	Grant access	True	Selected
	Require MFA	True	Check
	Require device to be marked as compliant	False	
	Require hybrid Azure AD-joined device	False	
	Require approved client app	False	
	Require all the selected controls	True	Selected

NOTE

Be sure to enable this policy, by choosing **On**. Also consider using the [What if](#) tool to test the policy.

Block clients that don't support modern authentication

1. Go to the [Azure portal](#), and sign in with your credentials. After you've successfully signed in, you see the Azure dashboard.
2. Choose **Azure Active Directory** from the left menu.
3. Under the **Security** section, choose **Conditional access**.
4. Choose **New policy**.

The following tables describes the conditional access policy settings to implement for this policy.

Assignments

Type	Properties	Values	Notes
Users and groups	Include	Select users and groups – Select specific security group containing targeted users	Start with security group including pilot users
	Exclude	Exception security group; service accounts (app identities)	Membership modified on an as needed temporary basis
Cloud apps	Include	Select the apps you want this rule to apply to. For example, select Office 365 Exchange Online	
Conditions	Configured	Yes	Configure Client apps

Type	Properties	Values	Notes
Client apps	Configured	Yes	Mobile apps and desktop clients, Other clients (select both)

Access controls

Type	Properties	Values	Notes
Grant	Block access	True	Selected
	Require MFA	False	
	Require device to be marked as compliant	False	
	Require hybrid Azure AD-joined device	False	
	Require approved client app	False	
	Require all the selected controls	True	Selected

Note

Be sure to enable this policy, by choosing **On**. Also consider using the [What if](#) tool to test the policy.

High risk users must change password

To ensure that all high-risk users' compromised accounts are forced to perform a password change when signing-in, you must apply the following policy.

Log in to the [Microsoft Azure portal](http://portal.azure.com) (<http://portal.azure.com>) with your administrator credentials, and then navigate to **Azure AD Identity Protection > User Risk Policy**.

Assignments

Type	Properties	Values	Notes
Users	Include	All users	Selected
	Exclude	None	
Conditions	User risk	High	Selected

Controls

Type	Properties	Values	Notes
	Access	Allow access	True

TYPE	PROPERTIES	VALUES	NOTES
	Access	Require password change	True

Review: not applicable

NOTE

Be sure to enable this policy, by choosing **On**. Also consider using the [What if](#) tool to test the policy

Define app protection policies

App protection policies define which apps are allowed and the actions they can take with your organization's data. Create Intune app protection policies from within the Azure portal.

Create a policy for each platform:

- iOS
- Android
- Windows 10

To create a new app protection policy, log in to the Microsoft Azure portal with your administer credentials, and then navigate to **Mobile apps > App protection policies**. Choose **Add a policy**.

There are slight differences in the app protection policy options between iOS and Android. The below policy is specifically for Android. Use this as a guide for your other policies.

The recommended list of apps includes the following:

- PowerPoint
- Excel
- Word
- Microsoft Teams
- Microsoft SharePoint
- Microsoft Visio Viewer
- OneDrive
- OneNote
- Outlook

The following tables describe the recommended settings:

TYPE	PROPERTIES	VALUES	NOTES
Data relocation	Prevent Android backup	Yes	On iOS this will specifically call out iTunes and iCloud
	Allow app to transfer data to other apps	Policy managed apps	
	Allow app to receive data from other apps	Policy managed apps	
	Prevent "Save As"	Yes	

Type	Properties	Values	Notes
	Select which storage services corporate data can be saved to	OneDrive for Business, SharePoint	
	Restrict cut, copy, and paste with other apps	Policy managed apps with paste in	
	Restrict web content to display in the managed browser	No	
	Encrypt app data	Yes	On iOS select option: When device is locked
	Disable app encryption when device is enabled	Yes	Disable this setting to avoid double encryption
	Disable contacts sync	No	
	Disable printing	No	
Access	Require PIN for access	Yes	
	Select Type	Numeric	
	Allow simple PIN	No	
	PIN length	6	
	Allow fingerprint instead of PIN	Yes	
	Disable app PIN when device PIN is managed	Yes	
	Require corporate credentials for access	No	
	Recheck the access requirement after (minutes)	30	
	Block screen capture and Android assistant	No	On iOS this is not an available option
Sign-in security requirements	Max PIN attempts	5	Reset Pin
	Offline grace period	720	Block access
	Offline interval (days) before app data is wiped	90	Wipe data
	Jailbroken/rooted devices		Wipe data

When complete, remember to select "Create". Repeat the above steps and replace the selected platform (dropdown) with iOS. This creates two app policies, so once you create the policy, then assign groups to the policy and deploy it.

To edit the policies and assign these policies to users, see [How to create and assign app protection policies](#).

Require approved apps

To require approved apps:

1. Go to the [Azure portal](#), and sign in with your credentials. After you've successfully signed in, you see the Azure dashboard.
2. Choose **Azure Active Directory** from the left menu.
3. Under the **Security** section, choose **Conditional access**.
4. Choose **New policy**.
5. Enter a policy name, then choose the **Users and groups** you want to apply the policy for.
6. Choose **Cloud apps**.
7. Choose **Select apps**, select the desired apps from the **Cloud apps** list. For example, select Office 365 Exchange Online. Choose **Select** and **Done**.
8. Choose **Grant** from the **Access controls** section.
9. Choose **Grant access**, select **Require approved client app**. For multiple controls, select **Require the selected controls**, then choose **Select**.
10. Choose **Create**.

Define device-compliance policies

Device-compliance policies define the requirements that devices must adhere to in order to be marked as compliant. Create Intune device compliance policies from within the Azure portal.

Create a policy for each platform:

- Android
- Android enterprise
- iOS
- macOS
- Windows Phone 8.1
- Windows 8.1 and later
- Windows 10 and later

To create device compliance policies, log in to the Microsoft Azure portal with your administer credentials, and then navigate to **Intune > Device compliance**. Select **Create policy**.

The following settings are recommended for Windows 10.

Device health: Windows Health Attestation Service evaluation rules

PROPERTIES	VALUES	NOTES
Require BitLocker	Require	

Properties	Values	Notes
Require Secure Boot to be enabled on the device	Require	
Require code integrity	Require	

Device properties

Type	Properties	Values	Notes
Operating system version	All	Not configured	

For all the above policies to be considered deployed, they must be targeted at user groups. You can do this by creating the policy (on Save) or later by selecting **Manage Deployment** in the **Policy** section (same level as Add).

System security

Type	Properties	Values	Notes
Password	Require a password to unlock mobile devices	Require	
	Simple passwords	Block	
	Password type	Device default	
	Minimum password length	6	
	Maximum minutes of inactivity before password is required	15	This setting is supported for Android versions 4.0 and above or KNOX 4.0 and above. For iOS devices, it's supported for iOS 8.0 and above
	Password expiration (days)	41	
	Number of previous passwords to prevent reuse	5	
	Require password when device returns from idle state (Mobile and Holographic)	Require	Available for Windows 10 and later
Encryption	Encryption of data storage on device	Require	
Device Security	Firewall	Require	
	Antivirus	Require	

TYPE	PROPERTIES	VALUES	NOTES
	Antispyware	Require	This setting requires an Anti-Spyware solution registered with Windows Security Center
Defender	Windows Defender Antimalware	Require	
	Windows Defender Antimalware minimum version		Only supported for Windows 10 desktop. Microsoft recommends versions no more than five behind from the most recent version
	Windows Defender Antimalware signature up to date	Require	
	Real-time protection	Require	Only supported for Windows 10 desktop

Windows Defender ATP

TYPE	PROPERTIES	VALUES	NOTES
Windows Defender Advanced Threat Protection rules	Require the device to be at or under the machine-risk score	Medium	

Require compliant PCs (but not compliant phones and tablets)

Before adding a policy to require compliant PCs, be sure to enroll devices for management into Intune. Using multi-factor authentication is recommended before enrolling devices into Intune for assurance that the device is in the possession of the intended user.

To require compliant PCs:

1. Go to the [Azure portal](#), and sign in with your credentials. After you've successfully signed in, you see the Azure dashboard.
2. Choose **Azure Active Directory** from the left menu.
3. Under the **Security** section, choose **Conditional access**.
4. Choose **New policy**.
5. Enter a policy name, then choose the **Users and groups** you want to apply the policy for.
6. Choose **Cloud apps**.
7. Choose **Select apps**, select the desired apps from the **Cloud apps** list. For example, select Office 365 Exchange Online. Choose **Select** and **Done**.
8. To require compliant PCs, but not compliant phones and tablets, choose **Conditions** and **Device platforms**. Choose **Select device platforms** and select **Windows** and **macOS**.

9. Choose **Grant** from the **Access controls** section.
10. Choose **Grant access**, select **Require device to be marked as compliant**. For multiple controls, select **Require all the selected controls**, then choose **Select**.
11. Choose **Create**.

If your objective is to require compliant PCs *and* mobile devices, do not select platforms. This enforces compliance for all devices.

Require compliant PCs *and* mobile devices

To require compliance for all devices:

1. Go to the [Azure portal](#), and sign in with your credentials. After you've successfully signed in, you see the Azure dashboard.
2. Choose **Azure Active Directory** from the left menu.
3. Under the **Security** section, choose **Conditional access**.
4. Choose **New policy**.
5. Enter a policy name, then choose the **Users and groups** you want to apply the policy for.
6. Choose **Cloud apps**.
7. Choose **Select apps**, select the desired apps from the **Cloud apps** list. For example, select Office 365 Exchange Online. Choose **Select** and **Done**.
8. Choose **Grant** from the **Access controls** section.
9. Choose **Grant access**, select **Require device to be marked as compliant**. For multiple controls, select **Require all the selected controls**, then choose **Select**.
10. Choose **Create**.

When creating this policy, do not select platforms. This enforces compliant devices.

Next steps

[Learn about policy recommendations for securing email](#)

Policy recommendations for securing email

12/5/2018 • 14 minutes to read • [Edit Online](#)

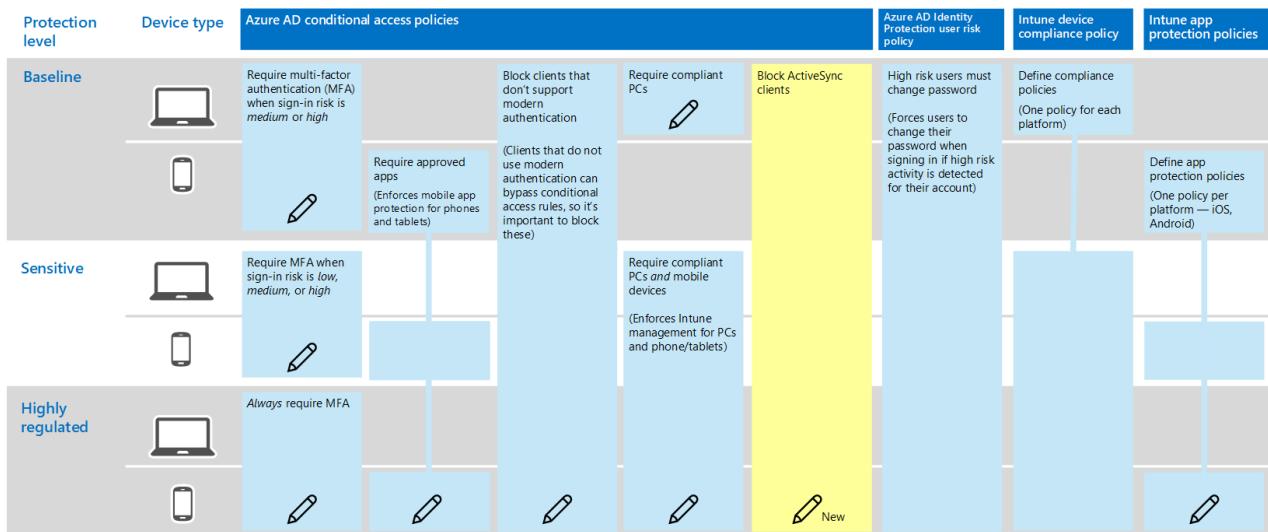
This article describes how to implement the recommended identity and device access policies to protect organizational email and email clients that support modern authentication and conditional access. This guidance builds on the [Common identity and device access policies](#) and also includes a few additional recommendations.

These recommendations are based on three different tiers of security and protection that can be applied based on the granularity of your needs: **baseline**, **sensitive**, and **highly regulated**. You can learn more about these security tiers, and the recommended client operating systems, referenced by these recommendations in the [recommended security policies and configurations introduction](#).

These recommendations require your users to use modern email clients, including Outlook for iOS and Android on mobile devices. Outlook for iOS and Android provide support for the best features of Office 365. These mobile Outlook apps are also architected with security capabilities that support mobile use and work together with other Microsoft cloud security capabilities. For more information, see [Outlook for iOS and Android FAQ](#).

Updating common policies to include email

The following diagram illustrates the common identity and device access policies and indicates which policies need to be updated to protect email. Note the addition of a new rule for Exchange Online to block ActiveSync clients. This forces the use of Outlook mobile.



If you included Exchange Online and Outlook in the scope of the policies when you set them up, you only need to create the new policy to block ActiveSync clients. Review the policies listed in the following table and either make the recommended additions, or confirm that these are already included. Each rule links to the associated configuration instructions in the [Common identity and device access policies](#) article.

PROTECTION LEVEL	POLICIES	MORE INFORMATION
Baseline	Require MFA when sign-in risk is medium or high Block clients that don't support modern authentication	Include Exchange Online in the assignment of cloud apps
		Include Exchange Online in the assignment of cloud apps

PROTECTION LEVEL	POLICIES	MORE INFORMATION
	Define app protection policies	Be sure Outlook is included in the list of apps. Be sure to update the policy for each platform (iOS, Android, Windows)
	Require approved apps	Include Exchange Online in the list of cloud apps
	Require compliant PCs	Include Exchange Online in list of cloud apps
	Block ActiveSync clients	Add this new policy
Sensitive	Require MFA when sign-in risk is <i>low, medium or high</i>	Include Exchange Online in the assignment of cloud apps
	Require compliant PCs <i>and</i> mobile devices	Include Exchange Online in the list of cloud apps
Highly regulated	Always require MFA	Include Exchange Online in the assignment of cloud apps

Block ActiveSync clients

This policy prevents ActiveSync clients from bypassing other conditional access rules. The rule configuration applies only to ActiveSync clients. By selecting **Require approved client app**, this policy blocks ActiveSync clients. To configure this policy:

1. Go to the [Azure portal](#), and sign in with your credentials. After you've successfully signed in, you see the Azure dashboard.
2. Choose **Azure Active Directory** from the left menu.
3. Under the **Security** section, choose **Conditional access**.
4. Choose **New policy**.
5. Enter a policy name, then choose the **Users and groups** you want to apply the policy for.
6. Choose **Cloud apps**.
7. Choose **Select apps**, select **Office 365 Exchange Online**. Choose **Select** and **Done**.
8. Choose **Conditions**, and then choose **Client apps**.
9. For **Configure**, select **Yes**. Check only the following: **Mobile apps and desktop clients** and **Exchange ActiveSync clients**. Choose **Done**.
10. Choose **Grant** from the **Access controls** section.
11. Choose **Grant access**, select **Require approved client app**. For multiple controls, select **Require the selected controls**, then choose **Select**.
12. Choose **Create**.

Setup Office 365 message encryption

With the new Office 365 Message Encryption (OME) capabilities, which leverage the protection features in Azure

Information Protection, your organization can easily share protected email with anyone on any device. Users can send and receive protected messages with other Office 365 organizations as well as non-Office 365 customers using Outlook.com, Gmail, and other email services.

For more information, see [Set up new Office 365 Message Encryption capabilities](#).

Next steps

[Learn about policy recommendations for securing SharePoint Sites and files](#)

Policy recommendations for securing SharePoint sites and files

12/5/2018 • 5 minutes to read • [Edit Online](#)

This article describes how to implement the recommended identity and device-access policies to protect SharePoint Online and OneDrive for Business. This guidance builds on the [Common identity and device access policies](#).

These recommendations are based on three different tiers of security and protection for SharePoint files that can be applied based on the granularity of your needs: **baseline**, **sensitive**, and **highly regulated**. You can learn more about these security tiers, and the recommended client operating systems, referenced by these recommendations in the [the overview](#).

In addition to implementing this guidance, be sure to configure SharePoint sites with the right amount of protection, including setting appropriate permissions for sensitive and highly-regulated content. For more information on creating sites for baseline, sensitive, and highly-regulated protection, see [Secure SharePoint Online sites and files](#).

Updating common policies to include SharePoint and OneDrive for Business

The following diagram illustrates the set of recommended policies for protecting files in SharePoint Online and OneDrive for Business. It indicates which policies should be updated or newly created to add protection for SharePoint Online and OneDrive for Business.

Protection level	Device type	Azure AD conditional access policies		Azure AD Identity Protection user risk policy	Intune device compliance policy	Intune app protection policies	SharePoint device access policies
Baseline	 	Require multi-factor authentication (MFA) when sign-in risk is medium or high Require approved apps (Enforces mobile app protection for phones and tablets) 	Block clients that don't support modern authentication (Clients that do not use modern authentication can bypass conditional access rules, so it's important to block these)	Require compliant PCs 	Use app enforced restrictions of SharePoint Online (This tells Azure to use the settings specified in SharePoint Online. This rule applies to all users but only affects access to sites included in SharePoint Online access policies.) 	High risk users must change password (Forces users to change their password when signing in if high risk activity is detected for their account) 	Define compliance policies (One policy for each platform) 
Sensitive	 	Require MFA when sign-in risk is low, medium, or high 		Require compliant PCs and mobile devices (Enforces Intune management for PCs and phone/tablets) 			Define app protection policies (One policy per platform — iOS, Android) 
Highly regulated	 	Always require MFA  				Access control policy: allow browser-only access to specific SharePoint sites from unmanaged devices 	Access control policy: block access to specific SharePoint sites from unmanaged devices 

If you included SharePoint Online when you created the common policies, you only need create the new policies. When configuring conditional access rules, SharePoint Online includes OneDrive for Business.

The new policies implement device protection for sensitive and highly-regulated content by applying specific access requirements to SharePoint sites that you specify.

The following table lists the policies you either need to review and update or create new for SharePoint Online. The common policies link to the associated configuration instructions in the [Common identity and device access policies](#) article.

PROTECTION LEVEL	POLICIES	MORE INFORMATION
Baseline	Require MFA when sign-in risk is <i>medium or high</i>	Include SharePoint Online in the assignment of cloud apps
	Block clients that don't support modern authentication	Include SharePoint Online in the assignment of cloud apps
	Define app protection policies	Be sure all recommended apps are included in the list of apps. Be sure to update the policy for each platform (iOS, Android, Windows)
	Require compliant PCs	Include SharePoint Online in list of cloud apps
	Use app enforced restrictions in SharePoint Online	Add this new policy. This tells Azure AD to use the settings specified in SharePoint Online. This rule applies to all users, but only affects access to sites included in SharePoint Online access policies
Sensitive	Require MFA when sign-in risk is <i>low, medium or high</i>	Include SharePoint Online in the assignments of cloud apps
	Require compliant PCs <i>and</i> mobile devices	Include SharePoint Online in the list of cloud apps
	SharePoint Online access control policy: Allow browser-only access to specific SharePoint sites from unmanaged devices	This prevents edit and download of files. Use PowerShell to specify sites
Highly regulated	Always require MFA	Include SharePoint Online in the assignment of cloud apps
	SharePoint Online access control policy: Block access to specific SharePoint sites from unmanaged devices	Use PowerShell to specify sites

Use app-enforced restrictions in SharePoint Online

If you implement access controls in SharePoint Online, you must create this conditional access policy in Azure AD to tell Azure AD to enforce the policies you configure in SharePoint Online. This rule applies to all users, but only affects access to the sites you specify using PowerShell when you create the access controls in SharePoint Online.

To configure this policy see "Block or limit access to specific SharePoint site collections or OneDrive accounts" in this article: [Control access from unmanaged devices](#).

SharePoint Online access control policies

Microsoft recommends you protect content in SharePoint sites with sensitive and highly-regulated content with device access controls. You do this by creating a policy that specifies the level of protection and the sites to apply the protection to.

- Sensitive sites: Allow browser-only access. This prevents users from editing and downloading files.

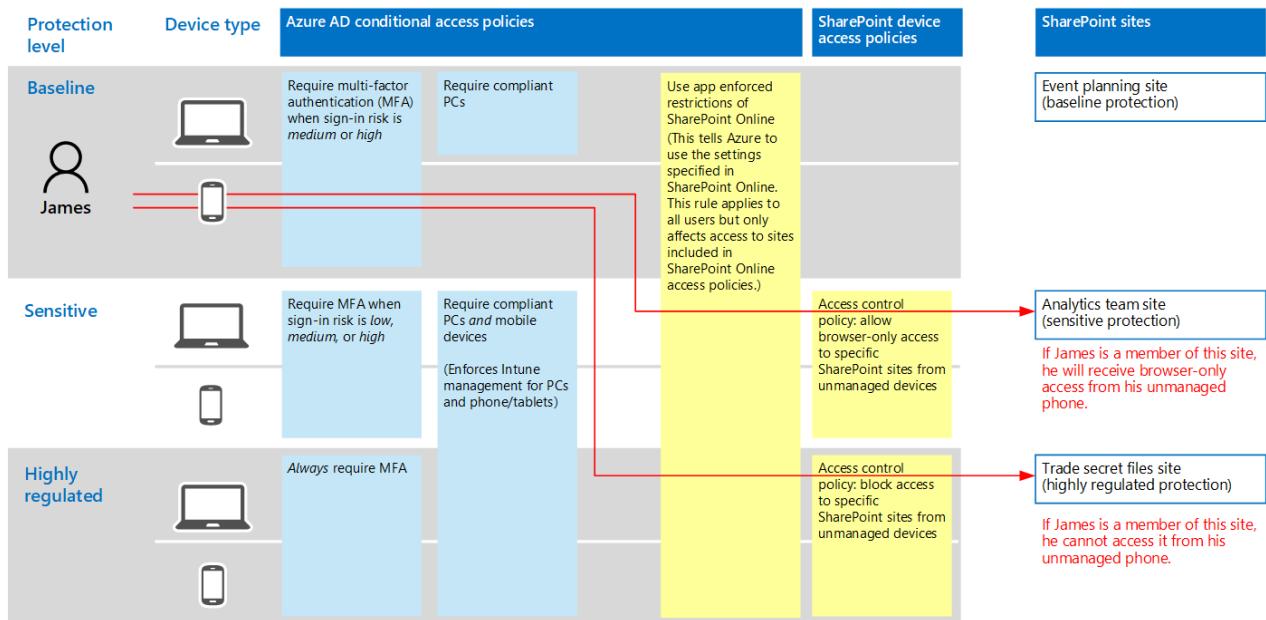
- Highly regulated sites: Block access from unmanaged devices.

See "Block or limit access to specific SharePoint site collections or OneDrive accounts" in this article: [Control access from unmanaged devices](#).

How these policies work together

It's important to understand that SharePoint site permissions are typically based on business need for access to sites. These permissions are managed by site owners and can be highly dynamic. Using SharePoint device access policies ensures protection to these sites, regardless of whether users are assigned to an Azure AD group associated with baseline, sensitive, or highly regulated protection.

The following illustration provides an example of how SharePoint device access policies protect access to sites.



In the illustration:

- James is assigned to conditional access policies associated with baseline protection, but he can be given access to SharePoint sites associated with sensitive or highly-regulated protection.
- If James accesses a sensitive or highly-regulated site he is a member of using his PC, his access is granted as long as his PC is compliant.
- If James accesses a sensitive site he is a member of using his unmanaged phone, which is allowed for baseline users, he will receive browser-only access to the sensitive site due to the device access policy configured for this site.
- If James accesses a highly regulated site he is a member of using his unmanaged phone, he will be blocked due to the access policy configured for this site. He can only access this site using his managed and compliant PC.

Next steps

[Secure SharePoint Online sites and files](#)

Compliance solutions

12/5/2018 • 2 minutes to read • [Edit Online](#)

This library provides technical resources for using capabilities in Microsoft 365 to work towards compliance of regulations that apply to many organizations, starting with [GDPR](#).

While we add more content to this library, be sure to look at compliance resources in the Microsoft Trust Center:

- [Compliance overview](#)
- [Compliance offerings](#)

Microsoft 365 ISO 27001 action plan — Top priorities for your first 30 days, 90 days, and beyond

12/5/2018 • 9 minutes to read • [Edit Online](#)

The International Organization for Standardization (ISO) is an independent nongovernmental developer of voluntary international standards. The International Electrotechnical Commission (IEC) leads the preparation and publication of international standards for electrical, electronic, and related technologies. The ISO/IEC 27000 family of standards outlines controls and mechanisms that help maintain the security of information assets.

ISO/IEC 27001 is the international standard for implementing an information security management system (ISMS). An ISMS describes the necessary methods used and evidence associated with requirements that are essential for the reliable management of information asset security in any type of organization.

This article includes a prioritized action plan you can follow as you work to meet the requirements of ISO/IEC 27001. This action plan was developed in partnership with Protiviti, a Microsoft partner specializing in regulatory compliance. Learn more about how to use this action plan at Microsoft Ignite by attending this session: [Chart your Microsoft 365 compliance path and information protection strategy](#), presented by Maithili Dandige (Microsoft) and Antonio Maio (Protiviti).

Action plan outcomes

These recommendations are provided across three phases in a logical order with the following outcomes.

Phase	Outcomes

30 days

Understand your ISO 27001 governance and compliance requirements.

- Conduct a risk assessment and align risk management and mitigation to that assessment's outcomes.
- Assess and manage your compliance risks by using the Microsoft Compliance Manager.
- Establish standard operating procedures (SOPs) for each of the 14 ISO 27001 groups.

Start planning a roll out of an information classification and retention policies and tools to the organization to help users identify, classify and protect sensitive data and assets.

- Learn how the Azure Information Protection application and policies can help users easily apply visual sensitivity markings and metadata to documents and emails. Develop your organization's information classification schema, along with an education and roll out plan.
- Consider rolling out Office 365 Labels to the organization to help users easily apply record retention and protection policies to content. Plan your organization's labels in accordance with your legal requirements for information record retention, along with an education and roll out plan.

Ensure that records related to information security are protected from loss, deletion, modification or unauthorized access by creating Audit and Accountability policies as part of your Standard Operating Procedures (SOPs).

- Enable audit logging (including mailbox auditing) to monitor Office 365 for potentially malicious activity and to enable forensic analysis of data breaches.
- On a regular cadence, search your Office 365 tenant's audit logs to review changes that have been made to the tenant's configuration settings.
- Enable alert policies for sensitive activities, such as when an elevation of privileges occurs on a user account.
- For long-term storage of Office 365 audit log data, use the Office 365 Management Activity API reference to integrate with a security information and event management (SIEM) tool.

Define administrative and security roles for the organization, along with appropriate policies related to segregation of duties.

- Utilize the Office 365 administrative roles to enable separation of administration duties.
- Segment permissions to ensure that a single administrator does not have greater access than necessary.

90 days	<p>Use Microsoft 365 security capabilities to control access to the environment, and protect organizational information and assets according to your defined standard operating procedures (SOPs).</p> <ul style="list-style-type: none"> • Protect administrator and end user accounts by enabling identity and authentication solutions, such as multi-factor authentication and modern authentication. • Establish strong password policies to manage and protect user account credentials. • Configure and roll out message encryption capabilities to help end users comply with your organization's SOPs when sending sensitive data via email. • Protect against malicious code and implement data breach prevention and response procedures. • Configure Data Loss Prevention (DLP) policies to identify, protect and control access to sensitive data. • Ensure that sensitive data is stored and accessed according to corporate policies. • Prevent the most common attack vectors including phishing emails and Office documents containing malicious links and attachments.
Beyond 90 days	<p>Use Microsoft 365 advanced data governance tools and information protection to implement ongoing governance programs for personal data.</p> <ul style="list-style-type: none"> • Automatically identify personal information in documents and emails • Protect sensitive data stored and accessed on mobile devices across the organization, and ensure compliant corporate devices are used to data. <p>Monitor ongoing compliance across Microsoft 365 and other Cloud applications.</p> <ul style="list-style-type: none"> • To evaluate performance against standard operating procedures (SOPs), utilize Microsoft Compliance Manager to perform regular assessments of the organization's information security policies and their implementation. • Review and monitor the information security management system on an on-going basis. • Control and perform regular reviews of all users and groups with high levels of permissions (ie. privileged or administrative users). • Deploy and configure Microsoft 365 capabilities for protecting privileged identities and strictly controlling privileged access. • As part of your standard operating procedures (SOPs), search the Office 365 audit logs to review changes that have been made to the tenant's configuration settings, elevation of end user privileges and risky user activities. • Monitor your organization's usage of cloud applications and implement advanced alerting policies. • Track risky activities, to identify potentially malicious administrators, to investigate data breaches, or to verify that compliance requirements are being met.

30 days — Powerful Quick Wins

These tasks can be accomplished quickly and have low impact to users.

Area	Tasks
Understand your ISO 27001 governance and compliance requirements.	<ul style="list-style-type: none"> Assess and manage your compliance risks by using the Microsoft Compliance Manager within the Microsoft Service Trust Portal (STP) to conduct an ISO 27001:2013 assessment of your organization. Establish standard operating procedures (SOPs) for each of the 14 ISO 27001 groups.
Start planning a roll out of an information classification and retention policies and tools to the organization to help users identify, classify and protect sensitive data and assets.	<ul style="list-style-type: none"> Help users easily identify and classify sensitive data, according to your information protection policies and standard operating procedures (SOPs), by rolling out classification policies and the Azure Information Protection application. Develop your organization's information classification schema (policies), along with an education and roll out plan. Help users easily apply record retention and protection policies to content by rolling out Office 365 Labels to the organization. Plan your organization's labels in accordance with your legal requirements for information record retention, along with an education and roll out plan.
Ensure that records related to information security are protected from loss, deletion, modification or unauthorized access by creating Audit and Accountability policies as part of your Standard Operating Procedures (SOPs).	<ul style="list-style-type: none"> Enable Office 365 audit logging and mailbox auditing (for all Exchange mailboxes) to monitor Office 365 for potentially malicious activity and to enable forensic analysis of data breaches. On a regular cadence, search your Office 365 tenant's audit logs to review changes that have been made to the tenant's configuration settings. Enable Office 365 Alert Policies in the Office 365 Security and Compliance Center for sensitive activities, such as when an elevation of privileges occurs on a user account. For long-term storage of Office 365 audit log data, use the Office 365 Management Activity API reference to integrate with a security information and event management (SIEM) tool.
Define administrative and security roles for the organization, along with appropriate policies related to segregation of duties.	<ul style="list-style-type: none"> Utilize the Office 365 administrative roles to enable separation of administration duties. Note: many administrator roles in Office 365 have a corresponding role in Exchange Online, SharePoint Online, and Skype for Business Online. Segment permissions to ensure that a single administrator does not have greater access than necessary.

90 days — Enhanced Protections

These tasks take a bit more time to plan and implement but greatly increase your security posture.

Area	Tasks

Use Microsoft 365 security capabilities to control access to the environment, and protect organizational information and assets according to your defined standard operating procedures (SOPs).

- Protect administrator and end user accounts by implementing [identity and device access policies](#), including enabling multi-factor authentication (MFA) for all user accounts and modern authentication for all apps.
- Establish [strong password policies](#) to manage and protect user account credentials.
- Set up [Office 365 Message Encryption \(OME\)](#) to help end users comply with your organization's SOPs when sending sensitive data via email.
- Deploy [Windows Defender Advanced Threat Protection \(ATP\)](#) to all desktops for protection against malicious code, as well as data breach prevention and response.
- Configure, test and deploy [Office 365 Data Loss Prevention \(DLP\) policies](#) to identify, monitor and [automatically protect](#) over 80 common sensitive data types within documents and emails, including financial, medical, and personally identifiable information.
- Automatically inform email senders that they may be about to violate one of your policies—even before they send an offending message by configuring [Policy Tips](#). Policy Tips can be configured to present a brief note in Outlook, Outlook on the web, and OWA for devices, that provides information about possible policy violations during message creation.
- Implement [Office 365 Advanced Threat Protection \(ATP\)](#) to help prevent the most common attack vectors including phishing emails and Office documents containing malicious links and attachments.

Beyond 90 Days – Ongoing Security, Data Governance, and Reporting

Secure personal data at rest and in transit, detect and respond to data breaches, and facilitate regular testing of security measures. These are important security measures that build on previous work.

Area	Tasks
Use Microsoft 365 advanced data governance tools and information protection to implement ongoing governance programs for personal data.	<ul style="list-style-type: none">• Use Office 365 Advanced Data Governance to identify personal information in documents and emails by automatically applying Office 365 Labels.• Use Microsoft Intune to protect sensitive data stored and accessed on mobile devices across the organization, and ensure compliant corporate devices are used to data.

Monitor ongoing compliance across Microsoft 365 and other Cloud applications.

- To evaluate performance against standard operating procedures (SOPs), utilize [Microsoft Compliance Manager](#) on an ongoing basis to perform regular ISO 27001:2013 assessments of the organization's information security policies and their implementation.
- Review and monitor the information security management system on an on-going basis.
- Use [Azure AD Privileged Identity Management](#) to control and perform regular reviews of all users and groups with high levels of permissions (ie. privileged or administrative users).
- Deploy and configure [Privileged Access Management in Office 365](#) to provide granular access control over privileged admin tasks in Office 365. Once enabled, users will need to request just-in-time access to complete elevated and privileged tasks through an approval workflow that is highly scoped and time-bound.
- As part of your standard operating procedures (SOPs), search the Office 365 audit logs to review changes that have been made to the tenant's configuration settings, elevation of end user privileges and risky user activities.
- Audit [non-owner mailbox access](#) to identify potential leaks of information and to proactively review non-owner access on all Exchange Online mailboxes.
- Use [Office 365 Alert Policies, data loss prevention reports and Microsoft Cloud App Security](#) to monitor your organization's usage of cloud applications and implement advanced alerting policies based on heuristics and user activity.
- Use [Microsoft Cloud App Security](#) to automatically track risky activities, to identify potentially malicious administrators, to investigate data breaches, or to verify that compliance requirements are being met.

Learn more

Microsoft Trust Center: [ISO/IEC 27001:2013 Information Security Management Standards](#)

[Microsoft Trust Center](#)

Microsoft 365 NIST 800-53 action plan — Top priorities for your first 30 days, 90 days, and beyond

12/5/2018 • 8 minutes to read • [Edit Online](#)

Microsoft 365 allows you to operate your enterprise with a cloud control framework, which aligns controls with multiple regulatory standards. Microsoft 365 includes Office 365, Windows 10, and Enterprise Mobility + Security. Microsoft's internal control system is based on the National Institute of Standards and Technology (NIST) special publication 800-53, and Office 365 has been accredited to latest NIST 800-53 standard. <!--As the framework was designed to be voluntary, the NIST framework has not formalized an accreditation process. However, Microsoft has undergone independent, third-party Federal Risk and Authorization Management Program (FedRAMP) Moderate and High Baseline audit certification using the test criteria defined in NIST 800-53A (Rev. 4). -->

Microsoft is recognized as an industry leader in cloud security. Using years of experience building enterprise software and running online services, our team is constantly learning and continuously updating our services and applications to deliver a secure cloud productivity service that meets rigorous industry standards for compliance. Microsoft's government cloud services, including Office 365 U.S. Government, meet the demanding requirements of the US Federal Risk and Authorization Management Program (FedRAMP), enabling U.S. federal agencies to benefit from the cost savings and rigorous security of the Microsoft Cloud.

This article includes a prioritized action plan you can follow as you work to meet the requirements of NIST 800-53. This action plan was developed in partnership with Protiviti, a Microsoft partner specializing in regulatory compliance. Learn more about how to use this action plan at Microsoft Ignite by attending this session: [Chart your Microsoft 365 compliance path and information protection strategy](#), presented by Maithili Dandige (Microsoft) and Antonio Maio (Protiviti).

Action plan outcomes

These recommendations are provided across three phases in a logical order with the following outcomes.

Phase	Outcomes
30 days	<ul style="list-style-type: none">Understand your NIST 800-53 requirements and consider engaging with a Microsoft Advisory Partner.Learn and understand the Microsoft 365 built-in defense-in-depth strategy.Protect user and administrator access to Office 365.Ensure all access to the system is auditable according to your organization's audit and accountability policies.
90 days	<ul style="list-style-type: none">Enhance your anti-malware, patching, and configuration management program.Use Microsoft 365 security capabilities to control access to the environment and to protect organizational information and assets.Utilize built in auditing capabilities to monitor sensitive or risky activities within Office 365.Deploy Advanced Threat Protection for both links and attachments in email and Office documents.

Beyond 90 days	<ul style="list-style-type: none"> • Use Microsoft 365 advanced tools and information protection to implement ongoing controls for devices and protection for corporate data. • Monitor ongoing compliance across Microsoft 365 and other Cloud applications. • Leverage enhanced threat detection and protection capabilities with advanced threat analytics to provide a robust and layered security strategy for the organization. Develop an incident response plan to mitigate the effects of compromised systems in your organization.
----------------	---

30 days — Powerful Quick Wins

These tasks can be accomplished quickly and have low impact to users.

Area	Tasks
Understand your NIST 800-53 requirements and consider engaging with a Microsoft Advisory Partner.	<ul style="list-style-type: none"> • Work with your Microsoft Partner to perform a gap analysis of your NIST 800-53 compliance for the organization and to develop a roadmap that charts your journey to compliance. • Utilize guidance in Microsoft Compliance Manager and the Microsoft Service Trust Portal (STP) to define and document policies and procedures for both access control and information sharing which addresses purpose, scope, roles, responsibilities, coordination among organizational entities, and compliance.
Learn and understand the Microsoft 365 built-in defense-in-depth strategy.	<ul style="list-style-type: none"> • Assess and manage your compliance risks by using Microsoft Compliance Manager within the Microsoft Service Trust Portal (STP) to conduct an NIST 800-53 assessment of your organization. Align Microsoft 365 security controls for managing and mitigating risks to the assessment's outcomes. • Utilize Microsoft Secure Score to track the organization's usage of Microsoft 365 security capabilities over time within both Office 365 and on Windows 10 desktops. • Learn about Microsoft's technologies and strategies used to provide Office 365 data encryption, as well as strategies for protection against denial-of-service attacks in the Microsoft Cloud.
Protect user and administrator access to Office 365.	<ul style="list-style-type: none"> • Establish strong credential management to protect user account credentials. • Learn about recommended identity and device access policies for Office 365 services. • Utilize the Office 365 administrative roles to implement role-based access to administration capabilities and to enable separation of administration duties. Note: many administrator roles in Office 365 have a corresponding role in Exchange Online, SharePoint Online, and Skype for Business Online. Segment permissions to ensure that a single administrator does not have greater access than necessary.
Ensure all access to the system is audited according to your organization's audit and accountability policies.	Enable Office 365 audit logging and mailbox auditing (for all Exchange mailboxes) to monitor Office 365 for potentially malicious activity and to enable forensic analysis of data breaches.

90 days — Enhanced Protections

These tasks take a bit more time to plan and implement.

Area	Tasks
Enhance your Anti-malware, patching, and configuration management program.	<ul style="list-style-type: none">• Protect corporate assets and desktops by deploying and enabling Windows Defender Antivirus to your organization and leveraging its tight integration with Windows 10.• Keep track of quarantined infected systems and prevent further damage until remediation steps are taken.• Confidently rely on Microsoft 365 rigorous standard change management process for trusted updates, hotfixes, and patches.
Use Microsoft 365 security capabilities to control access to the environment and to protect organizational information and assets.	<ul style="list-style-type: none">• Implement recommended identity and device access policies to protect user and administrative accounts.• Implement Office 365 Message Encryption (OME) capabilities to help users comply with your organization's policies when sending sensitive data via email.• Deploy Windows Defender Advanced Threat Protection (ATP) to all desktops for protection against malicious code, as well as data breach prevention and response.• Configure, test and deploy Office 365 Data Loss Prevention (DLP) policies to identify, monitor and automatically protect over 80 common sensitive data types within documents and emails, including financial, medical, and personally identifiable information.• Automatically inform email senders that they may be about to violate one of your policies — even before they send an offending message by configuring Policy Tips. Policy Tips can be configured to display a brief note (in Outlook, Outlook on the web, and OWA for devices) that provides information about possible policy violations during message creation.• Protect sensitive corporate data and meet your organization's information sharing policies by implementing controls for external sharing in SharePoint Online and OneDrive for Business. Ensure only authenticated external users can access corporate data.
Utilize built in auditing capabilities to monitor sensitive or risky activities within Office 365.	<ul style="list-style-type: none">• Enable Alert Policies in the Office 365 Security and Compliance Center to raise automatic notifications when sensitive activities occur, such as when a user's account privileges are elevated or when sensitive data is accessed. All privileged functions should be audited and monitored.• On a regular cadence, search your Office 365 audit logs in the Office 365 Security and Compliance Center to review changes that have been made to the tenant's configuration settings.• For long-term storage of Office 365 audit log data, use the Office 365 Management Activity API reference to integrate with a security information and event management (SIEM) tool.

Deploy Advanced Threat Protection for both links and attachments in email and Office documents.	Implement Office 365 Advanced Threat Protection (ATP) to help prevent the most common attack vectors including phishing emails and Office documents containing malicious links and attachments.

Beyond 90 Days – Ongoing Security, Data Governance, and Reporting

These actions take longer and build on previous work.

Area	Tasks
Use Microsoft 365 advanced tools and information protection to implement ongoing controls for devices and protection for corporate data.	<ul style="list-style-type: none"> • Use Microsoft Intune to protect sensitive data stored and accessed on mobile devices and to ensure compliant corporate devices are used to access cloud services.
Monitor ongoing compliance across Microsoft 365 and other Cloud applications.	<ul style="list-style-type: none"> • To evaluate performance against the organization's defined policies and procedures, utilize Microsoft Compliance Manager on an ongoing basis to perform regular assessments of the organization's enforcement of information security policies. • Use Azure AD Privileged Identity Management to control and perform regular reviews of all users and groups with high levels of permissions (ie. privileged or administrative users). • Deploy and configure Privileged Access Management to provide granular access control over privileged admin tasks in Office 365. Once enabled, users will need to request just-in-time access to complete elevated and privileged tasks through an approval workflow that is highly scoped and time-bound. • Audit non-owner mailbox access to identify potential leaks of information and to proactively review non-owner access on all Exchange Online mailboxes. • Use Office 365 Alert Policies, data loss prevention reports, and Microsoft Cloud App Security to monitor your organization's usage of cloud applications and to implement advanced alerting policies based on heuristics and user activity. • Use Microsoft Cloud App Security to automatically track risky activities, to identify potentially malicious administrators, to investigate data breaches, or to verify that compliance requirements are being met.

Leverage enhanced threat detection and protection capabilities with advanced threat analytics to provide a robust and layered security strategy for the organization. Develop an incident response plan to mitigate the effects of compromised systems in your organization.

- Deploy and configure [Windows Advanced Threat Analytics](#) to leverage rich analytics and reporting to gain critical insights into which users are being targeted in your organization and the cyber-attack methodologies being exploited.
- Leverage [Office 365 Advanced Threat Protection reports and analytics](#) to analyze threats through insights into malicious content and malicious emails automatically detected within your organization. Utilize built-in reports and message trace capabilities to investigate email messages that have been blocked due to an unknown virus or malware.
- Use [Office 365 Threat Intelligence](#) to aggregate insights and information from various sources to get a holistic view of your cloud security landscape.
- Integrate [Office 365 Threat Intelligence and Windows Defender Advanced Threat Protection](#) to quickly understand if users' devices are at risk when investigating threats in Office 365.
- Simulate common attack methods within your Office 365 environment using the [Office 365 Attack Simulator](#). Review results from attack simulations to identify training opportunities for users and to validate your organization's incident response procedures.
- Configure [permissions within the Office 365 Security and Compliance Center](#) to ensure access to monitoring and audit data is restricted to approved users and integrated with the organization's incident response measures.

Learn more

Learn more about Microsoft and the [NIST Cyber Security Framework \(CSF\)](#), including NIST 800-53.

[Microsoft Trust Center](#)

GDPR

2/22/2019 • 2 minutes to read • [Edit Online](#)

This library provides technical guidance for the General Data Protection Regulation (GDPR):

- [Information protection](#)
- [Data subject requests](#)
- [Breach notification](#)

For more information about how Microsoft can help you with the GDPR, see [GDPR Overview](#) at Trust Center.

Learn more

[Microsoft Trust Center](#)

Microsoft 365 GDPR action plan — Top priorities for your first 30 days, 90 days, and beyond

12/5/2018 • 6 minutes to read • [Edit Online](#)

This article includes a prioritized action plan you can follow as you work to meet the requirements of the General Data Protection Regulation (GDPR). This action plan was developed in partnership with Protiviti, a Microsoft partner specializing in regulatory compliance. Learn more about how to use this action plan at Microsoft Ignite by attending this session: [Chart your Microsoft 365 compliance path and information protection strategy](#), presented by Maithili Dandige (Microsoft) and Antonio Maio (Protiviti).

The GDPR introduces new rules for companies, government agencies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data for EU residents. The GDPR applies no matter where you or your enterprise are located.

Action plan outcomes

These recommendations are provided across three phases in a logical order with the following outcomes.

Phase	Outcomes
30 days	<p>Understand your GDPR requirements and consider engaging with a Microsoft GDPR Advisory Partner.</p> <ul style="list-style-type: none">Benchmark your readiness and get recommendations for next steps.Work with a Microsoft GDPR Advisory Partner to establish internal guidelines for responding to Data Subject Requests (DSRs), perform a GDPR compliance gap analysis for your organization and establish a roadmap to compliance. <p>Start discovering the types of personal data you are storing and where it resides to comply with DSRs.</p> <ul style="list-style-type: none">Use Content search and eDiscovery in the Office 365 Security & Compliance Center to discover personal data across the organization.When working with vast quantities of content, use Office 365 Advanced eDiscovery, powered by machine learning technologies, to perform more efficient and accurate content searches.

90 days	<p>Start implementing compliance requirements using Microsoft 365 data governance and compliance capabilities.</p> <ul style="list-style-type: none"> • Assess and manage your compliance risks by using the Microsoft Compliance Manager. • Help users identify and classify personal data, as defined by the GDPR. <p>Use Microsoft 365 security capabilities to prevent data breaches and implement protections for personal data.</p> <ul style="list-style-type: none"> • Protect administrator and end user accounts. • Protect against malicious code and implement data breach prevention and response. • Use audit logging to monitor for potentially malicious activity and to enable forensic analysis of data breaches. • Use Data Loss Prevention (DLP) policies to identify and protect sensitive data. • Prevent the most common attack vectors including phishing emails and Office documents containing malicious links and attachments.
Beyond 90 days	<p>Use Microsoft 365 advanced data governance tools and information protection to implement ongoing governance programs for personal data.</p> <ul style="list-style-type: none"> • Automatically identify personal information in documents and emails. • Protect personal data stored on devices across the organization, and ensure compliant corporate devices are used to access sensitive data. • Ensure that sensitive personal information is stored and accessed according to corporate policies. • Implement data retention policies to help ensure you are only retaining personal data for as long as necessary. <p>Monitor ongoing compliance across Microsoft 365 and other Cloud applications. Consider addressing data residency requirements for EU personal data.</p> <ul style="list-style-type: none"> • Monitor your organization's usage of cloud applications and implement advanced alerting policies. • Address data residency requirements while still operating as one global organization.

30 days — Powerful Quick Wins

These tasks can be accomplished quickly and have low impact to users.

Area	Tasks

<p>Understand your GDPR requirements and consider engaging with a Microsoft GDPR Advisory Partner.</p>	<ul style="list-style-type: none"> • Use the Microsoft GDPR Assessment Tool to privately benchmark your readiness and get recommendations for next steps. • Assess and manage your compliance risks by using the Microsoft Compliance Manager within the Microsoft Service Trust Portal (STP) to conduct a GDPR Assessment of your organization. • Work with your Microsoft GDPR Advisory Partner to establish internal guidelines for responding to Data Subject Requests (DSRs) and exclusions from DSRs. • Work with your Microsoft GDPR Advisory partner to perform a gap analysis in GDPR compliance for your organization, and develop a roadmap that charts your journey to GDPR compliance. • Learn how to use the GDPR Dashboard and Data Subject Request capability in the Office 365 Security & Compliance Center.
<p>Start discovering the types of personal data you are storing and where it resides to comply with DSRs.</p>	<ul style="list-style-type: none"> • Use Content Search and eDiscovery cases in the Office 365 Security & Compliance Center to easily search across mailboxes, public folders, Office 365 Groups, Microsoft Teams, SharePoint Online sites, One Drive for Business sites and Skype for Business conversations. Learn how to use sensitive information types to find personal data of EU citizens • When working with vast quantities of content, identify documents that are relevant to a particular subject (for example, a compliance investigation) quickly and with better precision than traditional keyword searches with Office 365 Advanced eDiscovery, powered by machine learning technologies. • Preview search results, get keyword statistics for one or more searches, bulk-edit content searches, and export the results using the Office 365 Security & Compliance Center.

90 days — Enhanced Protections

These tasks take a bit more time to plan and implement but greatly increase your security posture.

Area	Tasks
<p>Start implementing compliance requirements using Microsoft 365 data governance and compliance capabilities.</p>	<ul style="list-style-type: none"> • Manage your GDPR Compliance using the Microsoft Compliance Manager within the Microsoft Service Trust Portal (STP). • Help users identify and classify personal data, as defined by the GDPR, by rolling out a classification schema and associated Office 365 Labels to the organization for Exchange email, SharePoint sites, OneDrive for Business sites and Office 365 Groups. See Office 365 Information Protection for GDPR.

<p>Use Microsoft 365 security capabilities to prevent data breaches and implement protections for personal data.</p>	<ul style="list-style-type: none"> • Improve authentication for administrators and end users in the Microsoft Cloud by enabling multi-factor authentication for all user accounts and modern authentication for all apps. For recommended policy configuration, see Identity and device access configurations. • Deploy Windows Defender Advanced Threat Protection (ATP) to all desktops for protection against malicious code, as well as data breach prevention and response. • Enable Office 365 audit logging and mailbox auditing for all Exchange mailboxes to monitor for potentially malicious activity and to enable forensic analysis of data breaches. • Configure, test and deploy Office 365 Data Loss Prevention (DLP) policies to identify, monitor and automatically protect over 80 common sensitive data types within documents and emails, including financial, medical, and personally identifiable information. • Implement Office 365 Advanced Threat Protection (ATP) to help prevent the most common attack vectors including phishing emails and Office documents containing malicious links and attachments.
--	--

Beyond 90 Days – Ongoing Security, Data Governance, and Reporting

Secure personal data at rest and in transit, detect and respond to data breaches, and facilitate regular testing of security measures. These are important security measures that build on previous work.

Area	Tasks
<p>Use Microsoft 365 advanced data governance tools and information protection to implement ongoing governance programs for personal data.</p>	<ul style="list-style-type: none"> • Use Office 365 Advanced Data Governance to identify personal information in documents and emails by automatically applying Office 365 Labels. • Protect personal data stored on devices across the organization by deploying Microsoft Intune. • Implement AAD Conditional Access policies in conjunction with Microsoft Intune to ensure that sensitive personal information is stored and accessed according to corporate policies. For recommended policy configuration, see Identity and device access configurations • Implement data retention policies with Office 365 Labels, Advanced Data Governance and Retention Policies to help ensure you are only retaining personal data for as long as necessary in your jurisdiction.
<p>Monitor ongoing compliance across Microsoft 365 and other Cloud applications. Consider addressing data residency requirements for EU personal data.</p>	<ul style="list-style-type: none"> • Use Office 365 Alert Policies, data loss prevention reports and Microsoft Cloud App Security to monitor your organization's usage of cloud applications and implement advanced alerting policies based on heuristics and user activity. • Address organizational, regional, and local data residency requirements while still operating as one global organization by using Microsoft's multi-geo capabilities for Exchange Online mailboxes, OneDrive for Business sites and SharePoint Online sites.

Learn more

[Guide to the General Data Protection Regulation \(GDPR\)](#) by the Information Commissioner's Office

[General Data Protection Regulation \(GDPR\) FAQs for small organizations](#) by the Information Commissioner's Office

[Microsoft.com/GDPR](#)

[Microsoft Trust Center](#)

Accountability readiness checklists for the GDPR

2/22/2019 • 2 minutes to read • [Edit Online](#)

These accountability readiness checklists provide a convenient way to access information you may need to support the General Data Protection Regulation (GDPR) when using Microsoft products and services.

- [Office 365](#)
- [Azure](#)
- [Dynamics 365](#)
- [Microsoft Support and Professional Services](#)

Learn more

[Microsoft Trust Center](#)

Accountability Readiness Checklist for Microsoft Office 365

2/22/2019 • 30 minutes to read • [Edit Online](#)

1. Introduction

This accountability readiness checklist provides a convenient way to access information you may need to support the GDPR when using Microsoft Office 365.

You can manage the items in this checklist with [Compliance Manager](#) by referencing the Control ID and Control Title under *Customer Managed Controls* in the GDPR tile.

In addition, items in this checklist under *5. Data Protection & Security* provide references to controls listed under Microsoft Managed Controls in the GDPR tile in [Compliance Manager](#). Reviewing the Microsoft Implementation Details for these controls provide additional explanation of Microsoft's approach to fulfilling the customer considerations in the checklist item.

The checklist and Compliance Manager are organized using the titles and reference number (in parenthesis for each checklist topic) of a set of privacy and security controls for personal data processors drawn from *ISO/IEC CD 27552 Information technology -- Security techniques -- Enhancement to ISO/IEC 27001 for privacy management – Requirements. *

This control structure is also used to organize the presentation of the internal controls that Microsoft Office 365 implements to support GDPR, which you can [download](#).

ISO/IEC CD 27552, a standard under current development, will enhance *ISO/IEC 27001* requirements. It covers process for protecting the capture, accountability, availability, integrity and confidentiality of data. To purchase a copy of the complete draft ISO standard, please visit <https://shop.bsigroup.com/ProductDetail?pid=00000000030372571>.

2. Conditions for collection and processing

Category	Customer Consideration	Supporting Microsoft documentation	Addresses GDPR Article(s)
Determine when consent is to be obtained (7.2.3)	The customer should understand legal or regulatory requirements for obtaining consent from individuals prior to processing personal data (when it is required, if the type of processing is excluded from the requirement, etc.), including how consent is collected.	Office 365 does not provide direct support for gaining user consent.	(6)(1)(a), (8)(1), (8)(2)

Identify and document purpose (7.2.1)	The customer should document the purpose for which personal data is processed.	A description of the processing Microsoft performs for you, and the purposes of that processing, that can be included in your accountability documentation. - <i>Microsoft Online Services Terms, Data Protection Terms, see Processing of Personal Data; GDPR</i> [1]	(5)(1)(b), (32)(4)
Identify lawful basis (7.2.2)	The customer should understand any requirements related to the lawful basis of processing, such as whether consent must first be given.	A description of processing personal data by Microsoft services for inclusion in your accountability documentation. - <i>Key Information from Office 365 for Customer Data Protection Impact Assessments</i> [10]	(5)(1)(a), (6)(1)(a), (6)(1)(b), (6)(1)(c), (6)(1)(d), (6)(1)(e), (6)(1)(f), (6)(3), (6)4)(a), (6)(4)(b), (6)(4)(c), (6)(4)(d), (6)(4)(e), (8)(3), (9)(1), (9)(2)(b), (9)(2)(c), (9)(2)(d), (9)(2)(e), (9)(2)(f), (9)(2)(g), (9)(2)(h), (9)(2)(i), (9)(2)(j), (9)(3), (9)(4), (10), (17)(3)(a), (17)(3)(b), (17)(3)(c), (17)(3)(d), (17)(3)(e), (18)(2), (22)(2)(a), (22)(2)(b), (22)(2)(c), (22)(4)
Determine when consent is to be obtained (7.2.3)	The customer should understand legal or regulatory requirements for obtaining consent from individuals prior to processing personal data (when it is required, if the type of processing is excluded from the requirement, etc.), including how consent is collected.	Office 365 does not provide direct support for gaining user consent.	(6)(1)(a), (8)(1), (8)(2)
Obtain and record consent (7.2.4)	When it is determined to be required, the customer should appropriately obtain consent. The customer should also be aware of any requirements for how a request for consent is presented and collected.	Office 365 does not provide direct support for gaining user consent.	(7)(1), (7)(2), (9)(2)(a)

Privacy impact assessment (7.2.5)	The customer should be aware of requirements for completing privacy impact assessments (when they should be performed, categories of data that might necessitate one, timing of completing the assessment).	How Microsoft services determine when to perform a DPIA, and an overview of the DPIA program at Microsoft including the involvement of the DPO, is provided on the Service Trust Portal Data Protection Impact Assessments (DPIAs) page . For support for your DPIAs see: - <i>Key Information from Office 365 for Customer Data Protection Impact Assessments</i> [10]	(35)
Contracts with PII Processors (7.2.6)	The customer should ensure that their contracts with processors include requirements for aiding with any relevant legal or regulatory obligations related to processing and protecting personal data.	The Microsoft contracts that require us to aid with your obligations under the GDPR, including support for the data subject's rights. - <i>Microsoft Online Services Terms, Data Protection Terms, see Processing of Personal Data; GDPR</i> [1]	(5)(2), (28)(3)(e), (28)(9)
Records related to processing PII (7.2.7)	The customer should maintain all necessary and required records related to processing personal data (that is, purpose, security measures, etc.). Where some of these records must be provided by a sub-processor, the customer should ensure that they can obtain such records.	The tools provided by Microsoft services to help you maintain the records necessary demonstrate compliance and support for accountability under the GDPR. - <i>Search the audit log in Office 365 Security and Compliance Center</i> [16]	(5)(2), (24)(1), (30)(1)(a), (30)(1)(b), (30)(1)(c), (30)(1)(d), (30)(1)(g), (30)(1)(f), (30)(3), (30)(4), (30)(5)

3. Rights of data subjects

Category	Customer Consideration	Supporting Microsoft documentation	Addresses GDPR Article(s)

<p>Determining PII principals' rights and enabling exercise (7.3.1)</p>	<p>The customer should understand requirements around the rights of individuals related to the processing of their personal data. These rights may include things such as access, correction, and erasure. Where the customer uses a third-party system, they should determine which (if any) parts of the system provide tools related to enabling individuals to exercise their rights (e.g. to access their data). Where the system provides such capabilities, the customer should utilize them as necessary.</p>	<p>The capabilities Microsoft provides to help you support data subject rights.</p> <ul style="list-style-type: none"> - <i>Office 365 Data Subject Requests for the GDPR</i> [8] - <i>Microsoft Office 365 ISO/IEC 27001:2013 ISMS Statement of Applicability</i> [12] see ISO, IEC 27018, 2014 control A.1.1 	<p>(12)(2)</p>
<p>Determining information for PII principals (data subjects) (7.3.2)</p>	<p>The customer should understand requirements for the types of information about processing of personal data that is to be available to be provided to the individual. This may include things such as:</p> <ul style="list-style-type: none"> - Contact details about the controller or its representative; - information about the processing (purposes, international transfer and related safeguards, retention period, etc.); - information on how the principal may access and/or amend their personal data; requesting erasure or restriction of processing; receiving a copy of their personal data, and portability of their personal data - How and from where the personal data were obtained (if not obtained from the principal directly) - information about the right to lodge a complaint and to whom; - information regarding corrections to personal data; - Notification that the organization is no longer in position to identify the data subject (PII principal), in cases where the processing no longer requires the identification of the data 	<p>Information about Microsoft services that you can include in the data you provide to data subjects.</p> <ul style="list-style-type: none"> - <i>Office 365 Data Subject Requests for the GDPR</i> [8] - <i>Key Information from Office 365 for Customer Data Protection Impact Assessments</i> [10] 	<p>(11)(2), (13)(1)(a), (13)(1)(b), (13)(1)(c), (13)(1)(d), (13)(1)(e), (13)(1)(f), (13)(2)(c), (13)(2)(d), (13)(2)(e), (13)(3), (13)(4), (14)(1)(a), (14)(1)(b), (14)(1)(c), (14)(1)(d), (14)(1)(e), (14)(1)(f), (14)(2)(b), (14)(2)(e), (14)(2)(f), (14)(3)(a), (14)(3)(b), (14)(3)(c), (14)(4), (14)(5)(a), (14)(5)(b), (14)(5)(c), (14)(5)(d), (15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (15)(2), (18)(3), (21)(4)</p>

	<p>subject;</p> <ul style="list-style-type: none"> - Transfers and/or disclosures of personal data; - existence of automated decision making based solely on automated processing of personal data; - information regarding the frequency with which information to the data subject is updated and provided (that is, "just in time" notification, organization defined frequency, etc.) <p>Where the customer uses third-party systems or processors, they should determine which (if any) of this information may need to be provided by them and ensure that they can obtain the required information from the third-party.</p>		
<i>Providing information to PII principals (7.3.3)</i>	The customer should comply with any requirements around how/when/in what form the required information is to be given to an individual related to the processing of their personal data. In cases where a third-party may provide required information, the customer should ensure that it is within the parameters required by the GDPR.	<p>Templated information about Microsoft services that you can include in the data you provide to data subjects.</p> <ul style="list-style-type: none"> - <i>Office 365 Data Subject Requests for the GDPR</i> [8] - <i>Key Information from Office 365 for Customer Data Protection Impact Assessments</i> [10] 	(11)(2), (12)(1), (12)(7), (13)(3), (21)(4)
<i>Provide mechanism to modify or withdraw consent (7.3.4)</i>	The customer should understand requirements for informing users about their right to access, correct, and/or erase their personal data and for providing a mechanism for which them to do so. If a third-party system is used and provides this mechanism as part of its functionality, the customer should utilize that functionality as necessary.	<p>Information about capabilities in Microsoft services that you can use when defining the information you provide to data subjects when requesting consent.</p> <ul style="list-style-type: none"> - <i>Office 365 Data Subject Requests for the GDPR</i> [8] 	(7)(3), (13)(2)(c), (14)(2)(d), (18)(1)(a), (18)(1)(b), (18)(1)(c), (18)(1)(d)

Provide mechanism to object to processing (7.3.5)	The customer should understand requirements around rights of data subjects. Where an individual has a right to object to processing, the customer should inform them, and have a way for the individual to register their objection.	Information about Microsoft services relating to object to processing that you can include in the data you provide to data subjects. - <i>Office 365 Data Subject Requests for the GDPR</i> [8] see Step 4: Restrict	(13)(2)(b), (14)(2)(c), (21)(1), (21)(2), (21)(3), (21)(5), (21)(6)
Sharing the exercising of PII principals' rights (7.3.6)	The customer should understand requirements for notifying third-parties with whom personal data has been shared of instances of data modification based on the exercise of individual rights (e.g. an individual requesting erasure or modification, etc.)	Information about capabilities in Microsoft services that allow you to discover personal data that you have shared with third parties. - <i>Office 365 Data Subject Requests for the GDPR</i> [8]	(19)
Correction or erasure (7.3.7)	The customer should understand requirements for informing users about their right to access, correct, and/or erase their personal data and for providing a mechanism for which them to do so. If a third-party system is used and provides this mechanism as part of its functionality, the customer should utilize that functionality as necessary.	Templated information about Microsoft services relating to their ability to access, correct or erase personal data that you can include in the data you provide to data subjects. - <i>Office 365 Data Subject Requests for the GDPR</i> [8] see Step 5: Delete	(5)(1)(d), (13)(2)(b), (14)(2)(c), (16), (17)(1)(a), (17)(1)(b), (17)(1)(c), (17)(1)(d), (17)(1)(e), (17)(1)(f), (17)(2)
Providing copy of PII processed (7.3.8)	The customer should understand requirements around providing a copy of the personal data being processed to the individual. These may include requirements around the format of the copy (i.e. that it is machine readable), transferring the copy, etc. Where the customer uses a third-party system that provides the functionality to provide copies, they should utilize this functionality as necessary.	Information about capabilities in Microsoft services to allow you to obtain a copy of their personal data that you can include in the data you provide to data subjects. - <i>Office 365 Data Subject Requests for the GDPR</i> [8] see Step 6: Export	(15)(3), (15)(4), (20)(1), (20)(2), (20)(3), (20)(4)

Request management (7.3.9)	<p>The customer should understand requirements for accepting and responding to legitimate requests from individuals related to the processing of their personal data. Where the customer uses a third-party system, they should understand whether that system provides the capabilities for such handling of requests. If so, the customer should utilize such mechanisms to handle requests as necessary.</p>	<p>Information about capabilities in Microsoft services that you can use when defining the information you provide to data subjects as you manage data subject requests.</p> <ul style="list-style-type: none"> - <i>Office 365 Data Subject Requests for the GDPR</i> [8] <p>[8]Customer should understand requirements around automated personal data processing and where decisions are made by such automation. These may include providing information about the processing to an individual, objecting to such processing, or to obtain human intervention. Where such features are provided by a third-party system, the customer should ensure that the third party provides any required information or support.</p> <p>Information about any capabilities in Microsoft services that might support automated decision making that you can use in your accountability documentation, and templated information for data subjects about those capabilities.</p> <ul style="list-style-type: none"> - <i>Key Information from Office 365 for Customer Data Protection Impact Assessments</i> [10] 	(13)(2)(f), (14)(2)(g), (22)(1), (22)(3)

4. Privacy by design and default

Category	Customer Consideration	Supporting Microsoft documentation	Addresses GDPR Article(s)

Limit collection (7.4.1)	The customer should understand requirements around limits on collection of personal data (e.g. that the collection should be limited to what is needed for the specified purpose).	A description of the data collected by Microsoft services. - <i>Microsoft Online Services Terms, Data Protection Terms, see Processing of Personal Data; GDPR</i> [1] - <i>Key Information from Office 365 for Customer Data Protection Impact Assessments</i> [10]	(5)(1)(b), (5)(1)(c)
Limit processing (7.4.2)*	The customer is responsible for limiting the processing of personal data so that it is limited to what is adequate for the identified purpose.	A description of the data collected by Microsoft services. - <i>Microsoft Online Services Terms, Data Protection Terms, see Processing of Personal Data; GDPR</i> [1] - <i>Key Information from Office 365 for Customer Data Protection Impact Assessments</i> [10]	(25)(2)
Define and document PII minimization and de-identification objectives (7.4.3)	The customer should understand requirements around de-identification of personal data which may include, when it should be used, the extent to which it should de-identify, and instances when it cannot be used.	Microsoft applies de-identification and pseudonymization internally, where appropriate, to provide additional privacy safeguards for personal data.	(5)(1)(c)
Comply with identification levels (7.4.4)	The customer should use and comply with de-identification objectives and methods set by their organization.	Microsoft applies de-identification and pseudonymization internally, where appropriate, to provide additional privacy safeguards for personal data.	(5)(1)(c)
PII de-identification and deletion (7.4.5)	The customer should understand requirements around the retention of personal data past its use for the identified purposes. Where provided tooling by the system, the customer should utilize those tools to erase or delete as necessary.	Capabilities provided by Microsoft cloud services to support your data retention policies. - <i>Office 365 Data Subject Requests for the GDPR</i> [8] see <i>Step 5: Delete</i>	(5)(1)(c), (5)(1)(e), (6)(4)(e), (11)(1), (32)(1)(a)

Temporary files (7.4.6)	The customer should be aware of temporary files that may be created by the system that could lead to non-compliance with policies around processing of personal data (e.g. personal data might be retained in a temporary file longer than required or allowed). Where the system provides such tools for temporary file deletion or checking, the customer should utilize such tools to comply with requirements.	A description of capabilities provided by the service to identify personal data to support your temporary file policies. - Office 365 Data Subject Requests for the GDPR [8] see Step1: Discover	(5)(1)(c)
Retention (7.4.7)	The customer should determine how long personal data should be retained, taking into consideration the identified purposes.	Information about the retention of personal data by Microsoft services that you can include in documentation provided to data subjects. - <i>Microsoft Online Services Terms, Data Protection Terms, see Data Security, Retention</i> [1]	(13)(2)(a), (14)(2)(a)
Disposal (7.4.8)	The customer should utilize any deletion or disposal mechanisms provided by the system to delete personal data.	Capabilities provided by Microsoft cloud services to support your data deletion policies. -* Office 365 Data Subject Requests for the GDPR* [8] see Step 5: Delete	(5)(1)(f)
Collection procedures (7.4.9)	The customer should be aware of requirements around the accuracy of personal data (e.g., accuracy upon collection, keeping data up to date, etc.) and utilize any mechanisms provided by the system for such.	How Microsoft services support the accuracy of personal data, and any capabilities they provide to support your data accuracy policy. - <i>Office 365 Data Subject Requests for the GDPR</i> [8] see Step 3: Rectify	(5)(1)(d)
Transmission controls (7.4.10)	The customer should understand requirements around safeguarding the transmission of personal data, including who has access to transmission mechanisms, records of transmission, etc.	A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - <i>Key Information from Office 365 for Customer Data Protection Impact Assessments</i> [10]	(15)(2), (30)(1)(e), (5)(1)(f)

Identify basis for PII transfer (7.5.1)	The customer should be aware of requirements for transferring personal data (PII) to a different geographic location and document what measures are in place to meet such requirements.	A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - <i>Key Information from Office 365 for Customer Data Protection Impact Assessments</i> [10]	Articles (44), (45), (46), (47), (48), and (49)
Countries and organizations to which PII might be transferred (7.5.2)	The customer should understand, and be able to provide to the individual, the countries to which personal data is or may be transferred. Where a third-party/processor may perform this transfer, the customer should obtain this information from the processor.	A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - <i>Key Information from Office 365 for Customer Data Protection Impact Assessments</i> [10]	(30)(1)(e)
Records of transfers of PII (personal data) (7.5.3)	The customer should maintain all necessary and required records related to transfers of personal data. Where a third-party/processor performs the transfer, the customer should ensure that they maintain the appropriate records and obtain them as necessary.	A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - <i>Key Information from Office 365 for Customer Data Protection Impact Assessments</i> [10]	(30)(1)(e)
Records of PII disclosure to third parties (7.5.4)	The customer should understand requirements around recording to whom personal data has been disclosed. This may include disclosures to law enforcement, etc. Where a third-party/processor discloses the data, the customer should ensure that they maintain the appropriate records and obtain them as necessary.	Documentation provided about the categories of recipients of disclosures of personal data including available records of disclosure. - <i>Who can access your data and on what terms</i> [6]	(30)(1)(d)

Joint controller (7.5.5)	The customer should determine whether they are a joint controller with any other organization, and appropriately document and allocate responsibilities.	Documentation of Microsoft services that are a controller of personal information, including templated information that can be included in documentation to data subjects. - <i>Microsoft Online Services Terms, Data Protection Terms, see Processing of Personal Data; GDPR</i> [1]	

5. Data Protection & Security

Category	Customer Consideration	Supporting Microsoft documentation	Addresses GDPR Article(s)
Understanding the organization and its context (5.2.1)	Customers should determine their role in processing personal data (e.g. controller, processor, co-controller) to identify the appropriate requirements (regulatory, etc.) for processing personal data.	How Microsoft considers each service as either a processor or controller when processing personal data. - <i>Microsoft Online Services Terms, Data Protection Terms, see Processing of Personal Data; GDPR, Processor and Controller Roles and Responsibilities</i> [1]	(24)(3), (28)(10), (28)(5), (28)(6), (32)(3), (40)(1), (40)(2)(a), (40)(2)(b), (40)(2)(c), (40)(2)(d), (40)(2)(e), (40)(2)(f), (40)(2)(g), (40)(2)(h), (40)(2)(i), (40)(2)(j), (40)(2)(k), (40)(3), (40)(4), (40)(5), (40)(6), (40)(7), (40)(8), (40)(9), (40)(10), (40)(11), (41)(1), (41)(2)(a), (41)(2)(b), (41)(2)(c), (41)(2)(d), (41)(3), (41)(4), (41)(5), (41)(6), (42)(1), (42)(2), (42)(3), (42)(4), (42)(5), (42)(6), (42)(7), (42)(8)
Understanding the needs and expectations of interested parties (5.2.2)	Customers should identify parties that may have a role or interest in their processing of personal data (e.g. regulators, auditors, data subjects, contracted personal data processors), and be aware of requirements to engage such parties where required.	How Microsoft incorporates the views of all stakeholders in consideration of the risks involved in the processing of personal data. - <i>Key Information from Office 365 for Customer Data Protection Impact Assessments</i> [10] - <i>Office 365 ISMS Manual</i> [14] see 4.2 UNDERSTANDING THE NEEDS AND EXPECTATIONS OF INTERESTED PARTIES - Understanding the needs and expectations of interested parties 5.2.2 in <i>Compliance Manager</i>	(35)(9), (36)(1), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)

<p>Determining the scope of the information security management system (5.2.3, 5.2.4)</p>	<p>As part of any overall security or privacy program that a customer may have, they should include the processing of personal data and requirements relating to it.</p>	<p>How Microsoft services include the processing of personal data in information security management and privacy programs.</p> <ul style="list-style-type: none"> - <i>Microsoft Office 365 ISO/IEC 27001:2013 ISMS Statement of Applicability</i> [12] see A.19 - <i>SOC 2 Type 2 Audit Report</i> [11] - <i>Office 365 ISMS Manual</i> [14] see 4. Context of the Organization - 5.2.3 Determining the scope of the information security management system in Compliance Manager - 5.2.4 Information security management system in Compliance Manager 	<p>(32)(2)</p>
<p>Planning (5.3)</p>	<p>Customers should consider the handling of personal data as part of any risk assessment they complete and apply controls as they deem necessary to mitigate risk related to personal data they control.</p>	<p>How Microsoft services consider the risks specific to the processing of personal data as part of their overall security and privacy program.</p> <ul style="list-style-type: none"> - <i>Office 365 ISMS Manual</i> [14] see 5.2 Policy - 5.3 Planning in <i>Compliance Manager</i> 	<p>(32)(1)(b), (32)(2)</p>
<p>Information Security Policies (6.2)</p>	<p>The customer should augment any existing information security policies to include protection of personal data, including policies necessary for compliance with any applicable legislation.</p>	<p>Microsoft policies for information security and any specific measures for the protection of personal information.</p> <ul style="list-style-type: none"> - <i>Microsoft Office 365 (All-Up) ISO/IEC 27001:2013 ISMS Statement of Applicability</i> [12] see A.19 - <i>SOC 2 Type 2 Audit Report</i> [11] - 6.2 Information security policies in <i>Compliance Manager</i> 	<p>24(2)</p>

<p>Organization of Information Security Customer consideration (6.3)</p>	<p>The customer should, within their organization, define responsibilities for security and protection of personal data. This may include establishing specific roles to oversee privacy related matters, including a DPO. Appropriate training and management support should be provided to support these roles.</p>	<p>An overview of the role of Microsoft's Data Protection Officer, the nature of his duties, reporting structure and contact information.</p> <ul style="list-style-type: none"> - <i>Microsoft's Data Protection Officer</i> [18] - <i>Office 365 ISMS Manual</i> [14] see 5.3 <i>ORGANIZATIONAL ROLES, RESPONSIBILITIES, AND AUTHORITIES</i> - 6.3 Organization of information security in Compliance Manager 	<p>(37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)</p>
<p>Human Resource Security (6.4)</p>	<p>The customer should determine and assign responsibility for providing relevant training related to protecting personal data.</p>	<p>An overview of the role of Microsoft's Data Protection Officer, the nature of his duties, reporting structure and contact information.</p> <ul style="list-style-type: none"> - <i>Microsoft's Data Protection Officer</i> [18] - <i>Office 365 ISMS Manual</i> [14] see 5.3 <i>ORGANIZATIONAL ROLES, RESPONSIBILITIES, AND AUTHORITIES</i> - 6.4 Human resources security in Compliance Manager 	<p>(39)(1)(b)</p>
<p>Classification of Information (6.5.1)</p>	<p>The customer should explicitly consider personal data as part of a data classification scheme.</p>	<p>Capabilities in Office 365 to support personal data classification.</p> <ul style="list-style-type: none"> - <i>Office 365 Information Protection for GDPR</i> [5] see Architect a classification schema for personal data - 6.5.1 Classification of Information in Compliance Manager 	<p>(39)(1)(b)</p>
<p>Management of removable media (6.5.2)</p>	<p>The customer should determine internal policies for the use of removable media as it relates to the protection of personal data (e.g., encrypting devices).</p>	<p>How Microsoft services protect the security of personal information on any removable media.</p> <ul style="list-style-type: none"> - <i>FedRAMP Moderate FedRAMP System Security Plan</i> [3] see 13.10 Media Protection (MP) - Management of removable media in Compliance Manager 	<p>(32)(1)(a), (5)(1)(f)</p>

Physical media transfer (6.5.3)	The customer should determine internal policies for protecting personal data when transferring physical media (e.g. encryption).	How Microsoft services protect personal data during any transfer of physical media. - FedRAMP Moderate FedRAMP System Security Plan [3] see 13.10 Media Protection (MP) - 6.5.3 Physical media transfer in Compliance Manager	(32)(1)(a), (5)(1)(f)
User access management (6.6.1)	The customer should be aware of which responsibilities they have for access control within the service they are using, and manage those responsibilities appropriately, using the tools available.	The tools provided by Microsoft services to help you enforce access control. - Office 365 Security Documentation [2] see Protect access to data and services in Office 365 - 6.6.1 in Compliance Manager	(5)(1)(f)
User registration and de-registration (6.6.2)	The customer should manage user registration and de-registration within the service they utilize, using the tools available to them.	The tools provided by Microsoft services to help you enforce access control. - Office 365 Security Documentation [2] see Protect access to data and services in Office 365 - 6.6.2 User registration and de-registration in Compliance Manager	(5)(1)(f)
User access provisioning (6.6.3)	The customer should manage user profiles, especially for authorized access to personal data, within the service they utilize, using the tools available to them.	How Microsoft services support formal access control to personal data, including user IDs, roles, access to applications and the registration and de-registration of users. - Office 365 Security Documentation [2] see Protect access to data and services in Office 365 - Use Tenant Restrictions to manage access to SaaS cloud applications [15] - User access provisioning in Compliance Manager	(5)(1)(f)

Management of privileged access (6.6.4)	The customer should manage user ID's to facilitate tracking of access (especially to personal data), within the service they utilize, using the tools available to them.	How Microsoft services support formal access control to personal data, including user IDs, roles, and the registration and de-registration of users. <ul style="list-style-type: none"> - Office 365 Security Documentation [2] see Protect access to data and services in Office 365 - Use Tenant Restrictions to manage access to SaaS cloud applications [15] - 6.6.4 Management of privileged access in Compliance Manager 	(5)(1)(f)
Secure log on procedures (6.6.5)	The customer should utilize provided mechanisms in the service to ensure secure log on capabilities for their users where necessary.	How Microsoft services support internal access control policies related to personal data. <ul style="list-style-type: none"> - Who can access your data and on what terms [6] - 6.6.5 Secure log-on procedures in Compliance Manager 	(5)(1)(f)
Cryptography (6.7)	The customer should determine which data may need to be encrypted, and whether the service they are utilizing offers this capability. The customer should utilize encryption as needed, using the tools available to them.	How Microsoft services support encryption and pseudonymization to reduce the risk of processing personal data. <ul style="list-style-type: none"> - FedRAMP Moderate FedRAMP System Security Plan (SSP) see Cosmos pp29 - 6.7 Cryptography in Compliance Manager 	(32)(1)(a)
Secure disposal or re-use of equipment (6.8.1)	Where the customer uses cloud computing services (PaaS, SaaS, IaaS) they should understand how the cloud provider ensures that personal data is erased from storage space prior to that space being assigned to another customer.	How Microsoft services ensure that personal data is erased from storage equipment before that equipment is transferred or reused. <ul style="list-style-type: none"> - FedRAMP Moderate FedRAMP System Security Plan [3] see 13.10 Media Protection (MP) - 6.8.1 Secure disposal or re-use of equipment in Compliance Manager 	(5)(1)(f)

<i>Clear desk and clear screen policy (6.8.2)</i>	The customer should consider risks around hardcopy material that displays personal data, and potentially restrict the creation of such material. Where the system in use provides the capability to restrict this (e.g., settings to prevent printing or copying/pasting of sensitive data), the customer should consider the need to utilize those capabilities.	What Microsoft implements to manage hardcopy. - Microsoft maintains these controls internally, see Microsoft Office 365 ISO/IEC 27001:2013 ISMS Statement of Applicability [12] A.10.2, A.10.7 and A.4.1 - 6.8.2 Clear desk and clear screen policy in Compliance Manager	(5)(1)(f)
<i>Separation of development, testing and operational environments (6.9.1)</i>	The customer should consider the implications of using personal data in development and testing environments within their organization.	How Microsoft ensures that personal data is protected in development and test environments. - Microsoft Office 365 ISO/IEC 27001:2013 ISMS Statement of Applicability [12] see A.12.1.4 - 6.9.1 Separation of development, testing and operational environments in Compliance Manager	5(1)(f)
<i>Information backup (6.9.2)</i>	The customer should ensure that they use system provided capabilities to create redundancies in their data and test as necessary.	How Microsoft ensures the availability of data that may include personal data, how accuracy of restored data is ensured, and the tools and procedures Microsoft services provide to allow you to backup and restore data. - FedRAMP Moderate FedRAMP System Security Plan [3] see 10.9 Availability - 6.9.2 Information Backup in Compliance Manager	(32)(1)(c), (5)(1)(f)
<i>Event logging (6.9.3)</i>	The customer should understand the capabilities for logging provided by the system and utilize such capabilities to ensure that they can log actions related to personal data that they deem necessary.	The data Microsoft service records for you, including user activities, exceptions, faults and information security events, and how you can access those logs for use as part of your record keeping. - Search the audit log in Office 365 Security and Compliance Center [16] - 6.9.3 Event logging in Compliance Manager	(5)(1)(f)

<p>Protection of log information (6.9.4)</p>	<p>The customer should consider requirements for protecting log information that may contain personal data or that may contain records related to personal data processing. Where the system in use provides capabilities to protect logs, the customer should utilize these capabilities where necessary.</p>	<p>How Microsoft protects logs that may contain personal data.</p> <ul style="list-style-type: none"> - Search the audit log in Office 365 Security and Compliance Center [16] - 6.9.4 Protection of log information in Compliance Manager 	<p>(5)(1)(f)</p>
<p>Information transfer policies and procedures (6.10.1)</p>	<p>The customer should have procedures for cases where personal data may be transferred on physical media (such as a hard drive being moved between servers or facilities). These may include logs, authorizations, and tracking. Where a third-party or other processor may be transferring physical media, the customer should ensure that that organization has procedures in place to ensure security of the personal data.</p>	<p>How Microsoft services transfer physical media that may contain personal data, including the circumstances when transfer might occur, and the protective measures taken to protect the data.</p> <ul style="list-style-type: none"> - FedRAMP Moderate FedRAMP System Security Plan [3] see 13.10 Media Protection (MP) - 6.10.1 Information transfer policies and procedures in Compliance Manager 	<p>(5)(1)(f)</p>
<p>Confidentiality or non-disclosure agreements (6.10.2)</p>	<p>The customer should determine the need for confidentiality agreements or the equivalent for individuals with access to or responsibilities related to personal data.</p>	<p>How Microsoft services ensure that individuals with authorized access to personal data have committed themselves to confidentiality.</p> <ul style="list-style-type: none"> - SOC 2 Type 2 Audit Report [11] see CC1.4 pp33 - Confidentiality or non-disclosure agreements 6.10.2 in Compliance Manager 	<p>(5)(1)(f), (28)(3)(b), (38)(5)</p>
<p>Securing application services on public networks (6.11.1)</p>	<p>The customer should understand requirements for encryption of personal data, especially when sent over public networks. Where the system provides mechanisms to encrypt data, the customer should utilize those mechanisms where necessary.</p>	<p>Description of the measures Microsoft services take to protect data in transit, including encryption of the data, and how Microsoft services protect data that may contain personal data as it passes through public data networks, including any encryption measures.</p> <ul style="list-style-type: none"> - Encryption in the Microsoft Cloud [17] see <i>Encryption of Office 365 customer data in transit</i> - 6.11.1 Securing application services on public networks in Compliance Manager 	<p>(5)(1)(f), (32)(1)(a)</p>

Secure system engineering principles (6.11.2)	The customer should understand how systems are designed and engineered to consider protection of personal data. Where a customer uses a system engineered by a third-party, it is their responsibility to ensure that such protections have been considered.	How Microsoft services include personal data protection principles as a mandatory part of our secure design/engineering principles. - SOC 2 Type 2 Audit Report [11] see <i>Security Development Lifecycle</i> pp23, CC7.1 pp45 and [What is the Security De - Secure system engineering principles in Compliance Manager	(25)(1)
Supplier Relationships (6.12)	The customer should ensure that any information security and personal data protection requirements and that are the responsibility of a third-party are addressed in contractual information or other agreements. The agreements should also address the instructions for processing.	How Microsoft services address security and data protection in our agreements with our suppliers and how we ensure those agreements are effectively implemented. - Who can access your data and on what terms [6] - Contracts for sub-processors: Contracting with Microsoft [7] - 6.12 Supplier Relationships in Compliance Manager	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)
Management of information security incidents and improvements (6.13.1)	The customer should have processes for determining when a personal data breach has occurred.	How Microsoft services determine if a security incident is a breach of personal data, and how we communicate the breach to you. - Office 365 and Breach Notification Under the GDPR [9] - Management of information security incidents and improvements 6.13.1 in Compliance Manager	(33)(2)
Responsibilities and procedures (during information security incidents) (6.13.2)	The customer should understand and document their responsibilities during a data breach or security incident involving personal data. Responsibilities may include notifying required parties, communications with processors or other third-parties, and responsibilities within the customer's organization.	How to notify Microsoft services if you detect a security incident or breach of personal data - Office 365 and Breach Notification Under the GDPR [9] - 6.13.2 Responsibilities and procedures in Compliance Manager	(5)(1)(f), (33)(1), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2), (34)(3)(a), (34)(3)(b), (34)(3)(c), (34)(4)

<p>Response to information security incidents (6.13.3)</p>	<p>The customer should have processes for determining when a personal data breach has occurred.</p>	<p>Description of the information Microsoft services provide to help you decide if a breach of personal data has occurred.</p> <ul style="list-style-type: none"> - Office 365 and Breach Notification Under the GDPR [9] - 6.13.3 Response to information security incidents in Compliance Manager 	<p>(33)(1), (33)(2), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2)</p>
<p>Protection of records (6.15.1)</p>	<p>The customer should understand the requirements for records related to personal data processing that need to be maintained.</p>	<p>How Microsoft services store records relating to the processing of personal data</p> <ul style="list-style-type: none"> - Search the audit log in Office 365 Security and Compliance Center [16] - Microsoft Office 365 ISO/IEC 27001:2013 ISMS Statement of Applicability [12] see A.18.1.3 - Office 365 ISMS Manual [14] see 9 Performance evaluation 	<p>(5)(2), (24)(2)</p>
<p>Independent review of information security (6.15.2)</p>	<p>The customer should be aware of requirements for assessments of the security of personal data processing. This may include internal or external audits, or other measures for assessing the security of processing. Where the customer is dependent on another organization of third-party for all or part of the processing, they should collect information about such assessments performed by them.</p>	<p>How Microsoft services test and assesses the effectiveness of technical and organizational measures to ensure the security of processing, including any audits by third parties.</p> <ul style="list-style-type: none"> - Microsoft Online Services Terms, Data Protection Terms, see Data Security, Auditing Compliance [1] - Office 365 ISMS Manual [14] see 9 Performance evaluation - 6.15.2 Independent review of information security in Compliance Manager 	<p>(32)(1)(d), (32)(2)</p>

Technical compliance review (6.15.3)	<p>The customer should understand requirements for testing and evaluating the security of processing personal data. This may include technical tests such as penetration testing.</p> <p>Where the customer uses a third-party system or processor, they should understand what responsibilities they have for securing and testing the security (e.g. managing configurations to secure data and then testing those configuration settings).</p> <p>Where the third-party is responsible for all or part of the security of processing, the customer should understand what testing or evaluation the third-party performs to ensure the security of the processing.</p>	<p>How Microsoft services are tested security based on identified risks, including tests by third parties, and the types of technical tests and any available reports from the tests.</p> <ul style="list-style-type: none"> - Microsoft Online Services Terms, Data Protection Terms, see Data Security, Auditing Compliance [1] - For a listing of external certifications see <i>Microsoft Trust Center Compliance offerings</i> [13] - For more information about penetration testing your applications see FedRAMP Moderate FedRAMP System Security Plan (SSP) [3], CA-8 Penetration Testing (M) (H) pp204 - 6.15.3 Technical compliance review in Compliance Manager 	(32)(1)(d), (32)(2)

6. Bibliography of Resources and Links

ID	Documents	Link
1	Online Service Terms	http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=13754
2	Office 365 Security Documentation	https://support.office.com/article/protect-access-to-data-and-services-in-office-365-a6ef28a4-2447-4b43-aae2-f5af6d53c68e
3	FedRAMP Moderate FedRAMP System Security Plan (SSP)	https://servicetrust.microsoft.com/Page/MSComplianceGuide?command=Download&downloadType=Document&downloadId=053666de-e359-43ef-a7bb-3cf379208ed8&docTab=4ce99610-c9c0-11e7-8c2c-f908a777fa4d_FedRAMP_Reports

4	Microsoft Cloud Security Policy	https://servicetrust.microsoft.com/ViewPage/TrustDocuments?command=Download&downloadType=Document&downloadId=c83d1345-0cff-4beb-a521-27b837ed271a&docTab=6d000410-c9e9-11e7-9a91-892aae8839ad_FAQ_and_White_Papers
5	Office 365 Information Protection for GDPR	https://docs.microsoft.com/office365/enterprise/office-365-information-protection-for-gdpr
6	Who can access your data and on what terms?	https://www.microsoft.com/trustcenter/Privacy/Who-can-access-your-data-and-on-what-terms
7	Contracts for sub-processors: Contracting with Microsoft	https://www.microsoft.com/en-us/procurement/supplier-contracting.aspx#SSPA
8	365 Data Subject Requests for GDPR	https://aka.ms/DSROffice365
9	Office 365 and Breach Notification Under the GDPR	https://aka.ms/BreachOffice365
10	Key Information from Office 365 for Customer Data Protection Impact Assessments	https://docs.microsoft.com/microsoft-365/compliance/gdpr-dpia-office365
11	SOC 2 Type 2 Audit Report	https://servicetrust.microsoft.com/ViewPage/MSCComplianceGuide?command=Download&downloadType=Document&downloadId=0cf2cce9-972d-4a64-865f-b8e6eba4ed5e&docTab=4ce99610-c9c0-11e7-8c2c
12	Microsoft Office 365 ISO/IEC 27001:2013 ISMS Statement of Applicability	https://servicetrust.microsoft.com/ViewPage/MSCComplianceGuide?command=Download&downloadType=Document&downloadId=d7255c90-03e3-48a6-938d-e69d8f723c7a&docTab=4ce99610-c9c0-11e7-8c2c-f908a777fa4d_ISO_Reports
13	Microsoft Trust Center Compliance offerings	https://www.microsoft.com/trustcenter/compliance/complianceofferings
14	Office 365 ISMS Manual	https://servicetrust.microsoft.com/ViewPage/MSCComplianceGuide?command=Download&downloadType=Document&downloadId=72821313-c175-4857-b1f7-e3c5e6eb2db4&docTab=4ce99610-c9c0-11e7-8c2c-f908a777fa4d_ISO_Reports

15	Use Tenant Restrictions to manage access to SaaS cloud applications	https://docs.microsoft.com/azure/active-directory/active-directory-tenant-restrictions
16	Search the audit log in Office 365 Security and Compliance Center	https://support.office.com/article/Search-the-audit-log-in-the-Office-365-Security-Compliance-Center-0d4d0f35-390b-4518-800e-0c7ec95e946c
17	Encryption in the Microsoft Cloud	https://servicetrust.microsoft.com/ViewPage/TrustDocuments?command=Download&downloadType=Document&downloadId=ec66d938-6eb4-4d7d-b8c3-2168573bb534&docTab=6d000410-c9e9-11e7-9a91-892aae8839ad_FAQ_and_White_Papers
18	Microsoft's Data Protection Officer	https://docs.microsoft.com/microsoft-365/compliance/gdpr-data-protection-officer

Learn more

[Microsoft Trust Center](#)

[Service Trust Portal](#)

Azure accountability readiness checklist for the GDPR

2/22/2019 • 28 minutes to read • [Edit Online](#)

1. Introduction

This accountability readiness Checklist provides a convenient way to access information you may need to support GDPR when using Microsoft Azure. The checklist is organized using the titles and reference number (in parenthesis for each checklist topic) of a set of privacy and security controls for personal data processors drawn from ISO/IEC CD 27552 Information technology -- Security techniques -- Enhancement to ISO/IEC 27001 for privacy management – Requirements.

You can manage the items in this checklist with the Compliance Manager [16] by referencing the Control ID and Control Title under Customer Managed Controls in the GDPR tile. This control structure is also used to organize the presentation of the internal controls that Microsoft Azure implements to support GDPR, which you can download here <https://servicetrust.microsoft.com/ViewPage/TrustDocuments>.

This control structure is also used to organize the presentation of the internal controls that Microsoft Dynamics365 implements to support GDPR, which you can download here:

To purchase a copy of the complete draft ISO standard, please visit <https://shop.bsigroup.com/ProductDetail?pid=00000000030379002>

For more GDPR related documentation, visit <https://aka.ms/gdprgetstarted>.

2. Conditions for collection and processing

Category	Customer Consideration	Supporting Microsoft documentation	Addresses GDPR Article(s)
Identify lawful basis (7.2.2)	The customer should understand any requirements related to the lawful basis of processing, such as whether consent must first be given.	Windows Azure does not provide direct support for gaining user consent. A description of processing personal data by Microsoft services for inclusion in your accountability documentation is available here: <ul style="list-style-type: none">• <i>Key Information from Azure for Customer Data Protection Impact Assessments</i> [11]	(5)(1)(a), (6)(1)(a), (6)(1)(b), (6)(1)(c), (6)(1)(d), (6)(1)(e), (6)(1)(f), (6)(3), (6)4)(a), (6)(4)(b), (6)(4)(c), (6)(4)(d), (6)(4)(e), (8)(3), (9)(1), (9)(2)(b), (9)(2)(c), (9)(2)(d), (9)(2)(e), (9)(2)(f), (9)(2)(g), (9)(2)(h), (9)(2)(i), (9)(2)(j), (9)(3), (9)(4), (10), (17)(3)(a), (17)(3)(b), (17)(3)(c), (17)(3)(d), (17)(3)(e), (18)(2), (22)(2)(a), (22)(2)(b), (22)(2)(c), (22)(4)

Determine when consent is to be obtained (7.2.3)	The customer should understand legal or regulatory requirements for obtaining consent from individuals prior to processing personal data (when it is required, if the type of processing is excluded from the requirement, etc.), including how consent is collected.	Windows Azure does not provide direct support for gaining user consent.	(8)(1), (8)(2)
Obtain and record consent (7.2.4)	When it is determined to be required, the customer should appropriately obtain consent. The customer should also be aware of any requirements for how a request for consent is presented and collected.	Windows Azure does not provide direct support for gaining user consent.	(7)(1), (7)(2), (9)(2)(a)
Privacy impact assessment (7.2.5)	The customer should be aware of requirements for completing privacy impact assessments (when they should be performed, categories of data that might necessitate one, timing of completing the assessment).	How Microsoft services determine when to perform a DPIA, and an overview of the DPIA program at Microsoft including the involvement of the DPO, is provided in the Service Trust Portal Data Protection Impact Assessments (DPIAs) page. For support for your DPIAs see: - <i>Key Information from Azure for Customer Data Protection Impact Assessments [1]</i>	Article (35)
Contracts with PII Processors (7.2.6)	The customer should ensure that their contracts with processors include requirements for aiding with any relevant legal or regulatory obligations related to processing and protecting personal data.	The Microsoft contracts that require us to aid with your obligations under the GDPR, including support for the data subject's rights. See <i>Microsoft Online Services Terms, Data Protection Terms, see Processing of Personal Data; GDPR [1]</i>	(5)(2), (28)(3)(e), (28)(9)
Records related to processing PII (7.2.7)	The customer should maintain all necessary and required records related to processing personal data (e.g. purpose, security measures, etc.). Where some of these records must be provided by a sub-processor, the customer should ensure that they can obtain such records.	The tools provided by Microsoft services to help you maintain the records necessary demonstrate compliance and support for accountability under the GDPR. See the <i>Azure Security Documentation [2]</i> for <i>activity and diagnostic logging</i> and <i>logging of processing of personal data</i> .	(5)(2), (24)(1), (30)(1)(a), (30)(1)(b), (30)(1)(c), (30)(1)(d), (30)(1)(g), (30)(1)(f), (30)(3), (30)(4), (30)(5)

3. Rights of data subjects

Category	Customer Consideration	Supporting Microsoft documentation	Addresses GDPR Article(s)
Determining PII principals' rights and enabling exercise (7.3.1)	<p>The customer should understand requirements around the rights of individuals related to the processing of their personal data. These rights may include things such as access, correction, and erasure. Where the customer uses a third-party system, they should determine which (if any) parts of the system provide tools related to enabling individuals to exercise their rights (e.g. to access their data). Where the system provides such capabilities, the customer should utilize them as necessary.</p>	<p>The capabilities Microsoft provides to help you support data subject rights. See <i>Azure Data Subject Requests for the GDPR</i> [9], Microsoft Azure (All-Up) ISO/IEC 27001:2013 ISMS Statement of Applicability see ISO/IEC 27018 control A.1.1.</p>	(12)(2)
Determining information for PII principals (data subjects) (7.3.2)	<p>The customer should understand requirements for the types of information about processing of personal data that is to be available to be provided to the individual. This may include things such as:</p> <ul style="list-style-type: none"> - Contact details about the controller or its representative; - information about the processing (purposes, international transfer and related safeguards, retention period, etc.); - information on how the principal may access and/or amend their personal data; requesting erasure or restriction of processing; receiving a copy of their personal data, and portability of their personal data - How and from where the personal data were obtained (if not obtained from the principal directly) - information about the right to lodge a complaint and to whom; - information regarding 	<p>Information about Microsoft services that you can include in the data you provide to data subjects. See <i>Azure Data Subject Requests for the GDPR</i> [9], <i>Key Information from Azure for Customer Data Protection Impact Assessments</i> [11] and <i>Who can access your data and on what terms</i> [7].</p>	(11)(2), (13)(1)(a), (13)(1)(b), (13)(1)(c), (13)(1)(d), (13)(1)(e), (13)(1)(f), (13)(2)(c), (13)(2)(d), (13)(2)(e), (13)(3), (13)(4), (14)(1)(a), (14)(1)(b), (14)(1)(c), (14)(1)(d), (14)(1)(e), (14)(1)(f), (14)(2)(b), (14)(2)(e), (14)(2)(f), (14)(3)(a), (14)(3)(b), (14)(3)(c), (14)(4), (14)(5)(a), (14)(5)(b), (14)(5)(c), (14)(5)(d), (15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (15)(2), (18)(3), (21)(4)

	<p>corrections to personal data;</p> <ul style="list-style-type: none"> - Notification that the organization is no longer in position to identify the data subject (PII principal), in cases where the processing no longer requires the identification of the data subject; - Transfers and/or disclosures of personal data; - existence of automated decision making based solely on automated processing of personal data; - information regarding the frequency with which information to the data subject is updated and provided (e.g. "just in time" notification, organization defined frequency, etc.). <p>Where the customer uses third-party systems or processors, they should determine which (if any) of this information may need to be provided by them and ensure that they can obtain the required information from the third-party.</p>		
<i>Providing information to PII principals (7.3.3)</i>	The customer should comply with any requirements around how/when/in what form the required information is to be given to an individual related to the processing of their personal data. In cases where a third-party may provide required information, the customer should ensure that it is within the parameters required by the GDPR.	Templated information about Microsoft services that you can include in the data you provide to data subjects. See <i>Azure Data Subject Requests for the GDPR</i> [9] and <i>Key Information from Azure for Customer Data Protection Impact Assessments</i> [11].	(11)(2), (12)(1), (12)(7), (13)(3), (21)(4)
<i>Provide mechanism to modify or withdraw consent (7.3.4)</i>	The customer should understand requirements for informing users about their right to access, correct, and/or erase their personal data and for providing a mechanism for which them to do so. If a third-party system is used and provides this mechanism as part of its functionality, the customer should utilize that functionality as necessary.	Information about capabilities in Microsoft services that you can use when defining the information you provide to data subjects when requesting consent. - <i>Azure Data Subject Requests for the GDPR</i> [9]	(7)(3), (13)(2)(c), (14)(2)(d), (18)(1)(a), (18)(1)(b), (18)(1)(c), (18)(1)(d)

Provide mechanism to object to processing (7.3.5)	The customer should understand requirements around rights of data subjects. Where an individual has a right to object to processing, the customer should inform them, and have a way for the individual to register their objection.	Information about Microsoft services relating to object to processing that you can include in the data you provide to data subjects. - <i>Azure Data Subject Requests for the GDPR</i> [9] see Step 4: Restrict	(13)(2)(b), (14)(2)(c), (21)(1), (21)(2), (21)(3), (21)(5), (21)(6)
Sharing the exercising of PII principals' rights (7.3.6)	The customer should understand requirements for notifying third-parties with whom personal data has been shared of instances of data modification based on the exercise of individual rights (e.g. an individual requesting erasure or modification, etc.).	Information about capabilities in Microsoft services that allow you to discover personal data that you have shared with third parties. - <i>Azure Data Subject Requests for the GDPR</i> [9]	(19)
Correction or erasure (7.3.7)	The customer should understand requirements for informing users about their right to access, correct, and/or erase their personal data and for providing a mechanism for which them to do so. If a third-party system is used and provides this mechanism as part of its functionality, the customer should utilize that functionality as necessary.	Templated information about Microsoft services relating to their ability to access, correct or erase personal data that you can include in the data you provide to data subjects. - <i>Azure Data Subject Requests for the GDPR</i> [9] see "Step 5: Delete" - <i>Privacy and personal data in Intune</i> [15] see "View and correct personal data and Audit, export, or delete personal data in Intune."	(5)(1)(d), (13)(2)(b), (14)(2)(c), (16), (17)(1)(a), (17)(1)(b), (17)(1)(c), (17)(1)(d), (17)(1)(e), (17)(1)(f), (17)(2)
Providing copy of PII processed (7.3.8)	The customer should understand requirements around providing a copy of the personal data being processed to the individual. These may include requirements around the format of the copy (i.e. that it is machine readable), transferring the copy, etc. Where the customer uses a third-party system that provides the functionality to provide copies, they should utilize this functionality as necessary.	Information about capabilities in Microsoft services to allow you to obtain a copy of their personal data that you can include in the data you provide to data subjects. • <i>Azure Data Subject Requests for the GDPR</i> [9] see Step 6: Export • <i>Privacy and personal data in Intune</i> [15] see Audit, export, or delete personal data in Intune	(15)(3), (15)(4), (20)(1), (20)(2), (20)(3), (20)(4)

Request management (7.3.9)	The customer should understand requirements for accepting and responding to legitimate requests from individuals related to the processing of their personal data. Where the customer uses a third-party system, they should understand whether that system provides the capabilities for such handling of requests. If so, the customer should utilize such mechanisms to handle requests as necessary.	Information about capabilities in Microsoft services that you can use when defining the information you provide to data subjects as you manage data subject requests. - <i>Azure Data Subject Requests for the GDPR</i> [9]	(12)(3), (12)(4), (12)(5), (12)(6), (15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h)
Automated decision making (7.3.10)	The customer should understand requirements around automated personal data processing and where decisions are made by such automation. These may include providing information about the processing to an individual, objecting to such processing, or to obtain human intervention. Where such features are provided by a third-party system, the customer should ensure that the third party provides any required information or support.	Information about any capabilities in Microsoft services for that might support automated decision making that you can use in your accountability documentation, and templated information for data subjects about those capabilities. - <i>Key Information from Azure for Customer Data Protection Impact Assessments</i> [11]	(13)(2)(f), (14)(2)(g), (22)(1), (22)(3)

4. Privacy by design and default

Category	Customer Consideration	Supporting Microsoft documentation	Addresses GDPR Article(s)

Limit collection (7.4.1)	The customer should understand requirements around limits on collection of personal data (e.g. that the collection should be limited to what is needed for the specified purpose).	A description of the data collected by Microsoft services. - <i>Microsoft Online Services Terms, Data Protection Terms, see Processing of Personal Data; GDPR [1]</i> - Key Information from Azure for Customer Data Protection Impact Assessments [11] - <i>Privacy and personal data in Intune</i> [15]*see Data collection in Intune"	(5)(1)(b), (5)(1)(c)
Limit processing (7.4.2)	The customer is responsible for limiting the processing of personal data so that it is limited to what is adequate for the identified purpose.	A description of the data collected by Microsoft services. - Microsoft Online Services Terms, Data Protection Terms, see Processing of Personal Data; GDPR [1] - Key Information from Azure for Customer Data Protection Impact Assessments [11] - <i>Privacy and personal data in Intune</i> [15] "see Data storage and processing in Intune"	(25)(2)
Define and document PII minimization and de-identification objectives (7.4.3)	The customer should understand requirements around de-identification of personal data which may include, when it should be used, the extent to which it should de-identify, and instances when it cannot be used.	Microsoft applies de-identification and pseudonymization internally, where appropriate, to provide additional privacy safeguards for personal data.	(5)(1)(c)
Comply with identification levels (7.4.4)	The customer should use and comply with de-identification objectives and methods set by their organization.	Microsoft applies de-identification and pseudonymization internally, where appropriate, to provide additional privacy safeguards for personal data.	(5)(1)(c)
PII de-identification and deletion (7.4.5)	The customer should understand requirements around the retention of personal data past its use for the identified purposes. Where provided tooling by the system, the customer should utilize those tools to erase or delete as necessary.	Capabilities provided by Microsoft Services to support your data retention policies. - <i>Azure Data Subject Requests for the GDPR</i> "see Step 5: Delete"	(5)(1)(c), (5)(1)(e), (6)(4)(e), (11)(1), (32)(1)(a)

Temporary files (7.4.6)	The customer should be aware of temporary files that may be created by the system that could lead to non-compliance with policies around processing of personal data (e.g. personal data might be retained in a temporary file longer than required or allowed). Where the system provides such tools for temporary file deletion or checking, the customer should utilize such tools to comply with requirements.	A description of capabilities provided by the service to identify personal data to support your temporary file policies. - <i>Azure Data Subject Requests for the GDPR</i> "see Step 1: Discover"	(5)(1)(c)
Retention (7.4.7)	The customer should determine how long personal data should be retained, taking into consideration the identified purposes.	Information about the retention of personal data by Microsoft services that you can include in documentation provided to data subjects. - <i>Microsoft Online Services Terms, Data Protection Terms, see Data Security, Retention</i> [1]	(13)(2)(a), (14)(2)(a)
Disposal (7.4.8)	The customer should utilize any deletion or disposal mechanisms provided by the system to delete personal data.	Capabilities provided by Microsoft Services to support your data deletion policies. - <i>Azure Data Subject Requests for the GDPR</i> [9] see Step 5: Delete	(5)(1)(f)
Collection procedures (7.4.9)	The customer should be aware of requirements around the accuracy of personal data (e.g., accuracy upon collection, keeping data up to date, etc.) and utilize any mechanisms provided by the system for such.	How Microsoft services support the accuracy of personal data, and any capabilities they provide to support your data accuracy policy. - <i>Azure Data Subject Requests for the GDPR</i> [9] see Step 3: Rectify	(5)(1)(d)
Transmission controls (7.4.10)	The customer should understand requirements around safeguarding the transmission of personal data, including who has access to transmission mechanisms, records of transmission, etc.	A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - <i>Key Information from Azure for Customer Data Protection Impact Assessments</i> [11]	(5)(1)(f)

Identify basis for PII transfer (7.5.1)	The customer should be aware of requirements for transferring personal data (PII) to a different geographic location and document what measures are in place to meet such requirements.	A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - <i>Key Information from Azure for Customer Data Protection Impact Assessments</i> [11]	Articles (44), (45), (46), (47), (48), and (49)
Countries and organizations to which PII might be transferred (7.5.2)	The customer should understand, and be able to provide to the individual, the countries to which personal data is or may be transferred. Where a third-party/processor may perform this transfer, the customer should obtain this information from the processor.	A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - <i>Key Information from Azure for Customer Data Protection Impact Assessments</i> [11] - Who can access your data and on what terms [7]	(30)(1)(e)
Records of transfers of PII (personal data) (7.5.3)	The customer should maintain all necessary and required records related to transfers of personal data. Where a third-party/processor performs the transfer, the customer should ensure that they maintain the appropriate records and obtain them as necessary.	Look here and here for... A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - <i>Key Information from Azure for Customer Data Protection Impact Assessments</i> [11] - Who can access your data and on what terms [7]	(30)(1)(e)
Records of PII disclosure to third parties (7.5.4)	The customer should understand requirements around recording to whom personal data has been disclosed. This may include disclosures to law enforcement, etc. Where a third-party/processor discloses the data, the customer should ensure that they maintain the appropriate records and obtain them as necessary.	Documentation provided about the categories of recipients of disclosures of personal data including available records of disclosure. - Who can access your data and on what terms [7] - Privacy and personal data in Intune [15] see <i>Data security and sharing in Intune</i>	(30)(1)(d)

Joint controller (7.5.5)	The customer should determine whether they are a joint controller with any other organization, and appropriately document and allocate responsibilities.	As specified by the Online Services Terms (OST), Microsoft, as a data processor, processes Customer Data only to provide the requested services to our customer, the data controller. - <i>Microsoft Online Services Terms, Data Protection Terms, see Processing of Personal Data; GDPR</i> [1]	(26)(1), (26)(2),

5. Data Protection & Security

Category	Customer Consideration	Supporting Microsoft documentation	Addresses GDPR Article(s)
Understanding the organization and its context (5.2.1)	Customers should determine their role in processing personal data (e.g. controller, processor, co-controller) to identify the appropriate requirements (regulatory, etc.) for processing personal data.	How Microsoft considers each service as either a processor or controller when processing personal data. - <i>Microsoft Online Services Terms, Data Protection Terms, see "Processing of Personal Data; GDPR, Processor and Controller Roles and Responsibilities"</i> [1]	(24)(3), (28)(10), (28)(5), (28)(6), (32)(3), (40)(1), (40)(2)(a), (40)(2)(b), (40)(2)(c), (40)(2)(d), (40)(2)(e), (40)(2)(f), (40)(2)(g), (40)(2)(h), (40)(2)(i), (40)(2)(j), (40)(2)(k), (40)(3), (40)(4), (40)(5), (40)(6), (40)(7), (40)(8), (40)(9), (40)(10), (40)(11), (41)(1), (41)(2)(a), (41)(2)(b), (41)(2)(c), (41)(2)(d), (41)(3), (41)(4), (41)(5), (41)(6), (42)(1), (42)(2), (42)(3), (42)(4), (42)(5), (42)(6), (42)(7), (42)(8)
Understanding the needs and expectations of interested parties (5.2.2)	Customers should identify parties that may have a role or interest in their processing of personal data (e.g. regulators, auditors, data subjects, contracted personal data processors), and be aware of requirements to engage such parties where required.	How Microsoft incorporates the views of all stakeholders in consideration of the risks involved in the processing of personal data. - <i>Key Information from Azure for Customer Data Protection Impact Assessments</i> [1]	(35)(9), (36)(1), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)

Determining the scope of the information security management system (5.2.3, 5.2.4)	As part of any overall security or privacy program that a customer may have, they should include the processing of personal data and requirements relating to it.	How Microsoft services include the processing of personal data in information security management and privacy programs. <ul style="list-style-type: none"> • <i>Microsoft Azure (All-Up) ISO/IEC 27001:2013 ISMS Statement of Applicability</i> [13] see A.19-A.29 • SOC 2 Type 2 Audit Report [12] 	(32)(2)
Planning (5.3)	Customers should consider the handling of personal data as part of any risk assessment they complete and apply controls as they deem necessary to mitigate risk related to personal data they control.	How Microsoft services consider the risks specific to the processing of personal data as part of their overall security and privacy program. <ul style="list-style-type: none"> - <i>Microsoft Azure (All-Up) ISO/IEC 27001:2013 ISMS Statement of Applicability</i> [13] see A.19-A.29 	(32)(1)(b), (32)(2)
Information Security Policies (6.2)	The customer should augment any existing information security policies to include protection of personal data, including policies necessary for compliance with any applicable legislation.	Microsoft policies for information security and any specific measures for the protection of personal information. <ul style="list-style-type: none"> - <i>Microsoft Azure (All-Up) ISO/IEC 27001:2013 ISMS Statement of Applicability</i> [13] see A.19-A.29 - SOC 2 Type 2 Audit Report [12] 	(24)(2)
Organization of Information Security Customer consideration(6.3)	The customer should, within their organization, define responsibilities for security and protection of personal data. This may include establishing specific roles to oversee privacy related matters, including a DPO. Appropriate training and management support should be provided to support these roles.	An overview of the role of Microsoft's Data Protection Officer, the nature of his duties, reporting structure and contact information. <ul style="list-style-type: none"> - Microsoft DPO Information [17] 	(37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)
Human Resource Security (6.4)	The customer should determine and assign responsibility for providing relevant training related to protecting personal data.	An overview of the role of Microsoft's Data Protection Officer, the nature of his duties, reporting structure and contact information. <ul style="list-style-type: none"> - <i>Microsoft Cloud Security Policy</i> [4] see 03. Human Resources Security - <i>FedRAMP Moderate FedRAMP System Security Plan</i> [3] see 13.2 "Awareness and Training" (AT) 	(39)(1)(b)

Classification of Information (6.5.1)	The customer should explicitly consider personal data as part of a data classification scheme.	How Microsoft considers personal data in data classification, tagging and tracking information. - <i>GDPR Considerations for Data Controllers Using Windows</i> [11] see Data tagging and tracking	(39)(1)(b)
Management of removable media (6.5.2)	The customer should determine internal policies for the use of removable media as it relates to the protection of personal data (e.g., encrypting devices).	How Microsoft services protect the security of personal information on any removable media. - <i>FedRAMP Moderate FedRAMP System Security Plan</i> [3] see 13.10 Media Protection (MP)	(32)(1)(a), (5)(1)(f)
Physical media transfer (6.5.3)	The customer should determine internal policies for protecting personal data when transferring physical media (e.g. encryption).	How Microsoft services protects personal data during any transfer of physical media. - FedRAMP Moderate FedRAMP System Security Plan [3] see 13.10 Media Protection (MP)	(32)(1)(a), (5)(1)(f)
User access management (6.6.1)	The customer should be aware of which responsibilities they have for access control within the service they are using, and manage those responsibilities appropriately, using the tools available.	The tools provided by Microsoft services to help you enforce access control. - Azure Security Documentation egistration of users. - Azure Security Documentation [2] see Protect personal data with identity and access controls	(5)(1)(f)
User registration and de-registration (6.6.2)	The customer should manage user registration and de-registration within the service they utilize, using the tools available to them.	The tools provided by Microsoft services to help you enforce access control. - Azure Security Documentation egistration of users. - Azure Security Documentation [2] see Protect personal data with identity and access controls	(5)(1)(f)
User access provisioning (6.6.3)	The customer should manage user profiles, especially for authorized access to personal data, within the service they utilize, using the tools available to them.	How Microsoft services support formal access control to personal data, including user IDs, roles, and the registration and de-registration of users. - Azure Security Documentation [2] see Protect personal data with identity and access controls	(5)(1)(f)

Management of privileged access (6.6.4)	The customer should manage user ID's to facilitate tracking of access (especially to personal data), within the service they utilize, using the tools available to them.	How Microsoft services support formal access control to personal data, including user IDs, roles, and the registration and de-registration of users. - Azure Security Documentation [2] see Protect personal data with identity and access controls	(5)(1)(f)
Secure log on procedures (6.6.5)	The customer should utilize provided mechanisms in the service to ensure secure log on capabilities for their users where necessary.	How Microsoft services support internal access control policies related to personal data. - Who can access your data and on what terms [7]	(5)(1)(f)
Cryptography (6.7)	The customer should determine which data may need to be encrypted, and whether the service they are utilizing offers this capability. The customer should utilize encryption as needed, using the tools available to them.	How Microsoft services support encryption and pseudonymization to reduce the risk of processing personal data. - Azure Security Documentation [2] see Protect personal data at rest with encryption and Protect personal data in transit with encryption and https://docs.microsoft.com/azure/security/security-azure-encryption-overview	(32)(1)(a)
Secure disposal or re-use of equipment (6.8.1)	Where the customer uses cloud computing services (PaaS, SaaS, IaaS) they should understand how the cloud provider ensures that personal data is erased from storage space prior to that space being assigned to another customer.	How Microsoft services ensure that personal data is erased from storage equipment before that equipment is transferred or reused. - Microsoft Azure Data Security (Data Cleansing and Leakage) [5]	(5)(1)(f)
Clear desk and clear screen policy (6.8.2)	The customer should consider risks around hardcopy material that displays personal data, and potentially restrict the creation of such material. Where the system in use provides the capability to restrict this (e.g., settings to prevent printing or copying/pasting of sensitive data), the customer should consider the need to utilize those capabilities.	What Microsoft implements to manage hardcopy. - Microsoft maintains these controls internally, see <i>Microsoft Azure (All-Up) ISO/IEC 27001:2013 ISMS Statement of Applicability</i> [15] A.11.2.9	(5)(1)(f)

Separation of development, testing and operational environments (6.9.1)	<p>The customer should consider the implications of using personal data in development and testing environments within their organization.</p>	<p>How Microsoft ensures that personal data is protected in development and test environments.</p> <ul style="list-style-type: none"> - <i>Microsoft Azure (All-Up) ISO/IEC 27001:2013 ISMS Statement of Applicability</i> [13] see A.12.1.4 - Azure Standard Response to RFI on Security, Privacy, and Compliance [6]. - Azure Control 530: The production environment is separated from development/testing[16]. 	5(1)(f)
Information backup (6.9.2)	<p>The customer should ensure that they use system provided capabilities to create redundancies in their data and test as necessary.</p>	<p>How Microsoft ensures the availability of data that may include personal data, how accuracy of restored data is ensured, and the tools and procedures Microsoft services provide to allow you to backup and restore data.</p> <ul style="list-style-type: none"> - FedRAMP Moderate FedRAMP System Security Plan [3] see 10.9 Availability 	(32)(1)(c), (5)(1)(f)
Event logging (6.9.3)	<p>The customer should understand the capabilities for logging provided by the system and utilize such capabilities to ensure that they can log actions related to personal data that they deem necessary.</p>	<p>The data Microsoft service records for you, including user activities, exceptions, faults and information security events, and how you can access those logs for use as part of your record keeping.</p> <ul style="list-style-type: none"> - Azure Security Documentation egistration of users. - Azure Security Documentation [2] see Document protection of personal data with Azure reporting tools 	(5)(1)(f)
Protection of log information (6.9.4)	<p>The customer should consider requirements for protecting log information that may contain personal data or that may contain records related to personal data processing. Where the system in use provides capabilities to protect logs, the customer should utilize these capabilities where necessary.</p>	<p>How Microsoft protects logs that may contain personal data.</p> <ul style="list-style-type: none"> - Azure Security Documentation [2] see Document protection of personal data with Azure reporting tools 	(5)(1)(f)

<p>Information transfer policies and procedures (6.10.1)</p>	<p>The customer should have procedures for cases where personal data may be transferred on physical media (such as a hard drive being moved between servers or facilities). These may include logs, authorizations, and tracking. Where a third-party or other processor may be transferring physical media, the customer should ensure that that organization has procedures in place to ensure security of the personal data.</p>	<p>How Microsoft services transfer physical media that may contain personal data, including the circumstances when transfer might occur, and the protective measures taken to protect the data.</p> <ul style="list-style-type: none"> - <i>FedRAMP Moderate FedRAMP System Security Plan</i> [3] see 13.10 Media Protection (MP) 	<p>(5)(1)(f)</p>
<p>Confidentiality or non-disclosure agreements (6.10.2)</p>	<p>The customer should determine the need for confidentiality agreements or the equivalent for individuals with access to or responsibilities related to personal data.</p>	<p>How Microsoft services ensure that individuals with authorized access to personal data have committed themselves to confidentiality.</p> <ul style="list-style-type: none"> - <i>SOC 2 Type 2 Audit Report</i> [12] see CC1.4 pp72, SOC2 - 13 	<p>(5)(1)(f), (28)(3)(b), (38)(5)</p>
<p>Securing application services on public networks (6.11.1)</p>	<p>The customer should understand requirements for encryption of personal data, especially when sent over public networks. Where the system provides mechanisms to encrypt data, the customer should utilize those mechanisms where necessary.</p>	<p>Description of the measures Microsoft services take to protect data in transit, including encryption of the data, and how Microsoft services protect data that may contain personal data as it passes through public data networks, including any encryption measures.</p> <ul style="list-style-type: none"> - <i>Azure Security Documentation</i> [2] see Protect personal data in transit with encryption 	<p>(5)(1)(f), (32)(1)(a)</p>
<p>Secure system engineering principles (6.11.2)</p>	<p>The customer should understand how systems are designed and engineered to consider protection of personal data. Where a customer uses a system engineered by a third-party, it is their responsibility to ensure that such protections have been considered.</p>	<p>How Microsoft services include personal data protection principles as a mandatory part of our secure design/engineering principles.</p> <ul style="list-style-type: none"> - <i>SOC 2 Type 2 Audit Report</i> [12] see CC7.1 pp90 and What is the Security Development Lifecycle? 	<p>(25)(1)</p>

Supplier Relationships (6.12)	The customer should ensure that any information security and personal data protection requirements and that are the responsibility of a third-party are addressed in contractual information or other agreements. The agreements should also address the instructions for processing	How Microsoft services address security and data protection in our agreements with our suppliers and how we ensure those agreements are effectively implemented. - Who can access your data and on what terms [7]	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)
Management of information security incidents and improvements (6.13.1)	The customer should have processes for determining when a personal data breach has occurred.	How Microsoft services determine if a security incident is a breach of personal data, and how we communicate the breach to you. - <i>Azure and Breach Notification Under the GDPR</i> [10]	(33)(2)
Responsibilities and procedures (during information security incidents) (6.13.2)	The customer should understand and document their responsibilities during a data breach or security incident involving personal data. Responsibilities may include notifying required parties, communications with processors or other third-parties, and responsibilities within the customer's organization.	How to notify Microsoft services if you detect a security incident or breach of personal data. - <i>Azure and Breach Notification Under the GDPR</i> [10]	(5)(1)(f), (33)(1), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2), (34)(3)(a), (34)(3)(b), (34)(3)(c), (34)(4)
Response to information security incidents (6.13.3)	The customer should have processes for determining when a personal data breach has occurred.	Description of the information Microsoft services provide to help you decide if a breach of personal data has occurred. - <i>Azure and Breach Notification Under the GDPR</i> [10]	(33)(1), (33)(2), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2)
Protection of records (6.15.1)	The customer should understand the requirements for records related to personal data processing that need to be maintained.	How Microsoft services store records relating to the processing of personal data. - Azure Security Documentation registration of users. - Azure Security Documentation [2] see Document protection of personal data with Azure reporting tools	(5)(2), (24)(2)

Independent review of information security (6.15.2)	The customer should be aware of requirements for assessments of the security of personal data processing. This may include internal or external audits, or other measures for assessing the security of processing. Where the customer is dependent on another organization of third-party for all or part of the processing, they should collect information about such assessments performed by them.	How Microsoft services test and assesses the effectiveness of technical and organizational measures to ensure the security of processing, including any audits by third parties. <i>Microsoft Online Services Terms, Data Protection Terms, see Data Security, Auditing Compliance [1]</i>	(32)(1)(d), (32)(2)
Technical compliance review (6.15.3)	The customer should understand requirements for testing and evaluating the security of processing personal data. This may include technical tests such as penetration testing. Where the customer uses a third-party system or processor, they should understand what responsibilities they have for securing and testing the security (e.g. managing configurations to secure data and then testing those configuration settings). Where the third-party is responsible for all or part of the security of processing, the customer should understand what testing or evaluation the third-party performs to ensure the security of the processing.	How Microsoft services are tested security based on identified risks, including tests by third parties, and the types of technical tests and any available reports from the tests. - <i>Microsoft Online Services Terms, Data Protection Terms, see Data Security, Auditing Compliance [1]</i> - For a listing of external certifications see Microsoft Trust Center Compliance offerings [14] - For more information about penetration testing your applications see <i>Azure Security Documentation [2] Pen Testing</i>	(32)(1)(d), (32)(2)

6. Bibliography of Resources and Links

ID	Description	URL
1	Online Services Terms	http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeID=46

2	Azure Security Documentation on docs.microsoft.com	https://docs.microsoft.com/azure/security/ , see Governance and compliance, GDPR
3	FedRAMP Moderate FedRAMP System Security Plan (SSP)	https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide?command=Download&downloadType=Document&downloadId=e46a519a-bcf6-4dc2-8f60-6d0e4e00a85e&docTab=4ce99610-c9c0-11e7-8c2c-f908a777fa4d_FedRAMP_Reports
4	Microsoft Cloud Security Policy	https://servicetrust.microsoft.com/ViewPage/TrustDocuments?command=Download&downloadType=Document&downloadId=5868ecc8-50b7-4f91-b43f-640e2b99e86e&docTab=6d000410-c9e9-11e7-9a91-892aae8839ad_FAQ_and_White_Papers
5	Microsoft Azure Data Security (Data Cleansing and Leakage)	https://blogs.msdn.microsoft.com/walterm/2014/09/04/microsoft-azure-data-security-data-cleansing-and-leakage/
6	Azure Standard Response to RFI on Security, Privacy, and Compliance	https://gallery.technet.microsoft.com/Azure-Standard-Response-to-5de19cb6
7	Who can access your data and on what terms	https://www.microsoft.com/trustcenter/Privacy/Who-can-access-your-data-and-on-what-terms
8	Contracts for sub-processors: Contracting with Microsoft	https://www.microsoft.com/en-us/procurement/supplier-contracting.aspx#SSPA
9	Azure Data Subject Requests for the GDPR	https://docs.microsoft.com/microsoft-365/compliance/gdpr-dsr-azure
10	Azure and Breach Notification Under the GDPR	https://docs.microsoft.com/microsoft-365/compliance/gdpr-breach-azure
11	Key Information from Azure for Customer Data Protection Impact Assessments	https://aka.ms/DPIAAzure
12	SOC 2 Type 2 Audit Report [12]	https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide?command=Download&downloadType=Document&downloadId=3c7123a5-f507-48b7-8dce-cd948e6150e6&docTab=4ce99610-c9c0-11e7-8c2c-f908a777fa4d_SOC_%2F_SSAE_16_Reports

13	Microsoft Azure (All-Up) ISO/IEC 27001:2013 ISMS Statement of Applicability	https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide?command=Download&downloadType=Document&downloadId=47d89200-b24b-491d-b657-7c523ddfb6f9&docTab=4ce99610-c9c0-11e7-8c2c-f908a777fa4d_ISO_Reports
14	Microsoft Trust Center Compliance offerings	https://www.microsoft.com/trustcenter/compliance/complianceofferings
15	Privacy and personal data in Intune	https://review.docs.microsoft.com/intune/privacy-personal-data
16	Complete downloadable Azure GDPR Control Set	https://aka.ms/GDPRControls or via Compliance Manager Tool at https://servicetrust.microsoft.com/ComplianceManager
17	Microsoft DPO Information	https://aka.ms/GDPRDPO

Learn more

[Microsoft Trust Center](#)

[Secure Trust Portal](#)

Dynamics 365 accountability readiness checklist for the GDPR

2/22/2019 • 29 minutes to read • [Edit Online](#)

1. Introduction

This accountability readiness checklist provides a convenient way to access information you may need to support GDPR when using Microsoft Dynamics 365. The checklist is organized using the titles and reference number (in parenthesis for each checklist topic) of a set of privacy and security controls for personal data processors drawn from *ISO/IEC CD 27552 Information technology -- Security techniques -- Enhancement to ISO/IEC 27001 for privacy management – Requirements. *

You can manage the items in this checklist with the Compliance Manager [15] by referencing the Control ID and Control Title under *Customer Managed Controls* in the GDPR tile.

In addition, items in this checklist under 5. Data Protection & Security references controls listed in Compliance Manager, located in the Service Trust portal at <https://servicetrust.microsoft.com/ComplianceManager>. Reviewing the Microsoft Implementation Details for these controls provides additional explanation of the Microsoft approach to fulfilling the customer considerations in the checklist item.

This control structure is also used to organize the presentation of the internal controls that Microsoft Dynamics365 implements to support GDPR, which you can download here: <https://aka.ms/gdprcontrols>.

To purchase a copy of the complete draft ISO standard, please visit <https://shop.bsigroup.com/ProductDetail?pid=00000000030379002>

For more GDPR related documentation, visit <https://aka.ms/gdprgetstarted>.

2. Conditions for collection and processing

Category	Customer Consideration	Supporting Microsoft documentation	Addresses GDPR Article(s)
identify and document purpose (7.2.1)	The customer should document the purpose for which personal data is processed.	A description of the processing Microsoft performs for you, and the purposes of that processing, that can be included in your accountability documentation - Microsoft Online Services Terms, Data Protection Terms, see Processing of Personal Data; GDPR [1]	(5)(1)(b), (32)(4)

Identify lawful basis (7.2.2)	The customer should understand any requirements related to the lawful basis of processing, such as whether consent must first be given.	A description of processing personal data by Microsoft services for inclusion in your accountability documentation. - Key Information from Dynamics 365 for Customer Data Protection Impact Assessments [2]	(5)(1)(a), (6)(1)(a), (6)(1)(b), (6)(1)(c), (6)(1)(d), (6)(1)(e), (6)(1)(f), (6)(3), (6)(4)(a), (6)(4)(b), (6)(4)(c), (6)(4)(d), (6)(4)(e), (8)(3), (9)(1), (9)(2)(b), (9)(2)(c), (9)(2)(d), (9)(2)(e), (9)(2)(f), (9)(2)(g), (9)(2)(h), (9)(2)(i), (9)(2)(j), (9)(3), (9)(4), (10), (17)(3)(a), (17)(3)(b), (17)(3)(c), (17)(3)(d), (17)(3)(e), (18)(2), (22)(2)(a), (22)(2)(b), (22)(2)(c), (22)(4)
Determine when consent is to be obtained (7.2.3)	The customer should understand legal or regulatory requirements for obtaining consent from individuals prior to processing personal data (when it is required, if the type of processing is excluded from the requirement, etc.), including how consent is collected.	Dynamics365 does not provide direct support for gaining user consent. Dynamics365 processes data in accordance with our contractual obligations and online service terms (OST). Tenant admin is accountable to obtain consent from the data subject prior to collection.	(8)(1), (8)(2)
Obtain and record consent (7.2.4)	When it is determined to be required, the customer should appropriately obtain consent. The customer should also be aware of any requirements for how a request for consent is presented and collected.	Dynamics 365 does not provide direct support for gaining user consent (except for Dynamics 365 Marketing service). Dynamics365 processes data in accordance with our contractual obligations and online service terms (OST). Tenant admin is accountable for obtaining consent from the data subject prior to collection.	(7)(1), (7)(2), (9)(2)(a)
Privacy impact assessment (7.2.5)	The customer should be aware of requirements for completing privacy impact assessments (when they should be performed, categories of data that might necessitate one, timing of completing the assessment).	How Microsoft services determine when to perform a DPIA, and an overview of the DPIA program at Microsoft including the involvement of the DPO, is provided n the Service Trust Portal Data Protection Impact Assessments (DPIAs) page . For support for your DPIAs see: - Key Information from Dynamics 365 for Customer Data Protection Impact Assessments [2]	Article (35)

Contracts with PII Processors (7.2.6)	The customer should ensure that their contracts with processors include requirements for aiding with any relevant legal or regulatory obligations related to processing and protecting personal data.	The Microsoft contracts that require us to aid with your obligations under the GDPR, including support for the data subject's rights. - Microsoft Online Services Terms, Data Protection Terms, see Processing of Personal Data; GDPR [1]	(5)(2), (28)(3)(e), (28)(9)
Records related to processing PII (7.2.7)	The customer should maintain all necessary and required records related to processing personal data (e.g. purpose, security measures, etc.). Where some of these records must be provided by a sub-processor, the customer should ensure that they can obtain such records.	The tools provided by Microsoft services to help you maintain the records necessary demonstrate compliance and support for accountability under the GDPR. - Auditing and Reporting in Dynamics 365 [3]	(5)(2), (24)(1), (30)(1)(a), (30)(1)(b), (30)(1)(c), (30)(1)(d), (30)(1)(g), (30)(1)(f), (30)(3), (30)(4), (30)(5)

3. Rights of data subjects

Category	Customer Consideration	Supporting Microsoft documentation	Addresses GDPR Article(s)
Determining PII principals' rights and enabling exercise (7.3.1)	The customer should understand requirements around the rights of individuals related to the processing of their personal data. These rights may include things such as access, correction, and erasure. Where the customer uses a third-party system, they should determine which (if any) parts of the system provide tools related to enabling individuals to exercise their rights (e.g. to access their data). Where the system provides such capabilities, the customer should utilize them as necessary.	The capabilities Microsoft provides to help you support data subject rights. - Dynamics 365 Data Subject Requests for the GDPR [4] - Dynamics 365-ISO27018 Statement of Applicability [6] see A.1.1	(12)(2)
Determining information for PII principals (data subjects) (7.3.2)	The customer should understand requirements for the types of information about processing of personal data that is to be available to be provided to the	Information about Microsoft services that you can include in the data you provide to data subjects. - Dynamics 365 Data Subject Requests for the GDPR [4] - Key Information from	(11)(2), (13)(1)(a), (13)(1)(b), (13)(1)(c), (13)(1)(d), (13)(1)(e), (13)(1)(f), (13)(2)(c), (13)(2)(d), (13)(2)(e), (13)(3), (13)(4), (14)(1)(a), (14)(1)(b), (14)(1)(c), (14)(1)(d), (14)(1)(e), (14)(1)(f), (14)(2)(b), (14)(2)

<p>individual. This may include things such as:</p> <ul style="list-style-type: none"> • Contact details about the controller or its representative; • information about the processing (purposes, international transfer and related safeguards, retention period, etc.); • information on how the principal may access and/or amend their personal data; requesting erasure or restriction of processing; receiving a copy of their personal data, and portability of their personal data • How and from where the personal data were obtained (if not obtained from the principal directly) • information about the right to lodge a complaint and to whom; • information regarding corrections to personal data; • Notification that the organization is no longer in position to identify the data subject (PII principal), in cases where the processing no longer requires the identification of the data subject; • Transfers and/or disclosures of personal data; • existence of automated decision making based solely on automated processing of personal data; • information regarding the frequency with which information to the data subject is updated and provided (e.g. "just in time" notification, organization defined frequency, etc.) <p>Where the customer uses third-party systems or processors, they should determine which (if any) of this information may need to be provided by them and ensure that they can obtain the required information from the third-party.</p>	<p>Dynamics 365 for Customer Data Protection Impact Assessments [2]</p>	<p>(e), (14)(2)(f), (14)(3)(a), (14)(3)(b), (14)(3)(c), (14)(4), (14)(5)(a), (14)(5)(b), (14)(5)(c), (14)(5)(d), (15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (15)(2), (18)(3), (21)(4)</p>
--	---	--

Providing information to PII principals (7.3.3)	The customer should comply with any requirements around how/when/in what form the required information is to be given to an individual related to the processing of their personal data. In cases where a third-party may provide required information, the customer should ensure that it is within the parameters required by the GDPR.	Information about Microsoft services that you can include in the data you provide to data subjects. - Dynamics 365 Data Subject Requests for the GDPR [4] - Key Information from Dynamics 365 for Customer Data Protection Impact Assessments [2]	(11)(2), (12)(1), (12)(7), (13)(3), (21)(4)
Provide mechanism to modify or withdraw consent (7.3.4)	The customer should understand requirements for informing users about their right to access, correct, and/or erase their personal data and for providing a mechanism for which them to do so. If a third-party system is used and provides this mechanism as part of its functionality, the customer should utilize that functionality as necessary.	Information about capabilities in Microsoft services that you can use when defining the information you provide to data subjects when requesting consent. - Dynamics 365 Data Subject Requests for the GDPR [4]	(7)(3), (13)(2)(c), (14)(2)(d), (18)(1)(a), (18)(1)(b), (18)(1)(c), (18)(1)(d)
Provide mechanism to object to processing (7.3.5)	The customer should understand requirements around rights of data subjects. Where an individual has a right to object to processing, the customer should inform them, and have a way for the individual to register their objection.	Information about Microsoft services relating to object to processing that you can include in the data you provide to data subjects. - Dynamics 365 Data Subject Requests for the GDPR [4] <i>see: Restrict</i>	(13)(2)(b), (14)(2)(c), (21)(1), (21)(2), (21)(3), (21)(5), (21)(6)
Sharing the exercising of PII principals' rights (7.3.6)	The customer should understand requirements for notifying third-parties with whom personal data has been shared of instances of data modification based on the exercise of individual rights (e.g. an individual requesting erasure or modification, etc.)	Information about capabilities in Microsoft services that allow you to discover personal data that you have shared with third parties. - Dynamics 365 Data Subject Requests for the GDPR [4]	(19)

Correction or erasure (7.3.7)	The customer should understand requirements for informing users about their right to access, correct, and/or erase their personal data and for providing a mechanism for which them to do so. If a third-party system is used and provides this mechanism as part of its functionality, the customer should utilize that functionality as necessary.	Information about Microsoft services relating to their ability to access, correct or erase personal data that you can include in the data you provide to data subjects. - Dynamics 365 Data Subject Requests for the GDPR [4] <i>see: Delete</i>	(5)(1)(d), (13)(2)(b), (14)(2)(c), (16), (17)(1)(a), (17)(1)(b), (17)(1)(c), (17)(1)(d), (17)(1)(e), (17)(1)(f), (17)(2)
Providing copy of PII processed (7.3.8)	The customer should understand requirements around providing a copy of the personal data being processed to the individual. These may include requirements around the format of the copy (i.e. that it is machine readable), transferring the copy, etc. Where the customer uses a third-party system that provides the functionality to provide copies, they should utilize this functionality as necessary.	Information about capabilities in Microsoft services to allow you to obtain a copy of their personal data that you can include in the data you provide to data subjects. - Dynamics 365 Data Subject Requests for the GDPR [4] <i>see: Export</i>	(15)(3), (15)(4), (20)(1), (20)(2), (20)(3), (20)(4)
Request management (7.3.9)	The customer should understand requirements for accepting and responding to legitimate requests from individuals related to the processing of their personal data. Where the customer uses a third-party system, they should understand whether that system provides the capabilities for such handling of requests. If so, the customer should utilize such mechanisms to handle requests as necessary.	Information about capabilities in Microsoft services that you can use when defining the information you provide to data subjects as you manage data subject requests. - Dynamics 365 Data Subject Requests for the GDPR [4]	(12)(3), (12)(4), (12)(5), (12)(6), (15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h)

Automated decision making (7.3.10)	The customer should understand requirements around automated personal data processing and where decisions are made by such automation. These may include providing information about the processing to an individual, objecting to such processing, or to obtain human intervention. Where such features are provided by a third-party system, the customer should ensure that the third party provides any required information or support.	Information about any capabilities in Microsoft services for that might support automated decision making that you can use in your accountability documentation, and information for data subjects about those capabilities. - Key Information from Dynamics 365 for Customer Data Protection Impact Assessments [2]	(13)(2)(f), (14)(2)(g), (22)(1), (22)(3)

4. Privacy by Design and Default

Category	Customer Consideration	Supporting Microsoft documentation	Addresses GDPR Article(s)
Limit processing (7.4.2)	The customer is responsible for limiting the processing of personal data so that it is limited to what is adequate for the identified purpose	A description of the data collected by Microsoft services. - Microsoft Online Services Terms, Data Protection Terms, see Processing of Personal Data; GDPR [1] - Key Information from Dynamics 365 for Customer Data Protection Impact Assessments [2]	(25)(2)
Define and document PII minimization and de-identification objectives (7.4.3)	The customer should understand requirements around de-identification of personal data which may include, when it should be used, the extent to which it should de-identify, and instances when it cannot be used.	Microsoft applies de-identification and pseudonymization internally, where appropriate, to provide additional privacy safeguards for personal data.	(5)(1)(c)
Comply with identification levels (7.4.4)	The customer should use and comply with de-identification objectives and methods set by their organization.	Microsoft applies de-identification and pseudonymization internally, where appropriate, to provide additional privacy safeguards for personal data.	(5)(1)(c)

PII de-identification and deletion (7.4.5)	The customer should understand requirements around the retention of personal data past its use for the identified purposes. Where provided tooling by the system, the customer should utilize those tools to erase or delete as necessary. - Dynamics 365 Data Subject Requests for the GDPR [4] <i>see: Delete</i>	(5)(1)(c),(5)(1)(e), (6)(4)(e), (11)(1), (32)(1)(a)	
Temporary files (7.4.6)	The customer should be aware of temporary files that may be created by the system that could lead to non-compliance with policies around processing of personal data (e.g. personal data might be retained in a temporary file longer than required or allowed). Where the system provides such tools for temporary file deletion or checking, the customer should utilize such tools to comply with requirements.	A description of capabilities provided by the service to identify personal data to support your temporary file policies. - Dynamics 365 Data Subject Requests for the GDPR [4] <i>see: Discover</i> - Dynamics 365-ISO27018 Statement of Applicability [6], section 4.1	(5)(1)(c)
Retention (7.4.7)	The customer should determine how long personal data should be retained, taking into consideration the identified purposes.	Information about the retention of personal data by Microsoft services that you can include in documentation provided to data subjects. - Microsoft Online Services Terms, Data Protection Terms, see Data Security, Retention [1]	
Disposal (7.4.8)	The customer should utilize any deletion or disposal mechanisms provided by the system to delete personal data.	Capabilities provided by Microsoft Services to support your data deletion policies. - Dynamics 365 Data Subject Requests for the GDPR [4] <i>see: Delete</i>	
Collection procedures (7.4.9)	The customer should be aware of requirements around the accuracy of personal data (e.g., accuracy upon collection, keeping data up to date, etc.) and utilize any mechanisms provided by the system for such.	How Microsoft services support the accuracy of personal data, and any capabilities they provide to support your data accuracy policy. - Dynamics 365 Data Subject Requests for the GDPR [4] <i>see: Rectify</i>	(5)(1)(d)

Transmission controls (7.4.10)	The customer should understand requirements around safeguarding the transmission of personal data, including who has access to transmission mechanisms, records of transmission, etc.	A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - Key Information from Dynamics 365 for Customer Data Protection Impact Assessments [2]	(15)(2), (30)(1)(e), (5)(1)(f)
Identify basis for PII transfer (7.5.1)	The customer should be aware of requirements for transferring personal data (PII) to a different geographic location and document what measures are in place to meet such requirements.	A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - Key Information from Dynamics 365 for Customer Data Protection Impact Assessments [2]	Articles (44), (45), (46), (47), (48), and (49)
Countries and organizations to which PII might be transferred (7.5.2)	The customer should understand, and be able to provide to the individual, the countries to which personal data is or may be transferred. Where a third-party/processor may perform this transfer, the customer should obtain this information from the processor.	A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - Key Information from Dynamics 365 for Customer Data Protection Impact Assessments [2]	(30)(1)(e)
Records of transfers of PII (personal data) (7.5.3)	The customer should maintain all necessary and required records related to transfers of personal data. Where a third-party/processor performs the transfer, the customer should ensure that they maintain the appropriate records and obtain them as necessary.	A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - Key Information from Dynamics 365 for Customer Data Protection Impact Assessments [2]	(30)(1)(e)

Records of PII disclosure to third parties (7.5.4)	The customer should understand requirements around recording to whom personal data has been disclosed. This may include disclosures to law enforcement, etc. Where a third-party/processor discloses the data, the customer should ensure that they maintain the appropriate records and obtain them as necessary.	Documentation provided about the categories of recipients of disclosures of personal data including available records of disclosure. - Who can access your data and on what terms [7]	(30)(1)(d)
Joint controller (7.5.5)	The customer should determine whether they are a joint controller with any other organization, and appropriately document and allocate responsibilities.	Dynamics 365 is processor of personal data. - Online Services Terms [1] see <i>Processor and Controller Roles and Responsibilities</i> [1]	(26)(1), (26)(2), (26)(3)

5. Data Protection & Security

Category	Customer Consideration	Supporting Microsoft documentation	Addresses GDPR Article(s)
<i>Understanding the organization and its context (5.2.1)</i>	Customers should determine their role in processing personal data (e.g. controller, processor, co-controller) to identify the appropriate requirements (regulatory, etc.) for processing personal data.	How Microsoft considers each service as either a processor or controller when processing personal data. - Microsoft Online Services Terms, Data Protection Terms, see Processing of Personal Data; GDPR, Processor and Controller Roles and Responsibilities [1]	(24)(3), (28)(10), (28)(5), (28)(6), (32)(3), (40)(1), (40)(2)(a), (40)(2)(b), (40)(2)(c), (40)(2)(d), (40)(2)(e), (40)(2)(f), (40)(2)(g), (40)(2)(h), (40)(2)(i), (40)(2)(j), (40)(2)(k), (40)(3), (40)(4), (40)(5), (40)(6), (40)(7), (40)(8), (40)(9), (40)(10), (40)(11), (41)(1), (41)(2)(a), (41)(2)(b), (41)(2)(c), (41)(2)(d), (41)(3), (41)(4), (41)(5), (41)(6), (42)(1), (42)(2), (42)(3), (42)(4), (42)(5), (42)(6), (42)(7), (42)(8)

<i>Understanding the needs and expectations of interested parties (5.2.2)</i>	Customers should identify parties that may have a role or interest in their processing of personal data (e.g. regulators, auditors, data subjects, contracted personal data processors), and be aware of requirements to engage such parties where required.	How Microsoft incorporates the views of all stakeholders in consideration of the risks involved in the processing of personal data. - Key Information from Dynamics 365 for Customer Data Protection Impact Assessments [2] - Understanding the needs and expectations of interested parties 5.2.2 in Compliance Manager [15]	(35)(9), (36)(1), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)
<i>Determining the scope of the information security management system (5.2.3, 5.2.4)</i>	As part of any overall security or privacy program that a customer may have, they should include the processing of personal data and requirements relating to it.	How Microsoft services include the processing of personal data in information security management and privacy programs. - Dynamics 365-ISO27001 Statement of Applicability [5] - Dynamics 365-ISO27018 Statement of Applicability [6] - SOC 2 Type 2 Audit Report [8] - 5.2.3 Determining the scope of the information security management system in Compliance Manager [15] - 5.2.4 Information security management system in Compliance Manager [15]	(32)(2)
<i>Planning (5.3)</i>	Customers should consider the handling of personal data as part of any risk assessment they complete and apply controls as they deem necessary to mitigate risk related to personal data they control.	How Microsoft services consider the risks specific to the processing of personal data as part of their overall security and privacy program. - Dynamics 365-ISO27001 Statement of Applicability [5] - Dynamics 365-ISO27018 Statement of Applicability [6] - 5.3 Planning in Compliance Manager [15]	(32)(1)(b), (32)(2)
<i>Information Security Policies (6.2)</i>	The customer should augment any existing information security policies to include protection of personal data, including policies necessary for compliance with any applicable legislation.	Microsoft policies for information security and any specific measures for the protection of personal information. - Dynamics 365-ISO27001 Statement of Applicability [5] - Dynamics 365-ISO27018 Statement of Applicability [6] - SOC 2 Type 2 Audit Report [8] - 6.2 Information security policies in Compliance Manager [15]	24(2)

<p>Organization of Information Security Customer consideration (6.3)</p>	<p>The customer should, within their organization, define responsibilities for security and protection of personal data. This may include establishing specific roles to oversee privacy related matters, including a DPO. Appropriate training and management support should be provided to support these roles.</p>	<p>An overview of the role of Microsoft's Data Protection Officer, the nature of his duties, reporting structure and contact information.</p> <ul style="list-style-type: none"> - Microsoft DPO Information [16] - Dynamics 365-ISO27001 Statement of Applicability [5] - Dynamics 365-ISO27018 Statement of Applicability [6] - 6.3 Organization of information security in Compliance Manager [15] 	<p>(37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)</p>
<p>Human Resource Security6.4)</p>	<p>The customer should determine and assign responsibility for providing relevant training related to protecting personal data.</p>	<p>An overview of the role of Microsoft's Data Protection Officer, the nature of his duties, reporting structure and contact information.</p> <ul style="list-style-type: none"> - Microsoft DPO Information [16] - Dynamics 365-ISO27001 Statement of Applicability [5] <i>section A.7</i> - Dynamics 365-ISO27018 Statement of Applicability [6] <i>section 7.2</i> - 6.4 Information security awareness and training in Compliance Manager [15] 	<p>(39)(1)(b)</p>
<p>Classification of Information (6.5.1)</p>	<p>The customer should explicitly consider personal data as part of a data classification scheme.</p>	<p>Capabilities in Dynamics 365 to support personal data classification.</p> <ul style="list-style-type: none"> - 6.5.1 Classification of Information in Compliance Manager [15] Manager 	<p>(39)(1)(b)</p>
<p>Management of removable media (6.5.2)</p>	<p>The customer should determine internal policies for the use of removable media as it relates to the protection of personal data (e.g., encrypting devices).</p>	<p>How Microsoft services protect the security of personal information on any removable media.</p> <ul style="list-style-type: none"> - 6.5.2 Management of removable media in Compliance Manager [15] 	<p>(32)(1)(a), (5)(1)(f)</p>
<p>Physical media transfer (6.5.3)</p>	<p>The customer should determine internal policies for protecting personal data when transferring physical media (e.g. encryption).</p>	<p>How Microsoft services protects personal data during any transfer of physical media.</p> <ul style="list-style-type: none"> - 6.5.3 Physical media transfer in Compliance Manager [15] 	<p>(32)(1)(a), (5)(1)(f)</p>

User access management (6.6.1)	The customer should be aware of which responsibilities they have for access control within the service they are using, and manage those responsibilities appropriately, using the tools available.	The tools provided by Microsoft services to help you enforce access control. - Dynamics 365 - Discover built in security features [9] - 6.6.1 User Access Management in Compliance Manager [15]	(5)(1)(f)
User registration and de-registration (6.6.2)	The customer should manage user registration and de-registration within the service they utilize, using the tools available to them.	The tools provided by Microsoft services to help you enforce access control. - 6.6.2 User registration and de-registration in Compliance Manager - Dynamics 365 - Discover built in security features [9]	(5)(1)(f)
User access provisioning (6.6.3)	The customer should manage user profiles, especially for authorized access to personal data, within the service they utilize, using the tools available to them.	How Microsoft services support formal access control to personal data, including user IDs, roles, and the registration and de-registration of users. - Dynamics 365 - Discover built in security features [9] - 6.6.3 User access provisioning n Compliance Manager [15]	(5)(1)(f)
Management of privileged access (6.6.4)	The customer should manage user ID's to facilitate tracking of access (especially to personal data), within the service they utilize, using the tools available to them.	How Microsoft services support formal access control to personal data, including user IDs, roles, and the registration and de-registration of users. - Dynamics 365 - Discover built in security features [9] - 6.6.4 Management of privileged access [15]	(5)(1)(f)
Secure log on procedures (6.6.5)	The customer should utilize provided mechanisms in the service to ensure secure log on capabilities for their users where necessary.	How Microsoft services support internal access control policies related to personal data. - Who can access your data and on what terms [10] - 6.6.5 Information access restrictions in Compliance Manager [15]	(5)(1)(f)
Cryptography (6.7)	The customer should determine which data may need to be encrypted, and whether the service they are utilizing offers this capability. The customer should utilize encryption as needed, using the tools available to them.	How Microsoft services support encryption and pseudonymization to reduce the risk of processing personal data. - Dynamics 365 - Discover built in security features [9] - 6.7 Cryptography in Compliance Manager [15]	(32)(1)(a)

Secure disposal or re-use of equipment (6.8.1)	Where the customer uses cloud computing services (PaaS, SaaS, IaaS) they should understand how the cloud provider ensures that personal data is erased from storage space prior to that space being assigned to another customer.	How Microsoft services ensure that personal data is erased from storage equipment before that equipment is transferred or reused. - Dynamics 365-ISO27001 Statement of Applicability [5], section 10.1 - Dynamics 365-ISO27018 Statement of Applicability [6], section 8.3 - 6.8.1 Secure disposal or re-use of equipment in Compliance Manager [15]	(5)(1)(f)
Clear desk and clear screen policy (6.8.2)	The customer should consider risks around hardcopy material that displays personal data, and potentially restrict the creation of such material. Where the system in use provides the capability to restrict this (e.g., settings to prevent printing or copying/pasting of sensitive data), the customer should consider the need to utilize those capabilities.	What Microsoft implements to manage hardcopy. - Dynamics 365-ISO27001 Statement of Applicability [5], section 11.2 - 6.8.2 Clear desk and clear screen policy in Compliance Manager [15]	(5)(1)(f)
Separation of development, testing and operational environments (6.9.1)	The customer should consider the implications of using personal data in development and testing environments within their organization.	How Microsoft ensures that personal data is protected in development and test environments. - Dynamics 365-ISO27001 Statement of Applicability [5], section 12.1 - Dynamics 365-ISO27018 Statement of Applicability [6], section 12.1 - 6.9.1 Separation of development, testing and operational environments in Compliance Manager [15]	

Information backup (6.9.2)	The customer should ensure that they use system provided capabilities to create redundancies in their data and test as necessary.	How Microsoft ensures the availability of data that may include personal data, how accuracy of restored data is ensured, and the tools and procedures Microsoft services provide to allow you to backup and restore data. - Dynamics 365-ISO27001 Statement of Applicability [5], section 12.3 - Dynamics 365-ISO27018 Statement of Applicability [6], section 12.3 - 6.9.2 Information Backup in Compliance Manager [15]	(32)(1)(c), (5)(1)(f)
Event logging (6.9.3)	The customer should understand the capabilities for logging provided by the system and utilize such capabilities to ensure that they can log actions related to personal data that they deem necessary.	The data Microsoft service records for you, including user activities, exceptions, faults and information security events, and how you can access those logs for use as part of your record keeping. - Auditing and Reporting in Dynamics 365 [3] - 6.9.3 Event logging in Compliance Manager [15]	(5)(1)(f)
Protection of log information (6.9.4)	The customer should consider requirements for protecting log information that may contain personal data or that may contain records related to personal data processing. Where the system in use provides capabilities to protect logs, the customer should utilize these capabilities where necessary.	How Microsoft protects logs that may contain personal data. - Auditing and Reporting in Dynamics 365 [3] - 6.9.4 Protection of log information in Compliance Manager [15]	(5)(1)(f)
Information transfer policies and procedures (6.10.1)	The customer should have procedures for cases where personal data may be transferred on physical media (such as a hard drive being moved between servers or facilities). These may include logs, authorizations, and tracking. Where a third-party or other processor may be transferring physical media, the customer should ensure that that organization has procedures in place to ensure security of the personal data.	How Microsoft services transfer physical media that may contain personal data, including the circumstances when transfer might occur, and the protective measures taken to protect the data. - Dynamics 365-ISO27001 Statement of Applicability [5], section 8.3 - Dynamics 365-ISO27018 Statement of Applicability [6], section 10.4 - 6.10.1 Information transfer policies and procedures in Compliance Manager [15]	(5)(1)(f)

<p>Confidentiality or non-disclosure agreements (6.10.2)</p>	<p>The customer should determine the need for confidentiality agreements or the equivalent for individuals with access to or responsibilities related to personal data.</p>	<p>How Microsoft services ensure that individuals with authorized access to personal data have committed themselves to confidentiality.</p> <ul style="list-style-type: none"> - Dynamics 365 SOC 2 Type 2 Audit Report & Bridge letter [8] - 6.10.2 Confidentiality or non-disclosure agreements in Compliance Manager [15] 	<p>(5)(1)(f), (28)(3)(b), (38)(5)</p>
<p>Securing application services on public networks (6.11.1)</p>	<p>The customer should understand requirements for encryption of personal data, especially when sent over public networks. Where the system provides mechanisms to encrypt data, the customer should utilize those mechanisms where necessary.</p>	<p>Description of the measures Microsoft services take to protect data in transit, including encryption of the data, and how Microsoft services protect data that may contain personal data as it passes through public data networks, including any encryption measures.</p> <ul style="list-style-type: none"> - Dynamics 365 - Discover built in security features [9] - 6.11.1 Securing application services on public networks in Compliance Manager [15] 	<p>(5)(1)(f), (32)(1)(a)</p>
<p>Secure system engineering principles (6.11.2)</p>	<p>The customer should understand how systems are designed and engineered to consider protection of personal data. Where a customer uses a system engineered by a third-party, it is their responsibility to ensure that such protections have been considered.</p>	<p>How Microsoft services include personal data protection principles as a mandatory part of our secure design/engineering principles.</p> <ul style="list-style-type: none"> - Dynamics 365 SOC 2 Type 2 Audit Report & Bridge letter [8] see <i>Security Development Lifecycle</i> pp23, CC7.1 pp45 and What is the Security Development Lifecycle ? - Secure system engineering principles in Compliance Manager [15] 	
<p>Supplier Relationships (6.12)</p>	<p>The customer should ensure that any information security and personal data protection requirements and that are the responsibility of a third-party are addressed in contractual information or other agreements. The agreements should also address the instructions for processing.</p>	<p>How Microsoft services address security and data protection in our agreements with our suppliers and how we ensure those agreements are effectively implemented.</p> <ul style="list-style-type: none"> - Who can access your data and on what terms [10] - 6.12 Supplier Relationships in Compliance Manager [15] 	<p>(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)</p>

Management of information security incidents and improvements (6.13.1)	The customer should have processes for determining when a personal data breach has occurred.	How Microsoft services determine if a security incident is a breach of personal data, and how we communicate the breach to you. - Dynamics 365 Breach Notification Under the GDPR [12] - 6.13.1 Management of information security incidents and improvements in Compliance Manager [15]	(33)(2)
Responsibilities and procedures (during information security incidents) (6.13.2)	The customer should understand and document their responsibilities during a data breach or security incident involving personal data. Responsibilities may include notifying required parties, communications with processors or other third-parties, and responsibilities within the customer's organization.	How to notify Microsoft services if you detect a security incident or breach of personal data. - Dynamics 365 Breach Notification Under the GDPR [12] - 6.13.2 Responsibilities and procedures in Compliance Manager [15]	(5)(1)(f), (33)(1), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2), (34)(3)(a), (34)(3)(b), (34)(3)(c), (34)(4)
Response to information security incidents (6.13.3)	The customer should have processes for determining when a personal data breach has occurred.	Description of the information Microsoft services provide to help you decide if a breach of personal data has occurred. - Dynamics 365 Breach Notification Under the GDPR [12] - 6.13.3 Response to information security incidents in Compliance Manager [15]	(33)(1), (33)(2), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2)
Protection of records (6.15.1)	The customer should understand the requirements for records related to personal data processing that need to be maintained.	How Microsoft services store records relating to the processing of personal data. - Auditing and Reporting in Dynamics 365 [3] - Dynamics 365-ISO27001 Statement of Applicability [5]; section 18.1 - Dynamics 365-ISO27018 Statement of Applicability [6]; section 5.2	(5)(2), (24)(2)

Independent review of information security (6.15.2)	The customer should be aware of requirements for assessments of the security of personal data processing. This may include internal or external audits, or other measures for assessing the security of processing. Where the customer is dependent on another organization of third-party for all or part of the processing, they should collect information about such assessments performed by them.	How Microsoft services test and assesses the effectiveness of technical and organizational measures to ensure the security of processing, including any audits by third parties. - Microsoft Online Services Terms, Data Protection Terms, see Data Security, Auditing Compliance [1] - 6.15.2 Independent review of information security in Compliance Manager [15]	(32)(1)(d), (32)(2)
Technical compliance review (6.15.3)	The customer should understand requirements for testing and evaluating the security of processing personal data. This may include technical tests such as penetration testing. Where the customer uses a third-party system or processor, they should understand what responsibilities they have for securing and testing the security (e.g. managing configurations to secure data and then testing those configuration settings). Where the third-party is responsible for all or part of the security of processing, the customer should understand what testing or evaluation the third-party performs to ensure the security of the processing.	How Microsoft services are tested security based on identified risks, including tests by third parties, and the types of technical tests and any available reports from the tests. - Microsoft Online Services Terms, Data Protection Terms, see Data Security, Auditing Compliance [1] - For a listing of external certifications see <i>Microsoft Trust Center Compliance offerings</i> [13] - Dynamics 365 - Discover built in security features [9] - Dynamics 365 Penetration Testing and Security Assessment Report [14] - 6.15.3 Technical compliance review in Compliance Manager [15]	(32)(1)(d), (32)(2)

6. Bibliography of Resources and Links

ID	Documents	Link
1	Online Services Terms	http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeID=46

2	Key Information from Dynamics 365 for Customer Data Protection Impact Assessments	https://servicetrust.microsoft.com/ViewPage/GDPRDPIA?command=Download&downloadType=Document&downloadId=ef2902bb-3137-4f4a-8ca6-af35afaa6bec&docTab=2ba9a350-555c-11e8-b74a-77b1f31da06e_DPIA
3	Auditing and Reporting in Dynamics 365	https://docs.microsoft.com/dynamics365/customer-engagement/admin/use-comprehensive-auditing
4	Dynamics 365 Data Subject Requests for the GDPR	https://servicetrust.microsoft.com/ViewPage/GDPRDSR
5	Dynamics 365-ISO27001 Statement of Applicability	https://servicetrust.microsoft.com/ViewPage/MSCComplianceGuide?command=Download&downloadType=Document&downloadId=d383c8df-1387-4a08-8604-b3e8aa647206&docTab=4ce99610-c9c0-11e7-8c2c-f908a777fa4d_ISO_Reports
6	Dynamics 365-ISO27018 Statement of Applicability	https://servicetrust.microsoft.com/ViewPage/MSCComplianceGuide?command=Download&downloadType=Document&downloadId=7eecdb74-46c9-4774-af3a-c66e5704cb14&docTab=4ce99610-c9c0-11e7-8c2c-f908a777fa4d_ISO_Reports
7	Who can access your data and on what terms?	https://www.microsoft.com/trustcenter/Privacy/Who-can-access-your-data-and-on-what-terms
8	Dynamics 365 SOC 2 Type 2 Report & Bridge Letter	https://servicetrust.microsoft.com/ViewPage/MSCComplianceGuide?command=Download&downloadType=Document&downloadId=e06a247d-af6b-4933-8074-1002757984bd&docTab=4ce99610-c9c0-11e7-8c2c-f908a777fa4d_SOC_%2F_SSAE_16_Reports
9	Dynamics 365 - Discover built in security features	https://www.microsoft.com/trustcenter/security/dynamics365-security
10	Who can access data and at what terms	https://www.microsoft.com/trustcenter/Privacy/Who-can-access-your-data-and-on-what-terms
11	Contracts for sub-processors: Contracting with Microsoft	https://www.microsoft.com/en-us/procurement/supplier-contracting.aspx#SSPA

12	Dynamics 365 Breach Notification Under the GDPR	https://servicetrust.microsoft.com/ViewPage/GDPRBreach
13	Microsoft Trust Center Compliance offerings	https://www.microsoft.com/trustcenter/compliance/complianceofferings
14	Dynamics 365 Penetration Testing and Security Assessment Report	https://servicetrust.microsoft.com/ViewPage/TrustDocuments?command=Download&downloadType=Document&downloadId=25aa47b1-c510-43f2-84de-6b78ed3b1258&docTab=6d000410-c9e9-11e7-9a91-892aae8839ad_Pen_Test_and_Security_Assessments
15	Compliance Manager	https://servicetrust.microsoft.com/ComplianceManager
16	Microsoft DPO Information	https://docs.microsoft.com/microsoft-365/compliance/gdpr-data-protection-officer

Learn more

[Microsoft Trust Center](#)

[Secure Trust Portal](#)

Microsoft Support and Professional Services accountability readiness checklist for the GDPR

2/22/2019 • 27 minutes to read • [Edit Online](#)

1. Introduction

This accountability readiness checklist provides a convenient way to access information you may need to support GDPR when using Microsoft Professional Services and Support Services. The checklist is organized using the titles and reference number (in parenthesis for each checklist topic) of a set of privacy and security controls for personal data processors drawn from *ISO/IEC CD 27552 Information technology — Security techniques — Enhancement to ISO/IEC 27001 for privacy management – Requirements*.

This control structure is also used to organize the presentation of the internal controls that Microsoft Professional Services implements to support GDPR, which you can download here

<https://servicetrust.microsoft.com/ViewPage/TrustDocuments>.

To purchase a copy of the complete draft ISO standard, please visit <https://shop.bsigroup.com/ProductDetail?pid=000000000030372571>.

2. Conditions for collection and processing

Category	Customer Consideration	Supporting Microsoft documentation	Addresses GDPR Article(s)
Identify and document purpose (7.2.1)	The customer should document the purpose for which personal data is processed.	A description of the processing Microsoft performs for you, and the purposes of that processing, that can be included in your accountability documentation. - Microsoft Professional Services Data Protection Addendum [1]	(5)(1)(b), (32)(4)
Identify lawful basis (7.2.2)	The customer should understand any requirements related to the lawful basis of processing, such as whether consent must first be given.	A description of processing personal data by Microsoft services for inclusion in your accountability documentation. - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [10]	(5)(1)(a), (6)(1)(a), (6)(1)(b), (6)(1)(c), (6)(1)(d), (6)(1)(e), (6)(1)(f), (6)(3), (6)(4)(a), (6)(4)(b), (6)(4)(c), (6)(4)(d), (6)(4)(e), (8)(3), (9)(1), (9)(2)(b), (9)(2)(c), (9)(2)(d), (9)(2)(e), (9)(2)(f), (9)(2)(g), (9)(2)(h), (9)(2)(i), (9)(2)(j), (9)(3), (9)(4), (10), (17)(3)(a), (17)(3)(b), (17)(3)(c), (17)(3)(d), (17)(3)(e), (18)(2), (22)(2)(a), (22)(2)(b), (22)(2)(c), (22)(4)

Determine when consent is to be obtained (7.2.3)	The customer should understand legal or regulatory requirements for obtaining consent from individuals prior to processing personal data (when it is required, if the type of processing is excluded from the requirement, etc.), including how consent is collected.	Microsoft Professional Services does not provide direct support for gaining user consent.	(6)(1)(a), (8)(1), (8)(2)
Obtain and record consent (7.2.4)	When it is determined to be required, the customer should appropriately obtain consent. The customer should also be aware of any requirements for how a request for consent is presented and collected	Microsoft Professional Services does not provide direct support for gaining user consent.	(7)(1), (7)(2), (9)(2)(a)
Privacy impact assessment (7.2.5)	The customer should be aware of requirements for completing privacy impact assessments (when they should be performed, categories of data that might necessitate one, timing of completing the assessment).	Microsoft Professional Services provides guidance as to when and how to determine when to perform a DPIA, and an overview of the DPIA program at Microsoft including the involvement of the DPO, which is provided in the Service Trust Portal Data Protection ,Impact Assessments (DPIAs) page .< For support for your DPIAs see: - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [10]	Article (35)
Contracts with PII Processors (7.2.6)	The customer should ensure that their contracts with processors include requirements for aiding with any relevant legal or regulatory obligations related to processing and protecting personal data.	The Microsoft contracts that require us to aid with your obligations under the GDPR, including support for the data subject's rights. - Microsoft Professional Services Data Protection Addendum [1]	(5)(2), (28)(3)(e), (28)(9)

Records related to processing PII (7.2.7)	The customer should maintain all necessary and required records related to processing personal data (e.g. purpose, security measures, etc.). Where some of these records must be provided by a sub-processor, the customer should ensure that they can obtain such records.	Microsoft Professional Services maintains records necessary demonstrate compliance and support for accountability under the GDPR. See the Microsoft Professional Services Security Documentation [2]	(5)(2), (24)(1), (30)(1)(a), (30)(1)(b), (30)(1)(c), (30)(1)(d), (30)(1)(g), (30)(1)(f), (30)(3), (30)(4), (30)(5)
--	---	--	--

3. Rights of data subjects

Category	Customer Consideration	Supporting Microsoft documentation	Addresses GDPR Article(s)
Determining PII principals' rights and enabling exercise (7.3.1)	The customer should understand requirements around the rights of individuals related to the processing of their personal data. These rights may include things such as access, correction, and erasure. Where the customer uses a third-party system, they should determine which (if any) parts of the system provide tools related to enabling individuals to exercise their rights (e.g. to access their data). Where the system provides such capabilities, the customer should utilize them as necessary.	The capabilities Microsoft provides to help you support data subject rights. - Microsoft Professional Services Data Subject Requests for the GDPR [8] - Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [12]	(12)(2)
Determining information for PII principals (data subjects) (7.3.2)	The customer should understand requirements for the types of information about processing of personal data that is to be available to be provided to the individual. This may include things such as: <ul style="list-style-type: none">• Contact details about the controller or its representative;• information about the processing (purposes, international transfer and related safeguards, retention period, etc.);• information on how the principal may access and/or amend their personal data;	Information about Microsoft services that you can include in the data you provide to data subjects. - Microsoft Professional Services Data Subject Requests for the GDPR [8] - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [10]	(11)(2), (13)(1)(a), (13)(1)(b), (13)(1)(c), (13)(1)(d), (13)(1)(e), (13)(1)(f), (13)(2)(c), (13)(2)(d), (13)(2)(e), (13)(3), (13)(4), (14)(1)(a), (14)(1)(b), (14)(1)(c), (14)(1)(d), (14)(1)(e), (14)(1)(f), (14)(2)(b), (14)(2)(e), (14)(2)(f), (14)(3)(a), (14)(3)(b), (14)(3)(c), (14)(4), (14)(5)(a), (14)(5)(b), (14)(5)(c), (14)(5)(d), (15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (15)(2), (18)(3), (21)(4)

	<p>權利（如：個人資料， 請求刪除或 限制處理； 接收其個人資料的複印件， 以及個人資料的可移植性）</p> <ul style="list-style-type: none"> • 如何和從何處獲得個人資料（如非直接從主體獲得） • 關於權利的資訊，可以向誰投訴，以及向誰投訴 • 關於更正個人資料的資訊 • 註明該組織已不再能够識別資料主體（PII主體），在這種情況下，如果處理個人資料已不再需要識別資料主體，則不會再識別 • 轉移和/或披露個人資料 • 存在基於自動化決策的單一自動化處理過程 • 關於資訊頻率的資訊，這些資訊會定期更新資料主體，並提供（例如，“即時”通知，組織定義的頻率等） <p>Where the customer uses third-party systems or processors, they should determine which (if any) of this information may need to be provided by them and ensure that they can obtain the required information from the third-party.</p>		
Providing information to PII principals (7.3.3)	<p>The customer should comply with any requirements around how/when/in what form the required information is to be given to an individual related to the processing of their personal data. In cases where a third-party may provide required information, the customer should ensure that it is within the parameters required by the GDPR.</p>	<p>Templated information about Microsoft Professional Services that you can include in the data you provide to data subjects.</p> <ul style="list-style-type: none"> - Microsoft Professional Services Data Subject Requests for the GDPR [8] - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [10] 	(11)(2), (12)(1), (12)(7), (13)(3), (21)(4)

Provide mechanism to modify or withdraw consent (7.3.4)	The customer should understand requirements for informing users about their right to access, correct, and/or erase their personal data and for providing a mechanism for which them to do so. If a third-party system is used and provides this mechanism as part of its functionality, the customer should utilize that functionality as necessary.	Information about capabilities in Microsoft services that you can use when defining the information you provide to data subjects when requesting consent. - Microsoft Professional Services Data Subject Requests for the GDPR [8]	(7)(3), (13)(2)(c), (14)(2)(d), (18)(1)(a), (18)(1)(b), (18)(1)(c), (18)(1)(d)
Provide mechanism to object to processing (7.3.5)	The customer should understand requirements around rights of data subjects. Where an individual has a right to object to processing, the customer should inform them, and have a way for the individual to register their objection.	Information about Microsoft services relating to object to processing that you can include in the data you provide to data subjects. - Microsoft Professional Services Data Subject Requests for the GDPR [8]	(13)(2)(b), (14)(2)(c), (21)(1), (21)(2), (21)(3), (21)(5), (21)(6)
Sharing the exercising of PII principals' rights (7.3.6)	The customer should understand requirements for notifying third-parties with whom personal data has been shared of instances of data modification based on the exercise of individual rights (e.g. an individual requesting erasure or modification, etc.)	Information about capabilities in Microsoft services that allow you to discover personal data that you have shared with third parties. - Microsoft Professional Services Data Subject Requests for the GDPR [8]	(19)
Correction or erasure (7.3.7)	The customer should understand requirements for informing users about their right to access, correct, and/or erase their personal data and for providing a mechanism for which them to do so. If a third-party system is used and provides this mechanism as part of its functionality, the customer should utilize that functionality as necessary.	Templated information about Microsoft services relating to their ability to access, correct or erase personal data that you can include in the data you provide to data subjects. - Microsoft Professional Services Data Subject Requests for the GDPR [8]	

Providing copy of PII processed (7.3.8)	The customer should understand requirements around providing a copy of the personal data being processed to the individual. These may include requirements around the format of the copy (i.e. that it is machine readable), transferring the copy, etc. Where the customer uses a third-party system that provides the functionality to provide copies, they should utilize this functionality as necessary.	Information about capabilities in Microsoft services to allow you to obtain a copy of their personal data that you can include in the data you provide to data subjects.- Microsoft Professional Services Data Subject Requests for the GDPR [8]	(15)(3), (15)(4), (20)(1), (20)(2), (20)(3), (20)(4)
Request management (7.3.9)	The customer should understand requirements for accepting and responding to legitimate requests from individuals related to the processing of their personal data. Where the customer uses a third-party system, they should understand whether that system provides the capabilities for such handling of requests. If so, the customer should utilize such mechanisms to handle requests, as necessary.	Information about capabilities in Microsoft services that you can use when defining the information you provide to data subjects as you manage data subject requests.- Microsoft Professional Services Data Subject Requests for the GDPR [8]	(12)(3), (12)(4), (12)(5), (12)(6), (15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h)
Automated decision making (7.3.10)	The customer should understand requirements around automated personal data processing and where decisions are made by such automation. These may include providing information about the processing to an individual, objecting to such processing, or to obtain human intervention. Where such features are provided by a third-party system, the customer should ensure that the third party provides any required information or support.	Information about any capabilities in Microsoft services for that might support automated decision making that you can use in your accountability documentation, and templated information for data subjects about those capabilities. - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [10]	(13)(2)(f), (14)(2)(g), (22)(1), (22)(3)

4. Privacy by design and default

Category	Customer Consideration	Supporting Microsoft documentation	Addresses GDPR Article(s)

Limit collection (7.4.1)	The customer should understand requirements around limits on collection of personal data (e.g. that the collection should be limited to what is needed for the specified purpose).	A description of the data collected by Microsoft services. - Microsoft Professional Services Data Protection Addendum [1] - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [10]	(5)(1)(b), (5)(1)(c)
Limit processing (7.4.2)	The customer is responsible for limiting the processing of personal data so that it is limited to what is adequate for the identified purpose.	A description of the data collected by Microsoft services. - Microsoft Professional Services Data Protection Addendum [1] - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [10]	(25)(2)
Define and document PII minimization and de-identification objectives (7.4.3)	The customer should understand requirements around de-identification of personal data which may include, when it should be used, the extent to which it should de-identify, and instances when it cannot be used.	Customer is responsible for de-identification before transferring data to Microsoft. Microsoft applies de-identification and pseudonymization internally, where appropriate, to provide additional privacy safeguards for personal data.	(5)(1)(c)
Comply with identification levels (7.4.4)	The customer should use and comply with de-identification objectives and methods set by their organization.	Customer is responsible for de-identification before transferring data to Microsoft. Microsoft applies de-identification and pseudonymization internally, where appropriate, to provide additional privacy safeguards for personal data.	(5)(1)(c)
PII de-identification and deletion (7.4.5)	The customer should understand requirements around the retention of personal data past its use for the identified purposes. Where provided tooling by the system, the customer should utilize those tools to erase or delete as necessary.	Capabilities provided by Microsoft Services to support your data retention policies. - Microsoft Professional Services Data Subject Requests for the GDPR [8]	(5)(1)(c),(5)(1)(e), (6)(4)(e), (11)(1), (32)(1)(a)

Temporary files (7.4.6)	The customer should be aware of temporary files that may be sent to Microsoft that could lead to non-compliance with policies around processing of personal data (e.g. personal data might be retained in a temporary file longer than required or allowed).	A description of capabilities provided by the service to identify personal data to support your temporary file policies. - Microsoft Professional Services Data Subject Requests for the GDPR [8]	(5)(1)(c)
Retention (7.4.7)	The customer should determine how long personal data should be retained, taking into consideration the identified purposes.	Information about the retention of personal data by Microsoft services that you can include in documentation provided to data subjects. - Microsoft Professional Services Data Protection Addendum [1]	(13)(2)(a), (14)(2)(a)
Disposal (7.4.8)	The customer should utilize any deletion or disposal mechanisms provided by the system to delete personal data.	Capabilities provided by Microsoft Services to support your data deletion policies. - Microsoft Professional Services Data Subject Requests for the GDPR [8]	(5)(1)(f)
Collection procedures (7.4.9)	The customer should be aware of requirements around the accuracy of personal data (e.g., accuracy upon collection, keeping data up to date, etc.) and utilize any mechanisms provided by the system for such.	How Microsoft services support the accuracy of personal data, and any capabilities they provide to support your data accuracy policy. - Microsoft Professional Services Data Subject Requests for the GDPR [8]	(5)(1)(d)
Transmission controls (7.4.10)	The customer should understand requirements around safeguarding the transmission of personal data, including who has access to transmission mechanisms, records of transmission, etc.	A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [10]	(15)(2), (30)(1)(e), (5)(1)(f)

Identify basis for PII transfer (7.5.1)	The customer should be aware of requirements for transferring personal data (PII) to a different geographic location and document what measures are in place to meet such requirements.	A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [10]	Articles (44), (45), (46), (47), (48), and (49)
Countries and organizations to which PII might be transferred (7.5.2)	The customer should understand, and be able to provide to the individual, the countries to which personal data is or may be transferred. Where a third-party/processor may perform this transfer, the customer should obtain this information from the processor.	A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [10]	(30)(1)(e)
Records of transfers of PII (personal data) (7.5.3)	The customer should maintain all necessary and required records related to transfers of personal data. Where a third-party/processor performs the transfer, the customer should ensure that they maintain the appropriate records and obtain them as necessary.	A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [10]	(30)(1)(e)
Records of PII disclosure to third parties (7.5.4)	The customer should understand requirements around recording to whom personal data has been disclosed. This may include disclosures to law enforcement, etc. Where a third-party/processor discloses the data, the customer should ensure that they maintain the appropriate records and obtain them as necessary.	Documentation provided about the categories of recipients of disclosures of personal data including available records of disclosure. - Who can access your data and on what terms [7]	(30)(1)(d)
Joint controller (7.5.5)	The customer should determine whether they are a joint controller with any other organization, and appropriately document and allocate responsibilities.	Microsoft is not a joint controller of personal information provided as part of Support and Consulting Data.	(26)(1), (26)(2), (26)(3)

5. Data Protection & Security

Category	Customer Consideration	Supporting Microsoft documentation	Addresses GDPR Article(s)
<i>Understanding the organization and its context (5.2.1)</i>	Customers should determine their role in processing personal data (e.g. controller, processor, co-controller) to identify the appropriate requirements (regulatory, etc.) for processing personal data.	How Microsoft considers each service as either a processor or controller when processing personal data. - Microsoft Professional Services Data Protection Addendum [1]	(24)(3), (28)(10), (28)(5), (28)(6), (32)(3), (40)(1), (40)(2)(a), (40)(2)(b), (40)(2)(c), (40)(2)(d), (40)(2)(e), (40)(2)(f), (40)(2)(g), (40)(2)(h), (40)(2)(i), (40)(2)(j), (40)(2)(k), (40)(3), (40)(4), (40)(5), (40)(6), (40)(7), (40)(8), (40)(9), (40)(10), (40)(11), (41)(1), (41)(2)(a), (41)(2)(b), (41)(2)(c), (41)(2)(d), (41)(3), (41)(4), (41)(5), (41)(6), (42)(1), (42)(2), (42)(3), (42)(4), (42)(5), (42)(6), (42)(7), (42)(8)
<i>Understanding the needs and expectations of interested parties (5.2.2)</i>	Customers should identify parties that may have a role or interest in their processing of personal data (e.g. regulators, auditors, data subjects, contracted personal data processors), and be aware of requirements to engage such parties where required.	How Microsoft incorporates the views of all stakeholders in consideration of the risks involved in the processing of personal data. - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [10]	(35)(9), (36)(1), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)
<i>Determining the scope of the information security management system (5.2.3, 5.2.4)</i>	As part of any overall security or privacy program that a customer may have, they should include the processing of personal data and requirements relating to it	How Microsoft services include the processing of personal data in information security management and privacy programs. - Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [12] - ISO 27001 Audit Report [11]	(32)(2)
<i>Planning (5.3)</i>	Customers should consider the handling of personal data as part of any risk assessment they complete and apply controls as they deem necessary to mitigate risk related to personal data they control.	How Microsoft services consider the risks specific to the processing of personal data as part of their overall security and privacy program. - Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [12]	(32)(1)(b), (32)(2)

Information Security Policies (6.2)	The customer should augment any existing information security policies to include protection of personal data, including policies necessary for compliance with any applicable legislation.	Microsoft policies for information security and any specific measures for the protection of personal information. - Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [12] - ISO 27001 Audit Report [11]	24(2)
Organization of Information Security Customer consideration (6.3)	The customer should, within their organization, define responsibilities for security and protection of personal data. This may include establishing specific roles to oversee privacy related matters, including a DPO. Appropriate training and management support should be provided to support these roles.	Microsoft has published information on the Microsoft Data Protection Officer, the nature of their duties, reporting structure and contact information. - Microsoft DPO Information [14]	(37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)<
Human Resource Security (6.4)	The customer should determine and assign responsibility for providing relevant training related to protecting personal data.	An overview of the role of Microsoft's Data Protection Officer, the nature of his duties, reporting structure and contact information. - Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [12] - Training and Awareness Program Description [3]	(39)(1)(b)
Classification of Information (6.5.1)	The customer should explicitly consider personal data as part of a data classification scheme.	How Microsoft considers personal data in data classification, tagging and tracking information. - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [10]	(39)(1)(b)
Management of removable media (6.5.2)	The customer should determine internal policies for the use of removable media as it relates to the protection of personal data (e.g., encrypting devices).	How Microsoft services protect the security of personal information on any removable media. - Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [12] - Microsoft Professional Services Control Set [5]	(32)(1)(a), (5)(1)(f)

Physical media transfer (6.5.3)	The customer should determine internal policies for protecting personal data when transferring physical media (e.g. encryption).	How Microsoft services protect personal data during any transfer of physical media. - Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [12] - Microsoft Professional Services Control Set [5]	(32)(1)(a), (5)(1)(f)
User access management (6.6.1)	The customer should be aware of which responsibilities they have for access control within the service they are using, and manage those responsibilities appropriately, using the tools available.	The tools provided by Microsoft services to help you enforce access control. - Microsoft Professional Services Security Documentation on Microsoft Trust Center [2]	(5)(1)(f)
User registration and de-registration (6.6.2)	The customer should manage user registration and de-registration within the service they utilize, using the tools available to them.	The tools provided by Microsoft services to help you enforce access control. - Microsoft Professional Services Security Documentation on Microsoft Trust Center [2]	(5)(1)(f)
User access provisioning (6.6.3)	The customer should manage user profiles, especially for authorized access to personal data, within the service they utilize, using the tools available to them.	How Microsoft services support formal access control to personal data, including user IDs, roles, and the registration and de-registration of users. - Microsoft Professional Services Security Documentation on Microsoft Trust Center [2]	(5)(1)(f)
Management of privileged access (6.6.4)	The customer should manage user ID's to facilitate tracking of access (especially to personal data), within the service they utilize, using the tools available to them.	How Microsoft services support formal access control to personal data, including user IDs, roles, and the registration and de-registration of users. - Microsoft Professional Services Security Documentation on Microsoft Trust Center [2]	(5)(1)(f)
Secure log on procedures (6.6.5)	The customer should utilize provided mechanisms in the service to ensure secure log on capabilities for their users where necessary.	How Microsoft services support internal access control policies related to personal data. - Who can access your data and on what terms [7]	(5)(1)(f)

Cryptography (6.7)	The customer should determine which data may need to be encrypted, and whether the service they are utilizing offers this capability. The customer should utilize encryption as needed, using the tools available to them.	How Microsoft services support encryption and pseudonymization to reduce the risk of processing personal data. - Microsoft Professional Services Security Documentation on Microsoft Trust Center [2]	(32)(1)(a)
Secure disposal or re-use of equipment (6.8.1)	Where the customer uses cloud computing services (PaaS, SaaS, IaaS) they should understand how the cloud provider ensures that personal data is erased from storage space prior to that space being assigned to another customer.	How Microsoft Professional Services ensures that personal data is erased from storage equipment before that equipment is transferred or reused, when utilizing Microsoft Azure cloud computing services during professional services. - Microsoft Professional Services Data Security (Data Cleansing and Leakage) [4]	(5)(1)(f)
Clear desk and clear screen policy (6.8.2)	The customer should consider risks around hardcopy material that displays personal data, and potentially restrict the creation of such material. Where the system in use provides the capability to restrict this (e.g., settings to prevent printing or copying/pasting of sensitive data), the customer should consider the need to utilize those capabilities.	What Microsoft implements to manage hardcopy. - Microsoft maintains these controls internally, see Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [12] - Microsoft Professional Services GDPR Control Set [5]	(5)(1)(f)
Separation of development, testing and operational environments (6.9.1)	The customer should consider the implications of using personal data in development and testing environments within their organization.	How Microsoft ensures that personal data is protected in development and test environments. - Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [12] - Microsoft Professional Services Control Set [5]	(5)(1)(f)

Information backup (6.9.2)	The customer should ensure that they use system provided capabilities to create redundancies in their data and test as necessary.	How Microsoft ensures the availability of data that may include personal data, how accuracy of restored data is ensured, and the tools and procedures Microsoft services provide to allow you to backup and restore data. - Microsoft Enterprise Business Continuity Management Documentation [6]	(32)(1)(c), (5)(1)(f)
Event logging (6.9.3)	The customer should understand the capabilities for logging provided by the system and utilize such capabilities to ensure that they can log actions related to personal data that they deem necessary	The data Microsoft service records for you, including user activities, exceptions, faults and information security events, and how you can access those logs for use as part of your record keeping. - Microsoft Professional Services Security Documentation [2] - Microsoft Professional Services Control Set [5]	(5)(1)(f)
Protection of log information (6.9.4)	The customer should consider requirements for protecting log information that may contain personal data or that may contain records related to personal data processing. Where the system in use provides capabilities to protect logs, the customer should utilize these capabilities where necessary.	How Microsoft protects logs that may contain personal data. - Microsoft Professional Services Security Documentation[2] - Microsoft Professional Services Control Set [5]	(5)(1)(f)
Information transfer policies and procedures (6.10.)	The customer should have procedures for cases where personal data may be transferred on physical media (such as a hard drive being moved between servers or facilities). These may include logs, authorizations, and tracking. Where a third-party or other processor may be transferring physical media, the customer should ensure that that organization has procedures in place to ensure security of the personal data.	How Microsoft services transfer physical media that may contain personal data, including the circumstances when transfer might occur, and the protective measures taken to protect the data. - Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [12] - Microsoft Professional Services Control Set [5]	(5)(1)(f)

<i>Confidentiality or non-disclosure agreements (6.10.2)</i>	The customer should determine the need for confidentiality agreements or the equivalent for individuals with access to or responsibilities related to personal data.	How Microsoft services ensure that individuals with authorized access to personal data have committed themselves to confidentiality. - Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [12] - Microsoft Professional Services Control Set [5]	(5)(1)(f), (28)(3)(b), (38)(5)
<i>Securing application services on public networks (6.11.1)</i>	The customer should understand requirements for encryption of personal data, especially when sent over public networks. Where the system provides mechanisms to encrypt data, the customer should utilize those mechanisms where necessary.	Description of the measures Microsoft services take to protect data in transit, including encryption of the data, and how Microsoft services protect data that may contain personal data as it passes through public data networks, including any encryption measures. - Microsoft Professional Services Security Documentation [2]	(5)(1)(f), (32)(1)(a)
<i>Secure system engineering principles (6.11.2)</i>	The customer should understand how systems are designed and engineered to consider protection of personal data. Where a customer uses a system engineered by a third-party, it is their responsibility to ensure that such protections have been considered.	How Microsoft services include personal data protection principles as a mandatory part of our secure design/engineering principles. - Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [12] - What is the Security Development Lifecycle ?	(25)(1)
<i>Supplier Relationships (6.12)</i>	The customer should ensure that any information security and personal data protection requirements and that are the responsibility of a third-party are addressed in contractual information or other agreements. The agreements should also address the instructions for processing.	How Microsoft services address security and data protection in our agreements with our suppliers and how we ensure those agreements are effectively implemented. - Who can access your data and on what terms [7]	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)

Management of information security incidents and improvements (6.13.1)	The customer should have processes for determining when a personal data breach has occurred.	How Microsoft services determine if a security incident is a breach of personal data, and how we communicate the breach to you. - Microsoft Professional Services and Breach Notification Under the GDPR [9]	(33)(2)
Responsibilities and procedures (during information security incidents) (6.13.2)	The customer should understand and document their responsibilities during a data breach or security incident involving personal data. Responsibilities may include notifying required parties, communications with processors or other third-parties, and responsibilities within the customer's organization.	How to notify Microsoft services if you detect a security incident or breach of personal data. - Microsoft Professional Services and Breach Notification Under the GDPR [9]	(5)(1)(f), (33)(1), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2), (34)(3)(a), (34)(3)(b), (34)(3)(c), (34)(4)
Response to information security incidents (6.13.3)	The customer should have processes for determining when a personal data breach has occurred.	Description of the information Microsoft services provide to help you decide if a breach of personal data has occurred. - Microsoft Professional Services and Breach Notification Under the GDPR [9]	(33)(1), (33)(2), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2)
Protection of records (6.15.1)	The customer should understand the requirements for records related to personal data processing that need to be maintained.	How Microsoft services store records relating to the processing of personal data. - Microsoft Professional Services Security Documentation [2]	(5)(2), (24)(2)
Independent review of information security (6.15.2)	The customer should be aware of requirements for assessments of the security of personal data processing. This may include internal or external audits, or other measures for assessing the security of processing. Where the customer is dependent on another organization of third-party for all or part of the processing, they should collect information about such assessments performed by them.	How Microsoft services test and assesses the effectiveness of technical and organizational measures to ensure the security of processing, including any audits by third parties. - Microsoft Professional Services Data Protection Addendum [1]	(32)(1)(d), (32)(2)

Technical compliance review (6.15.3)	<p>The customer should understand requirements for testing and evaluating the security of processing personal data. This may include technical tests such as penetration testing. Where the customer uses a third-party system or processor, they should understand what responsibilities they have for securing and testing the security (e.g. managing configurations to secure data and then testing those configuration settings). Where the third-party is responsible for all or part of the security of processing, the customer should understand what testing or evaluation the third-party performs to ensure the security of the processing.</p>	<p>How Microsoft services are tested security based on identified risks, including tests by third parties, and the types of technical tests and any avail[1]</p> <ul style="list-style-type: none"> - For a listing of external certifications see Microsoft Trust Center Compliance offerings [13] - For more information about vulnerability testing your applications see Microsoft Professional Services Security Documentation [2] 	(32)(1)(d), (32)(2)

6. Bibliography of Resources and Links

ID	Description	URL
1	Microsoft Professional Services Data Protection Addendum	(http://aka.ms/professionalservicesdpa)
2	Microsoft Professional Services Security Documentation on Microsoft Trust Center	https://www.microsoft.com/TrustCenter/professional-services-security
3	Training and Awareness Program Description	Available on request through customer's account management team. https://gallery.technet.microsoft.com/Azure-Standard-Response-to-5de19cb6
4	Microsoft Azure Data Security (Data Cleansing and Leakage)	https://blogs.msdn.microsoft.com/walterm/2014/09/04/microsoft-azure-data-security-data-cleansing-and-leakage/
5	5. Microsoft Professional Services GDPR Control Set	Downloadable through Microsoft Service Trust Portal Compliance Manager at https://aka.ms/GDPRControls or via Compliance Manager https://servicetrust.microsoft.com/ComplianceManager

6	<i>Microsoft Enterprise Business Continuity Management Documentation</i>	Available on request through customer's account management team. https://gallery.technet.microsoft.com/Azure-Standard-Response-to-5de19cb6
7	<i>Who can access your data and on what terms</i>	https://www.microsoft.com/trustcenter/Privacy/Who-can-access-your-data-and-on-what-terms
8	<i>Microsoft Professional Services Data Subject Requests for the GDPR</i>	https://docs.microsoft.com/microsoft-365/compliance/gdpr-dsr-prof-services
9	<i>Microsoft Professional Services and Breach Notification Under the GDPR</i>	https://docs.microsoft.com/microsoft-365/compliance/gdpr-breach-microsoft-support-professional-services
10	<i>Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments</i>	https://docs.microsoft.com/microsoft-365/compliance/gdpr-dpia-prof-services
11	<i>ISO 27001 Audit Report</i>	
	Certification Report	https://www.bsigroup.com/Our-services/Certification/Certificate-and-Client-Directory-Search/Certificate-Client-Directory-Search-Results/?searchkey=licence%3d601002%26company%3dMicrosoft&licencenumber=IS%20601002
	Audit Report	Available on request through customer's technical account management team. https://gallery.technet.microsoft.com/Azure-Standard-Response-to-5de19cb6
12	<i>Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability</i>	SOA on request through customer's account management team https://gallery.technet.microsoft.com/Azure-Standard-Response-to-5de19cb6
13	<i>Microsoft Trust Center Compliance offerings</i>	https://www.microsoft.com/trustcenter/compliance/complianceofferings
14	<i>Microsoft DPO Information</i>	https://docs.microsoft.com/microsoft-365/compliance/gdpr-data-protection-officer

Learn more

[Microsoft Trust Center](#)

[Secure Trust Portal](#)

Information protection for GDPR with Microsoft 365 capabilities

12/5/2018 • 2 minutes to read • [Edit Online](#)

Microsoft 365 provides a rich set of capabilities to help you achieve compliance with the General Data Protection Regulation (GDPR). This article summarizes recommended capabilities with links to more information.

For more information about how Microsoft can help you with the GDPR, see [Get Started: Support for GDPR Accountability](#) in the Service Trust Portal.

Information protection

Office 365 provides a rich set of data governance capabilities. For help with finding, classifying, protecting, and monitoring personal data, see [Office 365 Information Protection for GDPR](#).

For help with on-premises servers, including file shares, SharePoint Server, Exchange Server, Skype for Business Server, Project Server, and Office Online Server, see [GDPR for on-premises Office servers](#).

Identity and access management

Azure Active Directory and other Microsoft 365 capabilities provide a rich set of capabilities to protect access to your data from identities and devices:

- Multi-factor authentication (MFA)
- Conditional access
- Privileged identity management
- Mobile device management
- Mobile application management
- Hardware protection for credentials

Microsoft provides a recommended configuration you can use as a starting point:

- [Identity and device access configurations](#): Recommended policy configurations to achieve three tiers of protection (baseline, sensitive, highly regulated). This guidance includes recommended policies for Exchange Online and SharePoint Online (including OneDrive for Business).
- [Security guidance for political campaigns, nonprofits, and other agile organizations](#): This includes the same set of policies but provides additional guidance for BYOD environments and for B2B accounts.

Threat Protection

Threat protection is built across Microsoft 365 services. Here are a few resources to get you started:

- [Office 365 security roadmap: Top priorities for the first 30 days, 90 days, and beyond](#). This roadmap includes recommendations for implementing capabilities.
- [Protect against threats in Office 365](#). Learn about protection actions you can take in the Office 365 Security and Compliance Center.
- [Windows Threat Protection](#). Learn more about Windows Defender Advanced Threat Protection and other capabilities in Windows 10.

[Learn more](#)

[Microsoft Trust Center](#)

Data Subject Requests for the GDPR

2/22/2019 • 2 minutes to read • [Edit Online](#)

The General Data Protection Regulation (GDPR) gives rights to people (known in the regulation as data subjects) to manage the personal data that has been collected by an employer or other type of agency or organization (known as the data controller or just controller). Personal data is defined very broadly under the GDPR as any data that relates to an identified or identifiable natural person. The GDPR gives data subjects specific rights to their personal data; these rights include obtaining copies of it, requesting changes to it, restricting the processing of it, deleting it, or receiving it in an electronic format so it can be moved to another controller. A formal request by a data subject to a controller to take an action on their personal data is called a Data Subject Request or DSR. The controller is obligated to promptly consider each DSR and provide a substantive response either by taking the requested action or by providing an explanation for why the DSR cannot be accommodated by the controller. A controller should consult with its own legal or compliance advisers regarding the proper disposition of any given DSR.

These articles discusses how to use Microsoft products, services, and administrative tools to help you find and act on personal data to respond to DSRs:

- [Office 365](#)
- [Azure](#)
- [Intune](#)
- [Dynamics 365](#)
- [Visual Studio Family](#)
- [Azure DevOps Services](#)
- [Microsoft Support and Professional Services](#)

For more information about how Microsoft enables you to respond to DSRs, see [GDPR: Data Subject Requests \(DSRs\)](#) in the Service Trust Portal.

Learn more

[Microsoft Trust Center](#)

Office 365 Data Subject Requests for the GDPR

2/22/2019 • 134 minutes to read • [Edit Online](#)

Introduction to DSRs

The General Data Protection Regulation (GDPR) gives rights to people (known in the regulation as *data subjects*) to manage the personal data that has been collected by an employer or other type of agency or organization (known as the *data controller* or just *controller*). Personal data is defined very broadly under the GDPR as any data that relates to an identified or identifiable natural person. The GDPR gives data subjects specific rights to their personal data; these rights include obtaining copies of it, requesting changes to it, restricting the processing of it, deleting it, or receiving it in an electronic format so it can be moved to another controller. A formal request by a data subject to a controller to take an action on their personal data is called a *Data Subject Request* or DSR. The controller is obligated to promptly consider each DSR and provide a substantive response either by taking the requested action or by providing an explanation for why the DSR cannot be accommodated by the controller. A controller should consult with its own legal or compliance advisers regarding the proper disposition of any given DSR.

The guide discusses how to use Office 365 products, services and administrative tools to help you find and act on personal data to respond to DSRs. Specifically, this includes how to find, access, and act on personal data that resides in Microsoft's cloud. Here's a quick overview of the processes outlined in this guide:

1. **Discover**—Use search and discovery tools, such as those offered by the Microsoft Security & Compliance Center (SCC), to more easily find customer content that may be the subject of a DSR. Once potentially responsive documents are collected, you can perform one or more of the DSR actions described in the following steps to respond to the DSR request. Alternatively, you may determine that the request doesn't meet your organizations guidelines for responding to DSRs.
2. **Access**—Retrieve personal data that resides in the Microsoft cloud and, if requested, make a copy of it available to the data subject.
3. **Rectify**—Make changes or implement other requested actions on the personal data, where applicable.
4. **Restrict**—Restrict the processing of personal data, either by removing licenses for various Office 365 services, or by turning off the desired services or features where possible. You can also remove data from the Microsoft cloud and retain it on-premises or at another location.
5. **Delete**—Permanently remove personal data that resides in the Microsoft cloud.
6. **Export**—Provide an electronic copy of personal data to the data subject. The GDPR's "right of data portability" allows a data subject to request an electronic copy of personal data that's in a structured, commonly used, machine-readable format.

Terminology

Here are definitions of terms from the GDPR that are relevant to this guide.

- **Controller**—The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- **Personal data and data subject**—Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social

identity of that natural person.

- **Processor**—A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

How to use this guide

To help you find information relevant to your use case, this guide is divided into four parts.

Part 1: Responding to DSRs for Customer Data - *Customer Data* is data produced and stored in Office 365 in the day-to-day operations of running your business. Examples of the most commonly used Office 365 applications which allow you to author data include Word, Excel, PowerPoint, Outlook and OneNote. Office 365 also consists of applications such as SharePoint Online, Teams, and Forms which allow you to better collaborate with others. Part 1 of this guide discusses how to discover access, rectify, restrict, delete, and export data from Office 365 applications that have been used to author and store data in Office 365 online services. It addresses products and services for which Microsoft is acting as a data processor to your organization, and thus DSR capability is made available to your tenant administrator.

Part 2: Responding to DSRs with Respect to Insights Generated by Office 365 - Office 365 provides certain insights through services like Delve, MyAnalytics, and Workplace Analytics. How these insights are generated and how to respond to DSRs related to them are explained in Part 2 of this guide.

Part 3: Responding to DSRs for system-generated Logs - When you use Office 365 enterprise services, Microsoft generates some information such as service logs that record the use or performance of features in the online services. Most service generated data contain pseudonymous identifiers generated by Microsoft and this category is thus generally referred to within this document as *system-generated logs*. Although this data can't be attributed to a specific data subject without the use of additional information, some of it may be deemed personal under GDPR's definition for "personal data." Part 3 of this guide discusses how to access, delete, and export system-generated logs.

Part 4: Additional resources to assist you with DSRs - Part 4 of this guide lists limited scenarios in which Microsoft is the data controller when certain Office 365 products and services are used.

NOTE

In most cases, when users in your organization use Microsoft Office 365 products and services, you are the data controller and Microsoft is the processor. As a data controller, you are responsible for responding to the data subject directly. To assist you with this, Parts 1-3 of this guide detail the technical capabilities available to your organization to respond to a DSR request. In some limited scenarios, however, Microsoft will be the data controller when people use certain Office 365 products and services. In these cases, the information in Part 4 provides guidance on how data subjects can submit DSR requests to Microsoft.

Office 365 national clouds

The Microsoft Office 365 services are also available in the following national cloud environments: [Office 365 Germany](#), [Office 365 operated by 21Vianet \(China\)](#), and [Office 365 US Government](#). Most of the guidance for managing data subject requests described in this document applies to these national cloud environments. However, due to the isolated nature of these environments, there are some exceptions. Where notable for a given subsection, these exceptions are called out in a corresponding note.

Hybrid deployments

Your Office 365 organization may consist of Microsoft offerings that are a combination of cloud-based services and on-premises server products. In general, a hybrid deployment is typically the sharing of user accounts (identity management) and resources (such as mailboxes, web sites, and data) that exist in the cloud and on-premises. Common hybrid scenarios include:

- Exchange hybrid deployments, where some users have an on-premises mailboxes and other users have

Exchange Online mailboxes.

- SharePoint hybrid deployments, where site and file servers are on-premises and OneDrive for Business accounts are in Office 365.
- The on-premises identity management system (Active Directory) that is synchronized with Azure Activity Directory, which is the underlying directory service in Office 365.

When responding to a DSR request, you may have to determine if data that's responsive to a DSR request is in the Microsoft cloud or in your on-premise organization, and then take the appropriate steps to respond to that request. The Office 365 Data Subject Request Guide (this guide) provides guidance for responding to cloud-based data. For guidance for data in your on-premises organization, see [GDPR for Office on-premises Servers](#).

Part 1: Responding to DSRs for Customer Data

The guidance for responding to DSRs for Customer Data is divided into the following four sections.

- [Using the Content Search eDiscovery tool to respond to DSRs](#)
- [Using In-App functionality to respond to DSRs](#)
- [Responding to DSR rectification requests](#)
- [Responding to DSR restriction requests](#)

How to determine the Office 365 applications that may be in scope for a DSR for Customer Data

To help you determine where to search for personal data or what to search for, it helps to identify the Office 365 applications that people in your organization can use to create and store data in Office 365. Knowing this narrows the Office 365 applications that are in-scope for a DSR and helps you determine how you will search for and access personal data that's related to a DSR. Specifically, this means whether you can use the Content Search tool or if you'll have to use the in-app functionality of the application the data was created in.

A quick way to identify the Office 365 applications that people in your organization are using to create Customer Data is to determine which applications are included in your organization's Office 365 subscription. To do this, you can access user accounts in the Office 365 admin portal and look at the product licensing information. See [Assign licenses to users in Office 365 for business](#).

Using the Content Search eDiscovery tool to respond to DSRs

When looking for personal data within the larger set of data your organization creates and stores using in Office 365, you may want to first consider which applications people have most likely used to author the data you're looking for. Microsoft estimates that over 90% of an organization's data that is stored in Office 365 is authored in Word, Excel, PowerPoint, OneNote, and Outlook. Documents authored in these Office applications, even if purchased through Office 365 ProPlus or an Office perpetual license, are most likely stored on a SharePoint Online site, in a user's OneDrive for Business account, or in a user's Exchange Online mailbox. That means you can use the Content Search eDiscovery tool to search (and perform other DSR-related actions) across SharePoint Online sites, OneDrive for Business accounts, and Exchange Online mailboxes (including the sites and mailboxes associated with Office 365 Groups, Microsoft Teams, EDU Assignments, and StaffHub) to find documents and mailbox items that may be relevant to the DSR you're investigating. You can also use the Content Search tool to discover Customer Data authored in other Office 365 applications.

The following table lists the Office 365 applications that people use to create Customer Authored Content and that can be discovered by using Content Search. This section of the DSR guide provides guidance about how discover, access, export, and delete data created with these Office 365 applications.

Table 1: Applications where Content Search can be used to find Customer Data

	Calendar		SharePoint Online
	Excel		Skype for Business
	Office Lens		Tasks
	OneDrive for Business		Teams
	OneNote		To-Do
	Outlook/Exchange Online		Video
	People		Visio
	PowerPoint		Word

NOTE

The Content Search eDiscovery tool is not available in [Office 365 operated by 21Vianet \(China\)](#). This means you won't be able to use this tool to search for and export Customer Data in the Office 365 applications shown in Table 1. However, you can use the In-Place eDiscovery tool in Exchange Online to search for content in user mailboxes. You can also use the eDiscovery Center in SharePoint Online to search for content in SharePoint sites and OneDrive accounts. Alternatively, you can ask a document owner to help you find and make changes or deletions to content or export it if necessary. For more information, see:

- [Create an In-Place eDiscovery search](#)
- [Set up an eDiscovery Center in SharePoint Online](#)

Using Content Search to find personal data

The first step in responding to a DSR is to find the personal data that is the subject of the DSR. This consists of

using Office 365 eDiscovery tools to search for personal data (among all your organization's data in Office 365) or going directly to the native application in which the data was created. This first step - finding and reviewing the personal data at issue - will help you determine whether a DSR meets your organization's requirements for honoring or declining a data subject request. For example, after finding and reviewing the personal data at issue, you may determine the request doesn't meet your organization's requirements because doing so may adversely affect the rights and freedoms of others, or because the personal data is contained in a business record your organization has a legitimate business interest in retaining.

As previously stated, Microsoft estimates that over 90% of an organization's data is created with Office applications, such as Word and Excel. This means that you can use the Content Search in the Security & Compliance Center to search for most DSR-related data.

This guide assumes that you or the person searching for personal data that may be responsive to a DSR request is familiar with or has experience using the Content Search tool in the Security & Compliance Center. For general guidance on using Content Search, see [Content Search in Office 365](#). Be sure that the person running the searches has been assigned the necessary permissions in the Security & Compliance Center. This person should be added as a member of the eDiscovery Manager role group in the Security & Compliance Center; see [Assign eDiscovery permissions in the Office 365 Security & Compliance Center](#). Consider adding other people in your organization who are involved in investigating DSRs to the eDiscovery Manager role group, so they can perform the necessary actions in the Content Search tool such as previewing and exporting search results. However, unless you set up compliance boundaries (as described [here](#)) be aware that an eDiscovery Manager can search all content locations in your organization, including ones that may not be related to a DSR investigation.

After you find the data, you can then perform the specific action to satisfy the request by the data subject.

NOTE

In Office 365 Germany, the Security & Compliance Center is located at <https://protection.office.de>.

Searching content locations

You can search the following types of content locations with the Content Search tool.

- Exchange Online mailboxes; this includes the mailboxes associated with Office 365 Groups and Microsoft Teams
- Exchange Online public folders
- SharePoint Online sites; this includes the sites associated with Office 365 Groups and Microsoft Teams
- OneDrive for Business accounts

NOTE

This guide assumes that all data that might be relevant to a DSR investigation is stored in Office 365; in other words, stored in the Microsoft cloud. Data stored on a user's local computer or on-premises on your organization's file servers is outside the scope of a DSR investigation for data stored in Office 365. For guidance about responding to DSR requests for data in on-premises organizations, see [GDPR for Office on-premises Servers](#).

Tips for searching content locations

- Begin by searching all content locations in your organization (which you can search in a single search) to quickly determine which content locations contain items that match your search query. Then you can re-run the search and narrow the search scope to the specific locations that contain relevant items.
- Use search statistics to identify the top locations that contain items that match your search query. See [View keyword statistics for Content Search results](#).

- Search the Office 365 audit log for recent file and folder activities performed by the user who is the subject of the DSR. Searching the audit log will return a list of auditing records that will contain the name and location of resources the user has recently interacted with. You may be able to use this information to build a content search query. See [Search the audit log in the Office 365 Security & Compliance Center](#).

Building search queries to find personal data

The DSR you're investigating most likely will contain identifiers that you can use in the keyword search query to search for the personal data. Here are some common identifiers that can be used in a search query to find personal data:

- Email address or alias
- Phone number
- Mailing address
- Employee ID number
- National ID number or EU member version of a Social Security Number

The DSR that you're investigating most likely will have an identifier and other details about the personal data that is the subject of the request that you can use in a search query.

Searching for just an email address or employee ID will probably return a lot of results. To narrow the scope of your search so it returns content most relevant to the DSR, you can add conditions to the search query. When you add a condition, the keyword and a search condition are logically connected by the **AND** Boolean operator. This means only items that match *both* the keyword and the condition will be returned in the search results.

The following table lists some conditions you can use to narrow the scope of a search. The table also lists the values that you can use for each condition to search for specific document types and mailbox items.

Table 2: Narrow scope of search by using conditions

Condition	Description	Example of condition values
File type	<p>The extension of a document or file. Use this condition to search for Office documents and files created by Office 365 applications. Use this condition when searching for documents located on SharePoint Online sites and OneDrive for Business accounts. Note that the corresponding document property is filetype.</p> <p>For a complete list of file extensions that you can search for, see Default crawled file name extensions and parsed file types in SharePoint.</p>	<ul style="list-style-type: none"> • csv – Searches for comma separated value (CSV) files; Excel files can be saved in CSV format and CSV file can easily be imported into Excel • docx – Searches for Word file • mpp – Searches for Project files
 • one – Searches for OneNote files • pdf – Search for files saved in a PDF format • pptx – Searches for PowerPoint files • xlxs – Searches for Excel files • vsd – Searches for Visio files • wmv – Searches for Windows Media video files

Message type	The email message type to search for. Use this condition to search mailboxes for contacts (People), meetings (Calendar) tasks, or Skype for Business conversations. Note that the corresponding email property is <i>kind</i> .	<ul style="list-style-type: none"> <i>contacts</i> – Searches the My Contacts list (People) of a mailbox <i>email</i> – Searches email messages <i>im</i> – Searches Skype for Business conversations <i>meetings</i> – Searches appointments and meeting requests (Calendar) <i>tasks</i> – Searches the My Tasks list (Tasks); using this value will also return tasks created in Microsoft To-Do.
Compliance tag	The label assigned to an email message or a document. Labels are used to classify email and documents for data governance and enforce retention rules based on the classification defined by the label. Use this condition to search for items that have been automatically or manually assigned a label. This is a useful condition for DSR investigations because your organization may be using labels to classify content related to data privacy or that contains personal data or sensitive information. See the "Using Content Search to find all content with a specific label applied to it" section in Overview of labels in Office 365 .	compliancetag="personal data"

There are many more email and document properties and search conditions that you can use to build more complex search queries. See the following sections in the [Keyword queries and search conditions for Content Search](#) help topic for more information.

- [Searchable email properties](#)
- [Searchable site \(document\) properties](#)
- [Search conditions](#)

Searching for personal data in SharePoint lists, discussions, and forms

In addition to searching for personal data in documents, you can also use Content Search to search for other types of data that's created by using native SharePoint Online apps. This includes data created by using SharePoint lists, discussions, and forms. When you run a Content Search and search SharePoint Online sites (or OneDrive for Business accounts) data from lists, discussions, and forms that match the search criteria will be returned in the search results.

Examples of search queries

Here are some examples of search queries that use keywords and conditions to search for personal data in response to a DSR. The examples show two versions of the query: one of the keyword syntax (where the condition is included in Keyword box) and one showing the GUI-based version of the query with conditions.

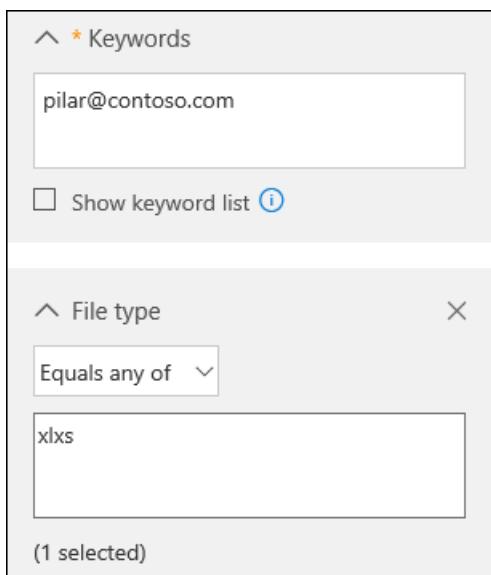
Example 1

This example returns Excel files located on SharePoint Online sites and OneDrive for Business accounts that contain the specified email address. Note that files might be returned if the email address appears in the file metadata.

Keyword syntax

pilar@contoso.com AND filetype="xlsx"

GUI

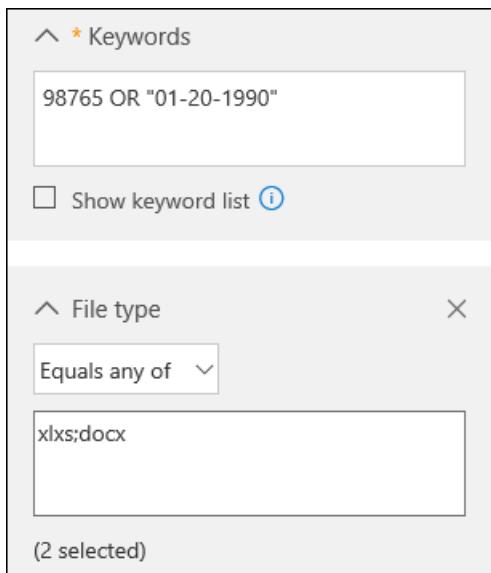


Example 2

This example returns Excel or Word files located on SharePoint Online sites and OneDrive for Business accounts that contain the specified employee ID or birth date.

(98765 OR "01-20-1990") AND (filetype="xlsx" OR filetype="docx")

GUI



Example 3

This example returns email messages that contain the specified ID numbers, which is a France Social Security Number (INSEE)

"1600330345678 97" AND kind="email"

GUI

The screenshot shows the Microsoft 365 search interface with two filter panels. The first panel, 'Keywords', contains the search term '"1600330345678 97"' and a checkbox for 'Show keyword list'. The second panel, 'Message kind', is set to 'Equals any of' and includes the option 'email', with '(1 selected)' indicating one item is chosen.

Working with partially indexed items in Content Search

Partially indexed items (also called *unindexed items*) are Exchange Online mailbox items and documents on SharePoint Online and OneDrive for Business sites that for some reason weren't completely indexed for search, which means they aren't searchable by using Content Search. Most email messages and site documents are successfully indexed because they fall within the [indexing limits for Office 365](#). The reasons that email messages or files aren't indexed for search include:

- The file type is file type is [unrecognized or unsupported for indexing](#); though sometimes the file type is supported for indexing but an indexing error occurred for a specific file
- Email messages have an attached file without a valid handler, such as image file (this is the most common cause of partially indexed email items)
- Files attached to email messages are too large or there are too many attached files

We recommend that you learn more about partially indexed items so that you can work with them when responding to DSR requests. For more information, see:

- [Partially indexed items in Content Search in Office 365](#)
- [Investigating partially indexed items in Office 365 eDiscovery](#)
- [Exporting unindexed items](#)

Tips for working with partially indexed items

It's possible that data responsive to a DSR investigation may be in a partially indexed item. Here's some suggestions for working with partially indexed items:

- After you run a search, the number of estimated partially items is displayed in the search statistics; this estimate doesn't include partially indexed items in SharePoint Online and OneDrive for Business. Export the reports for a Content Search to get information about partially indexed items. The **Unindexed Items.csv** report contains information about unindexed items, including the location of the item, the URL if the item is in SharePoint Online or OneDrive for Business, and the subject line (for messages) or name of the document. For more information, see [Export a Content Search report](#).
- The statistics and list of partially indexed items that are returned with the results of a Content Search are all the partially items from the content locations that are searched.
- To retrieve partially indexed items that are potentially responsive to a DSR investigation, you can do one of the following things.

[Export all partially indexed items](#)

You export the both the results of a content search and the partially indexed items from the content location that

were search. You can also export only the partially indexed items. Then you can open them in their native application and review the content. You have to use this option to export items from SharePoint Online and OneDrive for Business. See [Export Content Search results from the Office 365 Security & Compliance Center](#).

Export a specific set of partially indexed items from mailboxes

Instead of exporting all partially indexed mailbox items from a search, you can re-run a Content Search to search for a specific list of partially indexed items, and then export them. Note that you can do this only for mailbox items. See [Prepare a CSV file for a targeted Content Search in Office 365](#).

Next steps

After you find the personal data that's relevant to the DSR, be sure to retain the specific Content Search that you used to find the data. You will likely re-use this search to complete other steps in the DSR response process, such as [obtaining a copy of it, exporting it, or permanently deleting it](#).

Additional considerations for selected applications

The following sections describe things you should keep in mind when searching for data in the following Office 365 applications.

- [Office Lens](#)
- [OneDrive for Business and SharePoint Experience Settings](#)
- [Microsoft Teams for Education](#)
- [Microsoft To-Do](#)
- [Skype for Business](#)

Office Lens

A person using Office Lens (a camera app supported by devices running iOS, Android, and Windows) can take a picture of whiteboards, hardcopy documents, business cards, and other things that contain a lot of text. Office Lens uses optical character recognition technology that will extract text in an image and save it to an Office document such as a Word, PowerPoint, and OneNote or to a PDF file. Users can then upload the file that contains the text from the image to their OneDrive for Business account in Office 365. That means you can use the Content Search tool to search, access, delete, and export data in files that were created from an Office Lens image. For more information about Office Lens, see:

- [Office Lens for iOS](#)
- [Office Lens for Android](#)
- [Office Lens for Windows](#)

OneDrive for Business and SharePoint Online experience settings

In addition to user-created files stored in OneDrive for Business accounts and SharePoint Online sites, these services store information about the user that is used to enable various experiences. Users still in your organization can access much of this information by using in-product functionality. The following information provides guidance on how to access, view, and export OneDrive for Business and SharePoint Online application data.

SharePoint user profiles

The user's Delve profile allows users to maintain properties stored in the SharePoint Online user profile, including birthday, mobile phone number (and other contact information), about me, projects, skills and expertise, schools and education, interests, and hobbies.

End users

End users can discover, access, and rectify SharePoint Online user profile data using the Delve profile experience. See [View and update your profile in Office Delve](#) for more details.

Another way for users to access their SharePoint profile data is to navigate to the **edit profile page** in their OneDrive for Business account, which can be accessed by going to the **EditProfile.aspx** path under the OneDrive

for Business account URL. For example, for a user **user1@contoso.com**, the user's OneDrive for Business account is located at:

```
https://contoso-my.sharepoint.com/personal/user1\contoso\_com/\_layouts/15/OneDrive.aspx
```

The URL for the edit profile page would be:

```
https://contoso-my.sharepoint.com/personal/user1\contoso\_com/\_layouts/15/EditProfile.aspx
```

Note that properties sourced in Azure Active Directory can't be changed within SharePoint Online. However, users can go to their **Account** page by selecting their **photo** in the Office 365 header, and then selecting **My account**. Changing the properties here may require users to work with their admins to discover, access, or rectify a user profile property.

Admins

An admin can access and rectify profile properties in the SharePoint admin center. In the **SharePoint admin center**, click the **user profiles** tab. Click **Manage user profiles**, enter a user's name, and then click **Find**. The admin can right-click any user and select **Edit My Profile**. Note that properties sourced in Azure Active Directory can't be changed within SharePoint Online.

An admin can export all User Profile properties for a user by using the **Export-SPOUserProfile** cmdlet in SharePoint Online PowerShell. See [Export-SPOUserProfile](#).

For more information about user profiles, see [Manage user profiles in the SharePoint admin center](#).

User Information list on SharePoint Online sites

A subset of a user's SharePoint user profile is synchronized to the User information list of every site that they visit or have permissions to access. This is used by SharePoint Online experiences, such as People columns in document libraries, to display basic information about the user, such as the name of the creator of a document. The data in a User Information list will match the information stored in SharePoint user profile and will be automatically rectified if the source is changed. For deleted users, this data remains in the sites they interacted with for referential integrity of SharePoint column fields.

Admins can control which properties are replicable inside the SharePoint admin center. To do this:

1. Go to the **SharePoint admin center** and click the **user profiles** tab.
2. Click **Manage User Properties** to see a list of properties.
3. Right-click any property and select **Edit** and adjust various settings.
4. Under **Policy Settings**, the replicable property controls whether the property will be represented in the User information list. Note that not all properties support adjusting this.

An admin can export all User information properties for a user on a given site by using the **Export-SPOUserInfo** cmdlet in SharePoint Online PowerShell. See [Export-SPOUserInfo](#).

OneDrive for Business experience settings

A user's OneDrive for Business experience stores information to help the user find and navigate content of interest to them. Most of this information can be accessed by end users using in-product features. An admin can export the information using a [PowerShell Script](#) and [SharePoint Client-Side Object Model \(CSOM\)](#) commands.

See [Export OneDrive for Business experience settings](#) for more information about the settings, how they are stored, and how to export them.

OneDrive for Business and SharePoint Online search

The in-app search experience in OneDrive for Business and SharePoint Online stores a user's search queries for 30 days to increase relevance of search results. An admin can export search queries for a user by using the **Export-SPOQueryLogs** cmdlet in SharePoint Online PowerShell. See [Export-SPOQueryLogs](#).

Microsoft Teams for Education

Microsoft Teams for Education offers two additional collaboration features that teachers and students can use that creates and stores personal data: Assignments and OneNote Class Notebook. You can use Content Search to discover data in both.

Assignments

Students files associated with an Assignment are stored in a document library in the corresponding Teams SharePoint Online site. IT admins can use the Content Search tool to search for student files that are related to assignments. For example, an admin could search all SharePoint Online sites in the organization and use the student's name and class or assignment name in the search query to find data relevant to a DSR.

There's other data related to Assignments that isn't stored in the class team SharePoint Online site, which means it's not discoverable with Content Search. This includes:

- Files that the teacher assigns to students as part of the assignment
- Student grades and feedback from the teacher
- The list of documents submitted for an assignment by each student
- Assignment metadata

For this type of data, an IT admin or data owner (such as a teacher) may have to go into the Assignment in the class team to find data relevant to a DSR.

OneNote Class Notebook

The OneNote Class Notebook is stored in the class team SharePoint Online site. Every student in a class has a private notebook that's shared with the teacher. There's also a content library where a teacher can share documents with students, and a collaboration space for all students in the class. Data related to these capabilities is discoverable with Content Search.

Here's specific guidance to search for a Class Notebook.

1. Run a Content Search using the following search criteria:

- Search all SharePoint Online sites
- Include the name of the class team as a search keyword; for example, "9C Biology."

2. Preview the search results and look for the item that corresponds to the Class Notebook.

3. Select that item, and then copy the folder path that's displayed in the details pane. This is the root folder for the Class Notebook.

4. Edit the search that you created in step 1 and replace the class name in the keyword query with the folder path of the Class Notebook and precede the folder path with the **path** site property; for example, **path:"[https://contosoedu.onmicrosoft.com/sites/9C Biology/SiteAssets/9C Biology Notebook/](https://contosoedu.onmicrosoft.com/sites/9C%20Biology/SiteAssets/9C%20Biology%20Notebook/)"**. Be sure to include the quotation marks and the trailing forward slash.

5. Add a search condition and select the File Type condition and use one for the value of the file type. This will return all OneNote files in the search results. The resulting keyword syntax would look something like this:

```
path:"<https://contosoedu.onmicrosoft.com/sites/9C Biology/SiteAssets/9C Biology Notebook/>" AND filetype="one"
```

6. Re-run the Content Search. The search results should include all OneNote files for the Class Notebook from the class team.

Microsoft To-Do

Tasks (called *to-dos*, which are saved in *to-do lists*) in Microsoft To-Do are saved as tasks in a user's Exchange

Online mailbox. That means that you can use the Content Search tool to search, access, delete, and export to-dos. For more information, see [Set up Microsoft To-Do](#).

Skype for Business

Here some additional information about how to access, view, and export personal data in Skype for Business.

- Files attached to a meeting are retained in the actual meeting for 180 days and then become inaccessible. These files can be accessed by meeting participants by joining the meeting from the meeting request and then viewing or downloading the attached file. See the "Use the attachments in the meeting" section in [Preload attachments for a Skype for Business meeting](#).
- Conversations in Skype for Business are retained in the Conversation History folder in user mailboxes. You can use Content Search to search mailboxes for data in Skype conversations.
- A data subject can export their contacts in Skype for Business. To do this, they would right-click a contact group in Skype for Business and click **Copy**. Then they can paste the list of email addresses into a text or Word document.
- If the Exchange Online mailbox of a meeting participant is placed on Litigation Hold or assigned to an Office 365 retention policy, files attached to a meeting are retained in the participant's mailbox. You can use Content Search to search for those files in the participant's mailbox if the retention period for the file has not expired. For more information about retaining files, see [Retaining large files attached to a Skype for Business meeting](#).

Providing a copy of personal data

After you've found personal data that is potentially responsive to a DSR, it's up to you and your organization to decide which data to provide the data subject. For example, you can provide them with a copy of the actual document, an appropriately redacted version, or a screenshot of the portions that you've deemed appropriate to share. For each of these responses to an access request, you'll have to retrieve a copy of the document or other item that contains the responsive data.

When providing a copy to the data subject, you may have to remove or redact personal information about other data subjects and any confidential information.

Using Content Search to get a copy of personal data

There are two ways to use the Content Search tool to get a copy of a document or mailbox item that you've found after running a search.

- Preview the search results and then download a copy of the document or item. This is a good way to download a few items or files.
- Export the search results and then download a copy of all items returned by the search. This method is more complex, but it's a good way to download lots of items that are responsive to the DSR. Useful reports are also included with your export search results. You can use these reports to get additional information about each item. The **Results.csv** report is particularly useful because it contains a lot of information about the exported items, such as the exact location of the item (for example, the mailbox for email messages or the URL for documents or lists located on SharePoint Online and OneDrive for Business sites). This information will help you identify the owner of the item, in case you need to contact them during the DSR investigation process. For more information about the reports that are included when you export search results, see [Export a Content Search report](#).

Preview and download items

After you run a new search or open an existing search, you can preview each item that matched the search query to verify that it's related to the DSR you're investigating. This also includes SharePoint lists and web pages that are returned in the search results. You can also download the original file if you have to provide it to the data subject. In both cases you could take a screenshot to satisfy the data subject's request obtain the information.

Note that some types of items can't be previewed. If an item or file type isn't supported for preview, you have the option to download an individual item to your local computer or to a mapped network drive or other network location. You can only preview [supported file types](#).

To preview and download items:

1. Open the Content Search in the Security & Compliance Center.
2. If the results aren't displayed, click **Preview results**.
3. Click an item to view it.
4. Click **Download original file** to download the item to your local computer. You'll also have to download items that can't be previewed.

For more information about previewing search results, see [Preview search results](#).

Export and download items

You can also export the results of a content search to get a copy of email messages, documents, lists, and web pages containing the personal data, though this method is more involved than previewing items. See the next section for details about [exporting the results of a Content Search](#).

Exporting personal data

The "right of data portability" allows a data subject to request an electronic copy of personal data that's in a "structured, commonly used, machine-readable format", and to request that your organization transmit these electronic files to another data controller. Microsoft supports this right in two ways:

- Offering Office 365 applications that save data in native, machine-readable, commonly-used electronic format. For more information about Office file formats, see [Office File Formats-Technical Documents](#).
- Enabling your organization to export the data in the native file format, or a format (such as CSV, TXT, and JSON) that can be easily imported to another application.

To meet a DSR export request, you can export Office documents in their native file format and export data from other Office 365 applications.

Export and download content using Content Search

When you export the results of a Content Search, email items can be downloaded as PST files or as individual messages (.msg files). When you export documents and lists from SharePoint Online and OneDrive for Business sites, copies in the native file formats are exported. For example, SharePoint lists are exported as CSV files and Web pages are exported as .aspx or html files.

NOTE

Exporting mailbox items from a user's mailbox using Content Search requires that the user (whose mailbox you're exporting items from) is assigned an Exchange Online Plan 2 license.

To export and download items:

1. Open the Content Search in the Security & Compliance Center.
2. On the search fly out page, click **More**, and then click **Export results**. Note that you can also export a report.
3. Complete the sections on the **Export results** fly out page. Be sure to use the scroll bar to view all export options.

4. Go back to the Content search page in the Security & Compliance Center, and click the **Export** tab.
5. Click **Refresh** to update the page.
6. Under the **Name** column, click the export job that you just created. The name of the export job is the name of the content search appended with **_Export**.
7. On the export fly out page, under **Export key, click Copy to clipboard**. You'll use this key in step 10 to download the search results
8. On the top of the fly out page, click **Download results**.
9. If you're prompted to install the **Microsoft Office 365 eDiscovery Export Tool**, click **Install**.
10. In the **eDiscovery Export Tool**, paste the export key that you copied in step 7 in the appropriate box.
11. Click **Browse** to specify the location where you want to download the search result files.
12. Click **Start** to download the search results to your computer.

When the export process is complete, you can access the files in the location on your local computer where they were downloaded. Results of a content search are downloaded to a folder named after the Content Search. Documents from sites are copied to a subfolder named **SharePoint**. Mailbox items are copied to subfolder named **Exchange**.

For detailed step-by-step instructions, see [Export Content Search results from the Office 365 Security & Compliance Center](#).

Downloading documents and lists from SharePoint Online and OneDrive for Business

Another way to export data from SharePoint Online and OneDrive for Business is to download documents and lists directly from a SharePoint Online site or a OneDrive for Business account. You would have to get assigned the permissions to access a site, and then go to the site and download the contents. See:

- [Download files and folders from OneDrive or SharePoint](#)
- [Export SharePoint lists to Excel](#)

For some DSR export requests, you may want to allow the data subject to download content themselves. This enables the data subject to go to a SharePoint Online site or shared folder and click **Sync** to sync all contents in the document library or selected folders. See:

- [Enable users to sync SharePoint files with the new OneDrive sync client](#)
- [Sync SharePoint files with the new OneDrive sync client](#)

Deleting personal data

The “right to erasure” by the removal of personal data from an organization’s Customer Data is a key protection in the GDPR. Removing personal data includes deleting entire documents or files or deleting specific data within a document or file (which would be an action and process like the ones described in the Rectify section in this guide).

As you investigate or prepare to delete personal data in response to a DSR, here are a few important things to understand about how data deletion (and retention) works in Office 365.

- **Soft delete vs. hard delete** – In Office 365 services such as Exchange Online, SharePoint Online, and OneDrive for Business there is the concept of *soft deletion* and *hard deletion*, which relates to the recoverability of a deleted item (usually for a limited period) before it's permanently removed from the Microsoft cloud with no chance of recovery. In this context, a soft-deleted item can be recovered by a user and/or an admin for a limited amount of time before it's hard-deleted. When an item has been hard-deleted, it's marked for permanent removal and is purged as soon as it's processed by the corresponding Office 365

service. Here's how soft delete and hard delete works for items in mailboxes and sites (regardless of whether the data owner or an admin deletes an item):

- **Mailboxes:** A item is soft-deleted when it's deleted from the Deleted Items folder or when a user deletes an item by pressing **Shift + Delete**. When item is soft-deleted, it's moved to the Recoverable Items folder in the mailbox. At this point, the item can be recovered by the user until the deleted item retention period expires (in Office 365, the deleted item retention period is 14 days, but can be increased up to 30 days by an admin). After the retention period expires, the item is hard-deleted and moved to a hidden folder (called the *Purges* folder). The item will be permanently removed (purged) from Office 365 the next time the mailbox is processed (mailboxes are processed once every 7 days).
- **SharePoint Online and OneDrive for Business sites:** When a file or document is deleted, it is moved to the site's Recycle Bin (also called the *first-stage Recycle Bin* (which is like the Recycle Bin in Windows). The item will remain in the Recycle Bin for 93 days (the deleted item retention period for sites in Office 365). After that period, the item is automatically moved to Recycle Bin for the site collection, which also called the *second-stage Recycle Bin*. (Note that users or admins--with the appropriate permissions--can also delete items from the first-stage Recycle Bin). At this point, the item becomes soft-deleted; it can still be recovered by a site collection administrator in SharePoint Online or by the user or admin in OneDrive for Business). When an item is deleted from the second-stage Recycle Bin (either manually or automatically) it becomes hard-deleted and isn't accessible by user or an admin. Note that the retention period is 93 days for both the first-stage and second-stage recycle bins. That means the second-stage Recycle Bin retention starts when the item is first deleted; therefore, the total maximum retention time is 93 days for both recycle bins.

NOTE

Understanding the actions that result in an item being soft-deleted or hard-deleted will help you determine how to delete data in a way that meets GDPR requirements when responding to a deletion request.

- **Legal holds and retention policies** – In Office 365, a "hold" can be placed on mailboxes and sites; in short, this means that nothing will be permanently removed (hard-deleted) if a mailbox or site is on hold, until the retention period for an item expires or until the hold is removed. This is important in the context of deleting Customer Content in response to a DSR: if an item is hard-deleted from a content location that is on hold, the item is not permanently removed from Office 365. That means it could conceivably be recovered by an IT admin. If your organization has a requirement or policy that data be permanently deleted and unrecoverable in Office 365 in response to DSR, then a hold would have to be removed from a mailbox or site to permanently delete data in Office 365. More than likely, your organization's guidelines for responding to DSRs will have a process in place to determine whether a specific DSR deletion request or a legal hold takes precedence. If a hold is removed to delete items, it can be re-implemented after the item is deleted.

Deleting documents in SharePoint Online and OneDrive for Business

After you find the document located on a SharePoint Online site or in a OneDrive for Business account (by following the guidance in Discover section of this guide) that needs to be deleted, a data privacy officer or IT admin would need to be assigned the necessary permissions to access the site and delete the document. If appropriate, the document owner can also be instructed to delete the document.

Here's the high-level process for deleting documents from sites.

1. Go to the site and locate the document.
2. Delete the document. When you delete a document from a site, it's sent to the first-stage Recycle Bin.
3. Go to the first-stage Recycle Bin (the site Recycle Bin) and delete the same document you deleted in the previous step. The document is sent to the second-stage Recycle Bin. **At this point, the document is soft-deleted.**

4. Go to the second-stage Recycle Bin (which is the site collection Recycle Bin) and delete the same document that you deleted from the first-stage Recycle Bin. **At this point, the document is hard-deleted.**

IMPORTANT

You can't delete a document that is located on a site that is on hold (with one of the retention or legal hold features in Office 365). In the case where a DSR delete request takes precedence over a legal hold, the hold would have to be removed from the site before a document could be permanently deleted.

See the following topics for detailed procedures.

- [Delete a file, folder, or link from a SharePoint document library](#)
- [Delete items or empty the Recycle Bin of a SharePoint site](#)
- [Delete items from the site collection recycle bin](#)
- "Get access to the former employee's OneDrive for Business documents" section in [Get access to and back up a former user's data](#)
- [Delete files or folders in OneDrive for Business](#)
- [Delete a list in SharePoint](#)
- [Delete list items in SharePoint Online](#)

Deleting a SharePoint site

You may determine that the best way to respond to a DSR delete request is to delete an entire SharePoint site, which will delete all that data located in the site. You can do this by running cmdlets in SharePoint Online PowerShell.

- Use the [Remove-SPOSite](#) cmdlet to delete the site and move it to the SharePoint Online Recycle Bin (soft-delete).
- Use the [Remove-SPODeletedSite](#) cmdlet to permanently delete the site (hard-delete).

Note that you can't delete a site that is placed on an eDiscovery hold or is assigned to a retention policy. Sites must be removed from an eDiscovery hold or retention policy before you can delete it.

Deleting a OneDrive for Business site

Similarly, you may determine to delete a user's OneDrive for Business site in response to a DSR deletion request. If you delete the user's Office 365 account, their OneDrive for Business site is retained (and restorable) for 30 days. After 30 days, it's moved to the SharePoint Online Recycle Bin (soft-deleted), and then after 93 days, it's permanently deleted (hard-deleted). To accelerate this process, you can use the [Remove-SPOSite](#) cmdlet to move the OneDrive for Business site to the Recycle Bin and then use the [Remove-SPODeletedSite](#) cmdlet to permanently delete it. As with sites in SharePoint Online, you can't delete a user's OneDrive for Business site if it was assigned to an eDiscovery hold or a retention policy before the user's account was deleted.

Deleting OneDrive for Business and SharePoint Online Experience Settings

In addition to user-created files stored in OneDrive for Business accounts and SharePoint Online sites, these services store information about the user that is used to enable various experiences. These were previously documented in this document. See the [Additional considerations for select applications](#) section under [Using the Content Search eDiscovery tool to respond to DSRs](#), for information about how to access, view, and export OneDrive for Business and SharePoint Online application data.

Deleting a SharePoint user profile

The SharePoint user profile will be permanently deleted 30 days after the user account is deleted in Azure Active

Directory. However, you can hard-delete the user account, which will remove the SharePoint user profile. For more information, see the [Deleting a user section in this guide](#).

An admin can expedite the deletion of the User Profile for a user by using the **Remove-SPOUserProfile** cmdlet in SharePoint Online PowerShell. See [Remove-SPOUserProfile](#). This requires the user to be at least soft-deleted in Azure Active Directory.

Deleting User Information lists on SharePoint Online sites

For users that have left the organization, this data remains in the sites they interacted with for referential integrity of SharePoint column fields. An admin can delete all User information properties for a user on a given site by using the **Remove-SPOUserInfo** command in SharePoint Online PowerShell. See [Remove-SPOUserInfo](#) for information about running this PowerShell cmdlet.

By default, this command will retain the display name of the user and delete properties such as telephone number, email address, skills and expertise, or other properties that were copied from the SharePoint Online user profile. An admin can use the **RedactUser** parameter to specify an alternate display name for the user in the User Information list. This will affect several parts of the user experience and will result in information loss when looking at the history of files in the site.

Finally, the redaction capability will not remove all metadata or content referencing a user from documents. The way to achieve redaction of file content and metadata is described in the [Making changes to content in OneDrive for Business and SharePoint Online](#) section in this guide. This method consists of downloading, deleting, and then uploading a redacted copy of the file.

Deleting OneDrive for Business experience settings

The recommended way to delete all OneDrive for Business experience settings and information is to remove the user's OneDrive for Business site, after reassigning any retained files to other users. An admin can delete these lists using [PowerShell Script](#) and [SharePoint Client-Side Object Model \(CSOM\)](#) commands. See [Deleting OneDrive for Business experience settings](#) for more information about the settings, how they are stored, and how to delete them.

OneDrive for Business and SharePoint Online search queries

A user's search queries created in the OneDrive for Business and SharePoint Online search experience are automatically deleted 30 days after the user creates the query.

Deleting items in Exchange Online mailboxes

You may have to delete items in Exchange Online mailboxes to satisfy a DSR delete request. There are two ways that an IT admin can delete items in mailbox, depending on whether to soft-delete or hard-delete the target items. Like documents on SharePoint Online or OneDrive for Business sites, items in a mailbox that is on hold can't be permanently deleted from Office 365. The hold must be removed before the item can be deleted. Again, you'll have to determine whether the hold on the mailbox or the DSR delete request takes precedence.

Soft-delete mailbox items

You can use the Content Search Action functionality to soft-delete items that are return by a Content Search. As previously explained, soft-deleted items is moved to the Recoverable Items folder in the mailbox.

Here's a quick overview of this process:

1. Create and run a Content Search to find the items that you want to delete from the user mailbox. You may have to re-run the search to narrow that search results so that only the items that you want to delete are returned in the search results.
2. Use the **New-ComplianceSearchAction -Purge** command in Office 365 PowerShell to soft-delete the item that are returned by the Content Search that was created in the previous step.

For detailed instructions, see [Search for and delete email messages in your Office 365 organization](#).

Hard-delete mailbox items

If you have to hard-delete mailbox items in response to the DSR deletion request, you can use the **Search-**

Mailbox -DeleteContent command in Exchange Online PowerShell. If you use this method, consider using Content Search to develop and refine a search query so that only the items that are to be deleted are returned in the search. Then you can use that query syntax when you run the **Search-Mailbox -DeleteContent** command.

For detailed instructions, see [Search for and delete messages](#).

Hard-delete items in a mailbox on hold

As previously explained, if you hard-delete items in a mailbox on hold, items are not removed from the mailbox. They are moved to a hidden folder in the Recoverable Items folder (the **Purges** folder) and will remain there until the hold duration for the item expires or until the hold is removed from the mailbox. If either of those things happen, the items will be purged from Office 365 the next time that the mailbox is processed.

Your organization might determine that items being permanently deleted when the hold duration expires meets the requirements for a DSR deletion request. However, if you determine that mailbox items must be immediately purged from Office 365, you would have to remove the hold from the mailbox and then hard-delete the items from the mailbox. For detailed instructions, see [Delete items in the Recoverable Items folder of cloud-based mailboxes on hold](#).

NOTE

To hard-delete mailbox items to satisfy a DSR deletion request by following the procedure in the previous topic, you may have to soft-delete those items while the mailbox is still on hold so that they are moved to the Recoverable Items folder.

Deleting a user

In addition to deleting personal data in response to a DSR deletion request, a data subject's "right to be forgotten" may also be fulfilled by deleting their Office 365 user account. Here are some reasons that you might want to delete a user:

- The data subject has left (or is in the process of leaving) your organization.
- The data subject has requested that you delete system-generated logs that have been collected about them. Examples of data in system-generated logs include Office 365 app and service usage data, information about search requests performed by the data subject, and data generated by product and services as a product of system functionality and interaction by users or other systems. For more information, see [Part 3: Responding to DSRs for system-generated Logs](#) in this guide.
- Permanently prevent the data subject from accessing or processing data in Office 365 (as opposed to temporarily restriction access by the methods described in the section [Responding to DSR restriction requests](#)).

After you delete an Office 365 user account:

- The user can no longer sign-in to Office 365 or access any of your organization's Office 365 resources, such as their OneDrive for Business account, SharePoint Online sites, or their Exchange Online mailbox.
- Personal data, such as email address, alias, phone number, and mailing address, that's associated with the user account is deleted
- Some Office 365 apps will remove information about the user. For example, in Microsoft Flow, the deleted user will be removed from the list of owners for a shared flow.
- System-generated logs about the data subject will be deleted 30 days after the user account is deleted. For more information, see the section [Deleting system-generated logs](#).

IMPORTANT

After you delete a user account, that person will lose the ability to sign in to Office 365 and the ability to sign in to any products or services for which he or she formerly relied upon for a work or school account. That person would also be unable to initiate any DSR requests through Microsoft directly in instances where Microsoft is the data controller. For more information, see the [Product and services authenticated with an Org ID for which Microsoft is a data controller](#) section in Part 4 of this guide.

NOTE

In the event that you are a customer currently engaged in FastTrack migrations, deleting the Office 365 user account will not delete the data copy held by the Microsoft FastTrack team, which is held for the sole purpose of completing the migration. If, during the migration, you would like the Microsoft FastTrack team to also delete the data copy, you can [submit a request](#). In the ordinary course of business, Microsoft FastTrack will delete all data copies once the migration is complete.

Like the soft-deletion and hard-deletion of data that was described in the previous section on deleting personal data, when you delete a user account, there is also a soft-deleted and hard-deleted state.

- When you initially delete a user account (by deleting the user in the Office 365 admin center or in the Azure portal), the user account is soft-deleted, and moved the Recycle Bin in Azure for up to 30 days. At this point, the user account can be restored.
- If you permanently deleted the user account, the user account is hard-deleted and removed from the Recycle Bin in Azure. At this point, the user account can't be restored, and any data associated with the user account will be permanently removed from the Microsoft cloud. System-generated logs about the data subject will be deleted after the user account is hard-deleted.

Here's the high-level process for deleting a user from your Office 365 organization.

1. Go to the Office 365 admin center or the Azure portal and locate the user.
2. Delete the user. When you initially delete the user, the user's account is sent to the Recycle Bin. At this point, the user is soft-deleted. The account is retained in the soft-deleted for 30 days, which allows you to restore the account. After 30 days, the account is automatically hard-deleted. For specific instructions, see [Delete users from Azure AD](#).
3. You can also soft-delete a user account in the Office 365 admin center. See [Delete a user from your organization](#).
3. If you don't want to wait for 30-days for the user account to be hard-deleted, you can manually hard-delete it. To do this in the Azure portal, go to the Recently deleted users list and permanently delete the user. At this point the user is hard-deleted. For instructions, see [How to permanently delete a recently deleted user](#).

You can't hard-delete a user in the Office 365 admin portal.

NOTE

In Office 365 operated by 21Vianet (China), you can't permanently delete a user as previously described. To permanently delete a user, you can submit a request via the Office 365 admin portal at this [URL](#). Go to **Commerce** and then select **Subscription -> Privacy -> GDPR** and enter the required information.

Removing Exchange Online data

One thing to understand when deleting a user is what happens to the user's Exchange Online mailbox. After the user account is hard-deleted (in step 3 in the previously process) the deleted user's mailbox isn't automatically purged from Office 365. It will take up to 60 days after the user account is hard-deleted to permanently remove it

from Office 365. Here's the mailbox lifecycle after the user account is deleted and a description of the state of the mailbox data during that time:

- **Day 1 – Day 30:** The mailbox can be fully restored by restoring the soft-deleted user account.
- **Day 31 – Day 60:** For 30 days after the user account is hard-deleted, an admin in your organization can recover the data in the mailbox and import it into a different mailbox. This provides Office 365 organizations the ability to recover the mailbox data if necessary.
- **Day 61 – Day 90:** An admin can no longer recover the data in the mailbox. The mailbox data will be marked for permanent removal, and it will take up to 30 more days for the mailbox data to be purged from Office 365.

If you determine that this mailbox lifecycle doesn't meet your organization's requirements for responding to a DSR deletion request, you can [contact Microsoft Support](#) after you hard-delete the user account, and request Microsoft to manually initiate the process to permanently remove the mailbox data. Note that this process to permanently remove mailbox data starts automatically after day 61 in the lifecycle, so there would be no reason to contact Microsoft after this point in the lifecycle.

Using In-App functionality to respond to DSRs

While most Customer Data is authored and produced using the applications described in the previous section, Office 365 also offers many other applications that customers can use to produce and store Customer Data. However, Content Search doesn't currently have the ability to find data authored in these other Office 365 applications. To find data generated by these applications, you or the data owner must use in-product functionality or features to find data that may be relevant to a DSR. The following table lists these Office 365 applications. Click the application icon to go the section in this guide that describes how to respond to DSR requests for data authored in the application.

Table 3: Applications where in-app functionality can be used to find Customer Data

 Access	 Business Apps for Office 365	 Education
 Flow	 Forms	 Kaizala
 Planner	 PowerApps	 Power BI
 Project Online	 Publisher	 StaffHub
 Stream	 Sway	 Whiteboard
	 Yammer	

Access

The following sections explain how to use the in-app functionality in Microsoft Access to find, access, export, and delete personal data.

Discover

There are several ways that you can search for records in an Access database that might be responsive to a DSR request. For a DSR investigation, you can search for records that relate to the data subject or search for records that contain specific data. For example, you could either search or go to a record that corresponds to the data subject. Or you can search for records that contain specific data, such as personal data about the data subject. For more information, see:

- [Find records in an Access database](#)
- [Create a simple select query](#)

Access

After you find the records or fields that are relevant to the DSR request, you can take a screenshot of the data or export it to an Excel file, Word file, or a text file. You can also create and print a report based on a record source, or a select query that you created to find the data. See:

- [Introduction to reports in Access](#)
- [Export data to Excel](#)
- [Export data to a Word document](#)
- [Export data to a text file](#)

Export

As previously explained, you can export data from an Access database to different file formats. The file format that you choose to export to might be determined by the specific DSR export request from a data subject. See [Import and export](#) for a list of topics that describe how to export Access data in different file formats.

Delete

You can delete an entire record or just a field from an Access database. The quickest way to delete a record from an Access database is to open the table in Datasheet view, select the record (row) or just the data in a field that you want to delete, and then press Delete. You can also use a select query that you created to find data and then convert it to a delete query. See:

- [Delete one or more records from a database](#)
- [Create and run a delete query](#)

Business Apps for Office 365

This section explains how to use the in-app functionality in each of the following Business Apps for Office 365 to respond to DSR requests.

- [Bookings](#)
- [Listings](#)
- [Connections](#)
- [Outlook Customer Manager](#)
- [Invoicing](#)

Bookings

The following sections explain how to use the in-app functionality in Microsoft Bookings to find, access, export, and delete personal data. This applies to both the standalone Bookings app and to Bookings when accessed through the Business center.

Microsoft Bookings allows administrators and users or staff, with a Bookings license in their organization, to set up

booking pages so customers can schedule and make changes to appointments, receive confirmation emails, updates, cancellation, and reminders email. Business owners and their staff can also book events on behalf of their customers with Bookings.

The following types of data is created by customers, administrators, or staff:

- **Contact information of customers, partners and friends.** This data contains name, phone number, email address, address, and notes.
 - Contacts for anyone can be manually created by using the Bookings Web, iOS, and Android clients.
 - Contacts for anyone can be imported from a C1's mobile device into Bookings with the Bookings iOS and Android clients.
 - Contacts are also auto-created at the time of booking creation through the booking workflow for anyone booked – whether the booking is created by a user on a customer's behalf or if it's created by the customer using the owner's booking page.
- **Booking events.** These are meetings between the business owner or their designated staff and a customer, which are created either by the business owner or the customer through the business owner's public booking page. This data includes name, address, email address, phone number, and any other info the business owner collects from the customer at the time of booking.
- **Email confirmations/cancellations/updates.** These are email messages generated and sent by the system in association with specific booking events. They contain personal data about the staff who is scheduled to the deliver the relevant service and they contain personal data about the customer that was entered by either the business owner or the customer at the time of booking.

All customer content is stored in the Exchange Online mailbox that hosts the organization's Bookings. This content is retained for as long as the business owner and customer are active in the service, unless they explicitly request that the data be deleted or if they leave the service. This content can be deleted with in-product UI, with a cmdlet, or through deletion of the relevant booking mailbox. Once the deleted action is initiated, the data will be deleted within the time period set by the business owner.

If a customer decides to leave the service, their customer contents is deleted after 90 days. For more details about when mailbox content is deleted after a user accounts in deleted, see [Removing Exchange Online data](#).

End User Identifiable Information

End user Identifiable Information (EUII) includes personal and contact information about the staff that gets scheduled in Bookings. It's added to the Staff details pages when the business owner sets up Bookings and makes updates after the setup. It contains staff member's name, initials, email address, and phone number. This data is stored in the Exchange Online mailbox that hosts Bookings.

This data is retained for as long as the staff member is active in the service unless it's explicitly deleted the business owner or an admin using the in-app UI or by deleting the relevant booking mailbox. When the admin initiates the deletion of staff's details, or if the staff member leaves the service, their details are deleted in accordance with the Exchange Online mailbox's content retention policies set by the business owner or admin.

Discover/Access

Bookings gathers and stores the following types of data:

- Business profile information. Customer content about the business using Bookings is collected through the Bookings' Business information form and is synchronized with the Business Center Business Profile if a customer is using Bookings in conjunction with the Business center.
- The only EUII associated with this data is an email address the C1. This address is where new booking notifications and update emails are sent.
- Customer contacts. Contacts can be manually created in the Bookings Web, iOS, and Android clients, or they can be imported from a mobile device. Contacts are also automatically created during the use of the self-service booking page. They contain EUII and are stored in the Bookings mailbox.
- Staff details. Customer content includes data about the staff that are eligible to deliver the services created from

either the Bookings Web, iOS, or Android clients. Staff details can contain name, email address, and phone number.

- Booking events. These are customer meetings and related customer content created by the business using a Web client or Android/iOS app, or created by the customer using a public booking page (or a Facebook page). These events can include name, address, email address, phone number, and appointment details.

Meeting requests, email confirmations/cancellations/updates, and email reminders. These are email messages sent by the system in association with bookings. They contain staff data and customer data that was entered at time of booking.

Export

To export data corresponding to the business owner, staff and customers, you can use the Business center privacy portal. See [Export or delete user data using Business center privacy portal](#).

Delete

You can delete the following types of Bookings data in response to a DSR deleting request:

- **Business profile information and contacts.** You can delete the Bookings mailbox in the Office 365 admin center. After you delete the mailbox, you can restore it with 30 days. After 30 days, the account and the corresponding mailbox are permanently deleted. For details about deleting a user account, see the section [Deleting a user](#).
- **Staff details.** You can delete staff from the Bookings dashboard. To permanently detail staff, you can delete their Office 365 account.
- **Bookings events.** You can delete bookings events from the Bookings calendar, which will remove the customer's information.
- **Meeting requests, email confirmations/cancellations/updates, and email reminders.** You can delete these from the Bookings calendar, which will remove the customer's information.

Business owners and admins can also delete their customer's data by using the Business center privacy portal. See [Export or delete user data using Business center privacy portal](#).

Additionally, you can delete business owner and staff data, you can delete the corresponding Office 365 user account. See the section [Deleting a user](#).

Listings

The following sections explain how use the in-app functionality in Microsoft Listings to find, access, export, and delete personal data.

Discover

Listings owner can connect their business to Google, Bing, Yelp, and Facebook to see an aggregated view of ratings and reviews. Listings collects and stores the following types of data:

- Google reviews and ratings
- Bing reviews and ratings
- Yelp reviews and ratings
- Facebook reviews and ratings

Access

Listings owner can sign in to the Listings dashboard to see their reviews and ratings.

Export

To export business owner, staff and customer data, use the Business center privacy portal. See [Export or delete user data using Business center privacy portal](#).

Delete

If a Listings owner would like to delete their Listings information, they can disconnect from the provider on the Listings page. After they disconnect, their Listings information will be deleted.

Connections

The following sections explain how use the in-app functionality in Microsoft Connections to find, access, export, and delete personal data.

Discover

Connections collects and stores the following types of data:

- Customers/contacts are created by the business using the web client or mobile app (iOS, Android), or by using the app when a business contact is sent an email marketing campaign. Customer data can include name, address, email address, and tax ID numbers. Note that contacts are shared across all Business center apps.
- Customers can sign up on the Connections sign up page and save their personal information.
- Links from email campaigns

Access

A Connections owner can sign in to the Connections dashboard and see the email campaigns they've sent.

Export

To export business owner, staff and customer data, use the Business center privacy portal. See [Export or delete user data using Business center privacy portal](#).

Delete

After a Connections owner sends an email campaign, they can't delete the campaign. If there are any draft campaigns they want to delete, they can sign in to the Connections dashboard and delete the draft campaigns.

Outlook Customer Manager

The following sections explain how use the in-app functionality in Outlook Customer Manager to find, access, export, and delete personal data.

Discover

Outlook Customer Manager gathers and stores user information for both the Outlook Customer Manager owner and their customers and business contacts.

- Owner data. This includes name, address, and email address. Documents and files that an owner shares with a customer are stored in OneDrive for Business, SharePoint Online, and as tasks in Outlook.
- Customer and business contact data. Customer data can include name, address, and email address. Customer and contact data is created by the business in Outlook or Outlook web app. Contacts are shared across Business center. Documents and files that a customer shares with a business are stored in OneDrive for Business, SharePoint Online, and as tasks in Outlook.

Outlook Customer Manager also stores activities and insights about customers in Exchange.

Access

Outlook Customer Manager owners can sign in to Outlook or Outlook web app, and then go to the Outlook Customer Manager dashboard to see the interactions they've had with their customers.

Export

To export business owner and customer data, use the Outlook Customer Manager privacy portal. For details. See [Export or delete user data using the Outlook Customer Manager privacy portal](#).

Delete

To delete customer data, use the Outlook Customer Manager privacy portal. See [Export or delete user data using the Outlook Customer Manager privacy portal](#).

Invoicing

The following sections explain how use the in-app functionality in Microsoft Invoicing to find, access, export, and delete personal data.

Discover

Invoicing collects and stores the following types of data:

- **Contacts.** These are created by the business when an invoice or estimate is created for a customer/business contact. Contacts are shared across Business center. Customer data includes name, address, email address, and

tax ID numbers.

- **Invoices.** These are created and sent to customers and represent both a debt and a tax liability.
- **Estimates.** The business can also send estimates to customers. If a customer accepts an estimate, it is converted to an invoice. An estimate is converted to an invoice after it's accepted by the customer. Records of estimates aren't kept once they're converted to an invoice.

Access

Users can go to the Invoicing dashboard in the Business center to see drafts of the invoices they've created and the invoices that have been seen to customers.

Export

To export customer invoicing data, use the Business center privacy portal. See [Export or delete user data using Business center privacy portal](#).

Delete

After an invoice is created and sent, it can't be deleted due to accounting laws. The Invoicing owner can request that Microsoft delete some or all their information from Office 365.

Alternatively, you can delete the invoicing owner's user account in Office 365. See the section [Deleting a user](#).

Education

This section explains how to use the in-app functionality of the following Microsoft Education apps to respond to DSR requests.

- Assignments
- Class Notebook

Assignments

The following sections explain how to use the in-app functionality in Assignments to find, access, export, and delete personal data.

Discover/Access

Assignments stores information that is generated both by teachers and students. Some of this information is stored in SharePoint and some is stored in a non-SharePoint location.

Finding Assignments data stored in SharePoint

Students' files associated with a Submission for Assignment are stored in a document library (named **Student Work**) and files associated with Assignments that are created by teachers and (accessible by students) are stored in a different document library (named **Class Files**). Both document libraries are in the corresponding Class Team SharePoint site.

An admin can use the Content Search tool in the Office 365 Security & Compliance Center to search for student files (in the Student Work and Class Files libraries) that are related to submissions on assignments as well as files related to assignments. For example, an admin could search all SharePoint sites in the organization and use the student's name and class or assignment name in the search query to find data relevant to a DSR request.

Similarly, an admin can search for teacher files related to assignments for files that a teacher distributed to students. For example, an admin could search all SharePoint sites in the organization and use the teacher's name and class or assignment name in the search query to find data relevant to a DSR request.

See [Using the Content Search eDiscovery tool to respond to DSRs](#) section in this guide.

Finding Assignments data not stored in SharePoint

The following types of Assignments data is not stored in the class team SharePoint site, and therefore isn't discoverable by using Content Search. This data includes the following:

- Student grades and feedback from the teacher
- The list of documents submitted for an assignment by each student
- Assignment details, like the date the assignment is due

To find data, an admin or a teacher would have to go into the Assignment in the Class Team site to find data that may be relevant to a DSR request. An admin can add themselves as an owner to the class and view all the assignments for that class team.

Note that even if a student is no longer part of a class, their data might still be present in the class and marked as "no longer enrolled". In this case, a student submitting a DSR request would have to provide the admin the list of classes that they were formally enrolled in.

Export

You can export Assignments data for a specific student for all classes in which the student is currently enrolled by using a PowerShell script. See:

- [Using scripts to export and delete user data from Assignments.](#)
- [Export student and teacher data from Assignments.](#)

If the student has been removed from the Team Class site, the admin can add the student back to the site before running the export script. Or the admin can use the input file for the script to identify every class that the student was ever enrolled in. You can also use the Assignment export script to export submissions data for all assignments that a teacher has access to.

Delete

You can delete Assignments data for a specific student for all classes in which the student is currently enrolled by using a PowerShell script. You should do this before you remove the student from the class. See:

- [Using scripts to export and delete user data from Assignments.](#)
- [Delete student data from Assignments.](#)

If the student has been removed from the Team Class site, the admin can add the student back to the site before running the export script. Or the admin can use the input file for the script to identify every class that the student was ever enrolled in. You can't use the Assignments deletion script to delete teacher data because all Assignments are shared across the Class Team site. As an alternative, an admin would have to add themselves to the Class Team site and then delete a specific Assignment.

Class Notebook Searching for content in Class Notebook is discussed previously in this guide. See the [OneNote Class Notebook](#) section. You can also use the Content Search tool to export data from a Class Notebook.

Alternatively, an admin or the data subject can export data from a Class Notebook. See [Save a copy of a Class Notebook](#).

Flow

The following sections explain how to use the in-app functionality in Microsoft Flow to find, access, export, and delete personal data.

Discover

People can use Flow to perform data-related tasks such as synchronizing files between applications, copying files from one Office 365 service to another, and collecting data from one Office 365 app and storing it in another. For example, a user could set up a Flow to save Outlook email attachments to their OneDrive for Business account. In this example, you could use the Content Search tool to search the user's mailbox for the email message that contained the attachment or search their OneDrive for Business account for the file. This is an example where data handled by Flow might be discoverable in the Office 365 services connected by a Flow workflow.

Additionally, people can use Flow to copy or upload files from Office 365 to an external service, such as Dropbox. In these cases, a DSR request concerning the data in an external service would have to be submitted to the external service, who is processing the data in this type of scenario.

If an admin receives a DSR request, they can add themselves as an owner of a user's flows. This enables an admin to perform functions including exporting flow definitions, run histories and performing flow permission re-assignments. See [Manage Flows in the Admin Center](#).

An admin's ability to add themselves as an owner of a Flow requires an account with the following permissions:

- Flow/PowerApps Plan 2 license (paid or trial)
- [Office 365 global administrator](#)
or
- [Azure Active Directory global administrator](#)

Having these privileges enables the admin to use the Flow admin center to access all Flows in the organization.

To add yourself as an owner of a flow.

1. Go to <https://admin.flow.microsoft.com>
2. Sign in with your Office 365 credentials.
3. On the **Environments** page, click the environment for the flows that you want to access. Note that Office 365 organizations have a default environment.
4. On the page for the environment that you selected, click **Resources**, and then click **Flows**. A list of all flows in the environment is displayed.
5. Click **View details** for the flow that you want to add yourself as a member.
6. Under **Owners**, click **Manage sharing**.
7. On the **Share** flyout, add yourself as a member and then save the change.

After you make yourself an owner, go to **Flow > My flows > Team flows** to access the flow. From there you can download the run history or export the flow. See:

- [Download flow run history](#)
- [Export and import your flows across environments with packaging](#)

Access

A user can access the definitions and run histories of their flows.

- **Flow definitions** - A user can export the definition of a flow (which is exported as a Flow package, formatted as JSON in a zipped file). See [Export and import your flows across environments with packaging](#).
- **Flow run histories** - A user can download the run history of each of their flows. A flow run history is downloaded as a CSV file, which can be opened in Excel to filter or search. Users can also download the run history of multiple flows. See [Download flow run history](#).

Delete

An admin can add themselves as an owner of a user's flows in the Flow admin center. If a user leaves your organization and their Office 365 account is deleted, the flows that they are the sole owner of will be retained. This is to help your organization transition the flows to new owners and avoid any disruption to your business for flows that may be used for shared business processes. An admin then needs to determine whether to delete the flows that were owned by the user or simply re-assign to new owners, and take that action.

For shared flows, when a user is deleted from your organization, their name is removed from the list of owners.

Export

An admin can export the definition and run history of a user's flows. To do this, an admin must add themselves as an owner of the user's flow in the Flow admin center

- **Flow definitions** - After an admin adds themselves as an owner of a flow, they can go to **Flow > My Flows > Teams flows** to export the flow definition (which is exported as a Flow package, formatted as JSON in a

zipped file). See [Export and import your flows across environments with packaging](#).

- **Flow run histories** - Similarly, an admin must add themselves as an owner of a Flow to export its flow run history. The Flow run history is downloaded as a CSV file, which means you can use Excel to filter or search. You can also download the run history of multiple Flows, as long as you have ownership. See [Download flow run history](#).

Connections and custom connectors in Flow

Connections require users to provide credentials to connect to APIs, SaaS applications and custom developed systems. These connections are owned by the user that established the connection and can be [managed](#) in-product. After Flows have been re-assigned, an admin can use PowerShell cmdlets to list and delete these connections as part of deleting user data.

Custom connectors allow organizations to extend the capabilities of Flow by connecting to systems where an out-of-box connector is not available. A custom connector author can [share](#) their connector with others in an organization. After receiving a DSR deleting request, an admin should consider re-assigning ownership of these connectors to avoid business disruption. To expedite this process, an admin can use PowerShell cmdlets to list, re-assign or delete custom connectors.

Forms

The following sections explain how use the in-app functionality in Microsoft Forms to find, access, export, and delete personal data.

Discover

Forms users can go to <https://forms.office.com> and select **My forms** to see the Forms they've created. They can also select **Shared with me** to view Forms others have shared via a link. If there are many Forms to sort through, users can use the in-product search bar to search for Forms by title or author. To determine whether Microsoft Forms is a place where personal data responsive to your DSR is likely to reside, you can ask the Data Subject to search his or her **Shared with me** list to determine which users ("Forms owners") have sent Forms to the Data Subject. You can then ask the forms owners to select **Share** in the top navigation bar and send you a link to a specific form so you can view it and further determine whether it is material to your DSR.

Access

After the relevant Forms are found, you can access the responses to the Form by clicking on the **Responses** tab. Learn more about how to [check your quiz results](#) or [form results](#). To review response results in Excel, select the **Responses** tab, and then click **Open in Excel**. If you would like to send the Data Subject a copy of the Form, you can either take screenshots of the relevant questions and answers that are shown in the application in rich text format or send the Data Subject an Excel copy of the results. If you are using Excel and would like to share with the Data Subject only portions of the survey result, you can delete certain rows or columns or redact the remaining sections before sharing the results. Alternatively, you can go to **Share > Get a link to duplicate** (under Share as a template) to provide the Data Subject with a replicate of the entire Form.

Delete

Any survey, quiz, questionnaire, or poll can be permanently deleted by its owner. If you would like to honor a DSR "forget me" and delete a form in its entirety, find the Form in the list of forms, select the series of dots (ellipsis) in the upper right corner of the form preview window, and then click **Delete**. Once a Form is deleted, it can't be retrieved. For information, see [Delete a Form](#).

Export

To export form questions and responses to an Excel file, open the form, select the **Responses** tab, and then select **Open in Excel**.

Kaizala

The following sections explain how use the in-app functionality in Microsoft Kaizala to find, access, export, and delete personal data.

Discover

A user's organizational data, which is data that is shared in organizational groups, can be accessed by an admin from the Kaizala management portal. Organizational data is retained for a duration of time determined by your organization's retention policies. In addition to user data, Kaizala servers also store the following types of organizational data:

- List of members who are part of the organization's groups
- Organization group messages data, which are messages and responses shared across organizational groups
- A list of users in the organizations
- Product and service usage data captured for all users in the organization.
- Kaizala Actions created by the organization
- Kaizala connectors data

A user's consumer data can be accessed by the data subject using the Kaizala mobile app for consumer data. Consumer data includes the following types of data:

- Data belonging to private groups on Kaizala (stored on Kaizala servers for 90 days)
- A user's profile information, as well as the user's contacts
- List of members who are part of the same groups as the user
- Group messages and responses shared across groups
- The user's contact list (stored on Kaizala service)
- Transactions made by the user on Kaizala (applies to Kaizala users in India only)
- Product and service usage data for the user

Access

Kaizala users can go to their mobile device to see Kaizala content they've created on their device. To determine whether Kaizala mobile apps is a place where personal data responsive to a DSR is likely to reside, you can ask the data subject to search their Kaizala app for the requested information.

Export

When users in your organization use Kaizala, consumer data is generated, and organizational data may be generated if the user participates in an organization group. Admins can export a user's organizational data from the Kaizala management portal. Kaizala consumer users can export their private data from the Kaizala mobile app. In both cases, note that product and service usage data is also export when an admin or user exports Kaizala data. For details, see:

- [Export or delete a user's organizational data in Kaizala](#)
- [Export or delete your data in the Kaizala mobile app](#)

Delete

A Kaizala admin can remove a Kaizala user's account in the Kaizala management portal. After a user account is deleted, the user is removed from all groups that belong to your organization and organizational data is deleted from their device.

To remove all private data from the user's mobile device, the Kaizala user can delete their Kaizala account. After the account is deleted, all related Kaizala content including, chats, photos, and other data will be deleted from the device.

For details, see:

- [Export or delete a user's organizational data in Kaizala](#)
- [Export or delete your data in the Kaizala mobile app](#)

Planner

The following sections explain how use the in-app functionality in Microsoft Planner to find, access, export, and delete personal data.

Discover

Planner plans are associated with an Office 365 Group, and the files for Office 365 Groups are stored in an associated SharePoint Online site for the group. That means that you can use Content Search to find Planner files by searching the site for the Office 365 Group. To do this, you'll need to have the URL for the Office 365 Group. See [Searching Microsoft Teams and Office 365 Groups](#) in the "Content Search in Office 365" help topic for tips about getting information about Office 365 Groups to help you search for Planner files in the corresponding SharePoint Online site.

Access

As previously explained, you can search the underlying SharePoint Online site and mailbox that are associated with a plan. Then you can preview or download the related search results to access data.

Delete

You can manually delete a user's personally information by either giving yourself permissions to access the plans the user is part of or signing in as the user to make the changes. See [Delete user data in Microsoft Planner](#).

Export

You can use a PowerShell script to export a user's data from Planner. When you export the data, a separate JSON file is export for each plan that the user is a part of. See [Export user data from Microsoft Planner](#).

Power BI

The following sections explain how use the in-app functionality in Microsoft Power BI to find, access, export, and delete personal data.

Discover

You can search for content in the different workspaces in Power BI, including dashboards, reports, workbooks, and datasets. Each type of workspace contains a search field that you can use to search that workspace. See [Searching, finding, and sorting content in Power BI service](#).

Access

You can print dashboards, reports, and visuals from reports in Power BI to produce a physical copy. Note that you can't print entire reports; you can only print one page at a time. To do this, go to a report, use the search field to find specific data, and then print that page. See [Printing from Power BI service](#).

Delete

To delete dashboards, reports, and workbooks, see [Delete almost anything in Power BI service](#).

Deleting a dashboard, report, or workbook doesn't delete the underlying dataset. Because Power BI relies on a live connection to the underlying source data to be complete and accurate, deleting personal data must be done there. (For example, if you created a Power BI report that is connected to Dynamics 365 for Sales as the live data source, you would have to make any corrections to the data in Dynamics 365 for Sales.)

After the data is deleted, you can use the [scheduled data refresh](#) capabilities in Power BI to update the dataset that is stored in Power BI, after which the deleted data will no longer be reflected in any Power BI reports or dashboards that leveraged that data. To help comply with GDPR requirements, you should have policies in place to ensure that you are refreshing your data at an appropriate cadence.

Export

To facilitate a data portability request, you can export dashboards and reports in Power BI:

- You can export the underlying data for dashboards and reports to a static Excel file. See the video in [Printing from Power BI service](#). Using Excel, you can then edit the personal data to be included in the portability request, and save it in a commonly used, machine-readable format such as .csv or .xml.
- You can export (download) a report from the Power BI service in Office 365 to a .pbix file if it was originally published using Power BI Desktop. You can then import this file to Power BI Desktop and publish (export) it to the Power BI service of another organization. See [Export a report from Power BI service to Desktop](#).

PowerApps

The following sections explain how to use the in-app functionality in Microsoft Power Apps to find, access, export, and delete personal data. These steps outline how an admin can transition apps and their dependent resources to new owners to limit business disruption.

Discover

PowerApps is a service for building apps that can be shared and used within your organization. As a part of the process of building or running an app, a user will end up storing several types of resources and data in the PowerApps service, including apps, environments, connections, custom connectors, and permissions.

To help facilitate a DSR request related to PowerApps, you can leverage the administration operations exposed in the [PowerApps Admin Center](#) and [PowerApps Admin PowerShell cmdlets](#). Access to these tools will require an account with the following permissions:

- A paid PowerApps Plan 2 license or a PowerApps Plan 2 trial license. You can sign-up for a 30 day trial license [here](#).
- [Office 365 global administrator](#)
or
● [Azure Active Directory global administrator](#)

For more information about finding personal data, see [Discover PowerApps personal data](#).

The PowerApps service also includes the Common Data Service For Apps, which enables users to store data in standard and custom entities within a Common Data Service database. You can view the data stored in these entities from the [PowerApps Maker portal](#), and use the in-product search capabilities of [Advanced Find](#) to search for specific data in the entity. For more details around discovering personal data in the Common Data Service, see [Discover Common Data Service personal data](#).

Access

Admins have the ability to assign themselves privileges to access and run the apps and associated resources (including flows, connections, and custom connectors) using the [PowerApps Admin Center](#) or [PowerApps Admin PowerShell cmdlets](#).

After you have access to the user's app, you can use a web browser to open the app. After you open an app, you can take a screenshot of the data. See [Use PowerApps in a web browser](#).

Delete

Because PowerApps allows users to build line-of-business application that can be a critical part of your organization's day-to-day operations, when a user leaves your organization and their Office 365 account is deleted, the admin will need to determine whether to delete the apps owned by the user or simply re-assign to new owners. This is to help your organization transition apps to new owners and avoid any disruption to your business for apps that may be used for shared business processes.

For shared data, like apps, admins must decide whether or not they want to permanently delete that user's shared data or keep them by re-assigning the data to themselves or someone else within their organization. See [Delete PowerApps personal data](#).

Any data that was stored by a user in an entity in a Common Data Service For Apps database will also need to be reviewed and (if desired) deleted by an admin using the in-product capabilities. See [Delete Common Data Service user personal data](#).

Export

Admins have the ability to export personal data stored for a user within the PowerApps service using the [PowerApps Admin Center](#) and [PowerApps Admin PowerShell cmdlets](#). See [Export PowerApps personal data](#).

You can also use the in-product search capabilities of [Advanced Find](#) to search for a user's personal data in any

entity. For details about exporting personal data in the Common Data Service, see [Export Common Data Service personal data](#).

Connections and custom connectors in PowerApps

Connections require users to provide credentials to connect to APIs, SaaS applications and custom developed systems. These connections are owned by the user that established the connection and can be [managed](#) in-product. After PowerApps have been re-assigned, an admin can use PowerShell cmdlets to list and delete these connections as part of deleting user data.

Custom connectors allow organizations to extend the capabilities of PowerApps by connecting to systems where an out-of-box connector is not available. A custom connector author can [share](#) their connector with others in an organization. After receiving a DSR deleting request, an admin should consider re-assigning ownership of these connectors to avoid business disruption. To expedite this process, an admin can use PowerShell cmdlets to list, re-assign or delete custom connectors.

Project Online

The following sections explain how use the in-app functionality in Microsoft Project Online to find, access, export, and delete personal data.

Discover and access

You can use Content Search to search the SharePoint Online site that's associated with a Project (when a Project is first created, there's an option to create an associated SharePoint Online site); Content Search doesn't search the data in an actual project in Project Online, only the associated site. Though Content Search will search for metadata about projects such as people mentioned in the subject) However, this may help you find (and access) the Project that contains the data related to the DSR.

TIP

The URL for the site collection in your organization where sites associated with Projects is <https://<your org>.sharepoint.com/sites/pwa>; for example, <https://contoso.sharepoint.com/pwa>. You can use this specific site collection as the location of your content search and then the name of the Project in the search query. Additionally, an IT admin can use the Site Collections page in the SharePoint admin center to get a list of PWA site collections in the organization.

Delete

You can delete information about a user from your Project Online environment. See [Delete user data from Project Online](#).

Export

You can a specific user's content from your Project Online environment. This data is exported to multiple files in the JSON format. For step-by instructions see, [Export user data from Project Online](#). For detailed information about the files that are exported, see [Project Online export json object definitions](#).

StaffHub

The following sections explain how use the in-app functionality in Microsoft StaffHub to find, access, export, and delete personal data.

Discover

Most data within StaffHub is available to all StaffHub team members and managers. To review data in StaffHub, have a manager or team member go to <https://staffhub.office.com> to look for data that is potentially relevant to the DSR request or have them add you as a member of their team so that you can directly review the StaffHub information for potentially responsive data.

Access

After relevant StaffHub content is found, you can view and take screenshots of relevant data that you would like to provide to the data subject from within the application or download it.

- **Scheduling information** - The **Schedule** tab in StaffHub offers both a **People View** and a **Shifts View** that allows you to view daily, weekly and monthly schedules by team members or by work shifts. These views can be printed or downloaded to Excel by selecting the three dots (ellipsis) in the top left corner of the StaffHub web app and clicking **Export Schedule**.
- **Shared files** - All files in StaffHub are stored on SharePoint Online and can thus be discovered, accessed and exported by using Content Search as previously described above. They can also be viewed from within StaffHub under the tab **Files**.
- **Messaging** - Currently, messages can be accessed by following the steps about accessing user-specific data in the next item. In the future, all messages in StaffHub will be stored in Microsoft Teams, which means you be able to use the Content Search tool to access them.
- **User-specific data** - User-specific data consists of user settings, user activity feed and user shift request history, none of which can be viewed by team members or admins. To access or export user-specific data, have the data subject sign in to their StaffHub account to obtain it. Alternatively, if the data subject has left your organization, you can obtain this data by having your admin reset the user password for the data subject to allow you or the admin to sign in to their account.
- **Kronos** - StaffHub supports connections to [Kronos](#), which is a third-party workforce management tool. StaffHub and Kronos are independent processors and process your organization's data under individual terms that you have signed with each party. If your DSR relates to data held by Kronos you will need to contact Kronos for DSR assistance and vice versa.

Delete

- Most in-app data content mastered in StaffHub can be deleted by a team manager from the app itself. As previously stated in the Discover section for StaffHub, you can add yourself to a team as a team manager and delete the data.
- When a user account is permanently deleted, StaffHub redacts the user's name, phone number, email address, and profile picture within 30 days of the account being deleted.

Export

See the [Access](#) section for StaffHub.

Stream

The following sections explain how to use the in-app functionality in Microsoft Stream to find, access, export, and delete personal data.

Discover

To discover content that is generated or uploaded to Stream that may be relevant to a data subject request, a Stream admin can run a user report to determine what videos, video descriptions, groups, channels or comments a Stream user may have uploaded, created or posted by a user. For instructions on how to generate a report, see [Managing user data in Microsoft Stream](#). The report output is in HTML format and contains hyperlinks that can be used to navigate to videos of potential interest. If you would like to view a video that has custom permission set and you are not part of the original users for whom the video was intended, you can view in admin mode, See [Admin capabilities in Microsoft Stream](#).

Access

Depending on the nature of the data subject request, a copy of the report described above can be used to help satisfy a data subject request. The user report includes the Stream user's name and unique ID, a list of videos the user uploaded, a list of videos the user has access to, a list of channels the user created, a list of all the groups the user is a member of, and a list of all comments the user left on videos. The report further shows whether the user viewed each video listed in the user report. If you would like to provide the data subject with access to a video to satisfy a DSR request, you can share the video.

Export

See the Access section for Stream.

Delete

To delete or edit videos or any other Stream content, a Stream admin can select view in admin mode to perform the necessary function. See [Admin capabilities in Microsoft Stream](#). If a user has left the organization and would like to have their name removed from appearing next to videos that they uploaded, you can remove their name or replace it with another. See [Managing deleted users in Microsoft Stream](#).

Sway

The following sections explain how use the in-app functionality in Microsoft Sway to find, access, export, and delete personal data.

Discover

Content created using Sway (found at www.sway.com) can only be seen by the owner and those that the author has permissioned to view the Sway. See [Privacy Settings in Sway](#). To determine whether Sway is a place where personal data responsive to your DSR is likely to reside, you can ask the Data Subject and organizational users who are likely to have generated content about the Data Subject to search their Sways and share with you any Sways that are likely to contain personal data responsive to the Data Subject's request. For information on how to share a Sway, see "Share a Sway from your Organizational Account" in this [Share your Sway](#) article.

Access

If you have found personal data in a Sway that you would like to share with the Data Subject, you can provide the Data Subject with access to the data through one of several means. You can provide the Data Subject a copy of the online version of Sway (as described above); you can take screen shots of the relevant portion of the Sway that you would like to share; or you can print or download the Sway to Word or convert it to a PDF. How to download a Sway is further described in the "export" section below.

Delete

To learn how to delete a Sway, go to the "How do I delete my Sway?" section in [Privacy settings in Sway](#).

Export

To export a Sway, open the Sway that you would like to download, select the series of dots (ellipsis) in the upper right corner, select **Export**, and then choose either **Word** or **PDF**.

Whiteboard

The following sections explain how use the in-app functionality in Microsoft Whiteboard to find, access, export, and delete personal data.

- [Whiteboard 2016 on Surface Hub](#)
- [Whiteboard on all other platforms](#)

Whiteboard 2016 on Surface Hub

This section describes responding to DSR requests for data created using the built-in Whiteboard 2016 app on Surface Hub.

Discover

Whiteboard files (.wbx files) are stored in users' OneDrive for Business account. You can ask the data subject or other users if whiteboards they created may contain personal data responsive to a DSR request. They can share a whiteboard with you, or you can get a copy of it to give to the data subject.

To access and transfer whiteboards:

1. Give yourself access to the user's OneDrive for Business account. See the "Get access to the former employee's OneDrive for Business documents" section in [Get access to and back up a former user's data](#).
2. Go to the Whiteboard App Data folder in the user's OneDrive for Business account and copy the .wbx files of the whiteboards that you want to transfer.
3. Give yourself access to the data subject's OneDrive for Business account, and then go to Whiteboard App Data

folder.

- Paste the .wbx files that you copied in the previous step.

Access

If you find personal data in a whiteboard that's responsive to a DSR access request, you can provide the data subject access to a whiteboard in several ways:

- Take screenshots of the relevant portions of a whiteboard.
- Upload a copy of the .wbx file to the data subject's OneDrive for Business account. See the previous section for steps on accessing and transferring .wbx files.
- Export a copy of whiteboard as a .png file.

Export

If you've obtained a copy of a whiteboard, you can export it.

- Launch Whiteboard on the Surface Hub.
- Tap the Share button and then select Export a copy. You can export a whiteboard to a OneNote (.one) file or to an image (.png) file.

Delete

You can give yourself access to the user's OneDrive for Business account and then delete the whiteboards.

- Give yourself access to the data subject's OneDrive for Business account. See the "Get access to the former employee's OneDrive for Business documents" section in [Get access to and back up a former user's data](#)
- Go to the Whiteboard App Data folder and then delete the contents of this folder.

Whiteboard for PC, Surface Hub, and other platforms

If an admin receives a DSR request for data in the new Whiteboard app, they can use Whiteboard PowerShell to add themselves (or other users) as an owner of a user's whiteboards. This enables an admin to perform actions including accessing, exporting, and deleting whiteboards. Use either the **Set-WhiteboardOwner** cmdlet to add yourself or another user as the owner of a whiteboard or use the **Invoke-TransferAllWhiteboards** cmdlet to transfer the ownership of all whiteboards for a specific user to a new owner. For information about using these cmdlets and installing the Whiteboard PowerShell module, see Microsoft Whiteboard cmdlet reference. After you or another person has ownership of a whiteboard, see [Microsoft Whiteboard cmdlet reference](#).

After you or another person has ownership of a whiteboard, see the [Whiteboard support article](#) for detailed guidance about accessing, exporting, and deleting whiteboards.

Yammer

The following sections explain how use the in-app functionality in Microsoft Yammer to find, access, export, and delete personal data.

Discover

From the Yammer admin center, a Yammer verified admin (Office 365 global admin or verified admin set up in Yammer) can export data pertaining to a given user. The export includes the messages and files posted and modified by the user, as well as information about topics and groups created by the user. When a user-specific data export is run, the admin will also receive an inbox message with the user's account activity data that they can provide to the user if they so choose. For detailed instructions, see [Yammer Enterprise: Privacy](#).

User-specific exports are for a single network, so if the user is in an external Yammer network, the admin must export data for that external network, as well as for the home network.

To access data not included in data export, screen shots can be taken for the user's profile, settings, group memberships, bookmarked messages, followed users, and followed topics. Users or admins can collect this information. For more information, see [Yammer Enterprise: Privacy](#).

Access

You can view data in the exported files, including the full text of messages and the contents of files. You can also

click links in the exported files to go directly to the posted messages and files in Yammer, and to groups, and topics the user created, messages the user liked, messages where the user is @mentioned, polls the user has voted on, and links the user has added.

Per-user data export does not include:

- The user's profile:
 - If the user has a Yammer identity, the user has full control of their profile. For information on how to view and modify the profile, see [Change my Yammer profile and settings](#).
 - If the user has an Office 365 identity, the Yammer user profile is pulled automatically from Office 365, which gets the profile information from Azure Active Directory (AAD). Yammer users can temporarily change their profiles in Yammer, but these changes are overwritten when there is a change in AAD, so you must view and change directory data in AAD. See [Manage Yammer users across their lifecycle from Office 365](#) and [Add or change profile information for a user in Azure Active Directory](#).
- The user's settings:
 - The user can view and change their own settings. For information on how to view and modify user settings, see [Change my Yammer profile and settings](#). An admin can view this information and take screenshots, but can't change it. Go to Yammer settings > **People**, and then click the name of the user.
 - The user's group membership, bookmarked messages, followed users, and followed topics.
 - The user can view this information. For information on how, see [Tips for staying organized in Yammer](#). An admin can view this information and take screenshots, but can't change it. Go to Yammer settings > **People**, and then click the name of the user.

Export

For instructions for how to export data, see [Manage GDPR data subject requests in Yammer Enterprise](#). You must run a per-user export for each Yammer network the user is a member of.

Note that Yammer has data retention settings that either soft-delete or hard-delete data when a user deletes a message or file. If this is set to soft-delete, data a user has deleted will be included in the export. If the Yammer data retention setting is set to hard-delete, the deleted information is no longer stored in Yammer, so will not be included in the export.

Delete

Yammer allows verified admins to execute a GDPR-compliant delete via the Yammer admin center if they receive a DSR. This option is called Erase User, and it suspends the user for 14 days and then removes all their personal data, excluding files and messages. If the user is a guest user, this must be done for each external network the guest user is a member of.

NOTE

If an admin wants to remove the files and messages of a user during the 14-day window, they will have to perform a user level export to identify the files and messages, and then decide which ones to delete either by in-product deletion or by using a PowerShell script. After the 14-day window, the admin can no longer associate the user with their files or messages.

When a user is deleted with the Erase User option, notification is sent to the Yammer Inbox of all network admins and verified admins. The Erase User option deletes the user's Yammer profile, but does not delete their Office 365 or Azure Active Directory profile.

For detailed steps to remove a user, see [Manage GDPR data subject requests in Yammer Enterprise](#).

Responding to DSR rectification requests

If a data subject has asked you to rectify the personal data that resides in your organization's data stored in Office

365, you and your organization will have to determine whether it's appropriate to honor the request. If you choose to honor the request, then rectifying the data may include taking actions such as editing, redacting, or removing personal data from a document or other type or item. The most expedient way to do this is to ask the data/document owner to use the appropriate Office 365 application to make the requested change. An alternative is to have an IT admin in your organization make the change. This will probably require the IT admin (or other people in your organization with the appropriate privileges, such as a SharePoint Online site collection administrator) to assign to themselves or someone else working on the DSR the necessary permissions to gain access to the document or the content location where the document is located to make the change directly to the document.

Requesting that the data owner to make the approved change

The most direct way to rectify personal data is to ask the data owner to make the change. After you locate the data that is the subject of the DSR, you can provide the following information so that they can make the change.

- The location and file name (for documents and other files) of the item that needs to be changed; locating the data in question is part of the discovery process [discovery process](#) that was previously explained.
- The approved change the data owner should make

You may want to consider implementing a confirmation process where you or another person involved in the DSR investigation verifies that the requested change has been made.

Gaining access to a SharePoint Online site or OneDrive for Business account to make changes

If it's not feasible for the data owner to implement the data subject's request for rectification, an IT admin or SharePoint admin in your organization can get access to the content location and make the required changes. Or, an admin can assign you or another data privacy officer the necessary permissions.

SharePoint Online

To assign administrator or owner permissions to a SharePoint Online site so that you or someone else can access and edit that document, see

- [Manage administrators for a site collection](#)
- [Edit and manage permissions for a SharePoint list or library](#)

OneDrive for Business

An Office 365 global admin can access a user's OneDrive for Business account by using the Office 365 admin center.

1. Sign in to Office 365 with your global admin credentials.
2. Go to the Office 365 admin center.
3. Go to **Active users** and select the user.
4. Expand **OneDrive for Business Settings** in the details pane, and then click **Access files**.
5. Click the URL to go to the user's OneDrive for Business account.

Gaining access to an Exchange Online mailbox to make changes to data

An Office 365 global admin can assign themselves the permissions necessary to open and edit (or delete) items in another user's mailbox, as if they were the mailbox owner. A global admin can also assign these permissions to another user. Specifically, the global admin needs to add the **Read and manage** permission, which is the Full Access permission in Exchange Online. For details, see:

- [Give mailbox permissions to another user in Office 365](#)
- [Access another person's mailbox](#)

Note that if the user mailbox is placed on a legal hold or has been assigned to a retention policy, all versions of a mailbox are retained until the retention period expires or the hold is removed from the mailbox. That means if a mailbox item is changed in response to DSR rectification request, a copy of original item (before the change was made) is retained and stored in a hidden folder in the Recoverable Items folder in the user's mailbox.

Making changes to content in OneDrive for Business and SharePoint Online

Admins or data owners can make changes to SharePoint Online documents, lists, and pages. Keep the following things in mind when making changes to SharePoint content:

- Updating a document will save a new version of the document, which will contain the revision. Older versions of the document will not be updated. That means it's possible that the data that's the subject of a DSR rectification request may persist in older versions of the topic. Note that older versions of a topic can be deleted and then permanently removed from Office 365. See the [Deleting documents in SharePoint Online and OneDrive for Business](#) section in this guide.
- To completely redact a SharePoint file in a way that removes all traces of a data subject from the file, including all versions of the file and all recorded activity performed by the data subject, you would have to perform the following steps:
 1. Download a copy of the file to your local computer.
 2. Permanently delete the file from SharePoint Online, by deleting the file, and then deleting it from the first-stage and second-stage Recycle Bin. See the [Deleting documents in SharePoint Online and OneDrive for Business](#) section in this guide.
 3. Make the revisions to the copy of the document on your local computer.
 4. Upload the revised file to the original SharePoint Online location.
- Data in SharePoint lists can be edited. See [Add, edit, or delete list items](#).

IT admins can also correct certain personal properties associated with a document:

User information from the SharePoint User Profile or Office 365 is often associated with OneDrive for Business and SharePoint Online documents to represent that person. For example, a user's name in a Created By or Modified By People column for a document or list item. This user information can be rectified in several ways, depending on the source:

- Rectify user properties in their own on-premises Active Directory. For customers syncing user properties such as user Display Name, First Name, etc. from an on-premises AD, those properties should be rectified there. Appropriately mapped properties will flow into Office 365, and then OneDrive for Business and SharePoint Online.
- Rectify user properties in the Office 365 Admin Center. Changes made to account information there will automatically be reflected in OneDrive for Business and SharePoint Online experiences. For info, see [Add or change profile information for a user in Azure Active Directory](#). Note that for properties sourced in Office 365, no changes can be made on the SharePoint side.
- Rectify user properties in the SharePoint user profile experience of the SharePoint admin center. In the user profiles tab of the SharePoint admin center, admins can click **Manage user profiles**, and look up any user's properties. Then they can choose to Edit the user's properties.
- Rectify user properties in a custom source. Custom SharePoint profile properties may be syncing from a custom source via Microsoft Identity Manager (MIM) or another method.

Note that this will not affect all experiences, which may retain the older information. For example, the user's name as text in the document.

Making changes to content in Power BI

Power BI relies on the underlying source data used in its dashboards and reports to be complete and accurate, so correcting inaccurate or incomplete source data must be done there. For example, if you created a Power BI report that is connected to Dynamics 365 for Sales as the live data source, you would have to make any corrections to the data in Dynamics 365 for Sales.

After those changes are made, you can take advantage of the [scheduled data refresh](#) capabilities to update the dataset that is stored in Power BI so that the revised data is reflected in the dependent Power BI assets. To help comply with GDPR requirements, you should have policies in place to ensure that you are refreshing your data at an appropriate cadence.

Making changes to content in Yammer

For messages, a user can edit a given message to rectify any inaccuracies. They can request a list of all their messages from a Yammer verified admin, and then click a link in the file to review each message.

For files, a user can edit a given file to rectify any inaccuracies. They can request a list of all the files they posted from a Yammer verified admin, and then access the files in Yammer. Files that are exported into the Files folder can be viewed by searching for the file by number. For example, for a file named 12345678.ppx in the export, use the Search box in Yammer to search for 1235678.ppx. Or, go to

https://www.yammer.com/<network_name>/#/files/<file_number>; for example,

<https://www.yammer.com/contosomkt.onmicrosoft.com/#/files/12345678>.

For data that the user can access through their profile and settings, the user can make any needed changes.

- The user's profile:
 - If the user has a Yammer identity, the user has full control of their profile. For information on how to view and modify the profile, see [Change my Yammer profile and settings](#).
 - If the user has an Office 365 identity, the Yammer user profile is pulled automatically from Office 365, which gets the profile information from Azure Active Directory (AAD). Yammer users can temporarily change their profiles in Yammer, but these changes are overwritten when there is a change in AAD, so the best place to view and change directory data is AAD. The user will need to request that AAD be updated. See [Manage Yammer users across their lifecycle from Office 365](#) and [Add or change profile information for a user in Azure Active Directory](#).
- The user's settings:
 - The user can change their own settings. For information on how to view and modify user settings, see [Change my Yammer profile and settings](#).
 - The user's group membership, bookmarked messages, followed users, and followed topics. The user can change this information; see [Tips for staying organized in Yammer](#).

Responding to DSR restriction requests

Here are the ways to restrict the processing of data in Office 365:

- Remove an Office 365 application license to prevent users from accessing data via an application
- Prevent users from accessing their OneDrive for Business account
- Turn off an Office 365 service from processing the data
- Temporarily remove the data from SharePoint Online and OneDrive for Business and retain it on-premises
- Temporarily restrict all access to a SharePoint Online site
- Prevent a user from signing in to Office 365

If your organization determines later that a restriction no longer applies, you can end the restriction by reversing the steps you took to restrict it; such as re-assigning licenses, turning a service back on, or allowing a user to sign in to Office 365.

Removing the license for an Office 365 application

As previously explained, licenses for all Office 365 applications that are included in your organization's Office 365 subscription are assigned to all users by default. If necessary to restrict access to data that's subject to a DSR, an IT admin can use the Office 365 admin portal temporarily turn off a user's license for an application. If a user then tries to use that application, they'll receive an unlicensed product notification or a message saying they no longer have access. For details, see [Remove licenses from users in Office 365 for business](#).

Notes:

- To restrict a user from accessing Yammer, you must first [enforce Office 365 identify for a Yammer user](#) and then remove the user's Yammer license.
- For scenarios that take advantage of Power BI Embedded, you can restrict access to the independent software vendor (ISV) application that the content is embedded in.

Preventing users from accessing their OneDrive for Business account

Removing a user's SharePoint Online license won't prevent them from accessing their OneDrive for Business account if it already exists. You have to remove the user's permissions to their OneDrive for Business account to. You can do this by removing the user as a site collection owner of their OneDrive for Business account. Specifically, you have to remove the user from the Primary Site Collection Administrator and Site Collection Administrators groups in their user profile. See the "Add and remove admins on a OneDrive for Business account" section in [Manage user profiles in the SharePoint admin center](#).

Turning off an Office 365 Service

Another way to address a DSR request to restrict the processing of data is to turn off an Office 365 service. Of course, this will impact all users in your entire organization and prevent everyone from using the service or accessing data in the service.

The most expedient way to turn off a service is to use Office 365 PowerShell and remove the corresponding user license from all users in the organization. This will in effect restrict anyone from access data in that service. For detailed instructions, see [Disable access to services with Office 365 PowerShell](#) and follow the procedures to disable Office 365 services for users from a single licensing plan.

NOTE

For Yammer, in addition to removing the Yammer license from user accounts, you also must disable users' ability to sign in to Yammer with Yammer credentials (by enforcing the use of their Office 365 credentials when signing in). For detailed instructions, see [Turn off Yammer access for Office 365 users](#).

Temporarily removing data from SharePoint Online or OneDrive for Business sites

Another way to restrict the processing of personal data is to temporarily remove it from Office 365 in response to a DSR. When your organization determines that the restriction no longer applies, you can import the data back into Office 365.

Because most Office documents are located on a SharePoint Online or OneDrive for Business site, here's a high-level process for removing documents from sites and then re-importing them.

1. Get a copy of the document that is the subject of the restriction request. You may have to request either access to the site or ask an Office 365 global admin or a site collection administrator to provide you with a copy of the document.
2. Store the document in an on-premises location (such as a file server or a file share) or another location other

than your Office 365 tenant in the Microsoft cloud.

3. Permanently delete (purge) the original document from Office 365. This is a 3-step process:
 - a. Delete the original copy of the document. When you delete a document from a site, it's sent to the site Recycle Bin (also called the *first-stage Recycle Bin*).
 - b. Go to the site Recycle Bin and delete that copy of the document. When you delete a document from the site Recycle Bin, it's sent to the site collection Recycle Bin (also called the *second-stage Recycle Bin*). See [Delete a file, folder, or link from a SharePoint document library](#).
 - c. Go to the site collection Recycle Bin and delete that copy of the document, which permanently removes it from Office 365. See [Delete items from the site collection recycle bin](#).
4. When the restriction no longer applies, the copy of the document that was stored on-premises can be re-uploaded to the site in Office 365.

IMPORTANT

The preceding procedure won't work if the document is located on a site that is on hold (with one of the retention or legal hold features in Office 365). In the case where a restriction request for a DSR takes precedence over a legal hold, the hold would have to be removed from the site before a document could be permanently deleted. Additionally, the document history for deleted documents is permanently removed.

Temporarily restricting access to SharePoint Online sites

A SharePoint Online administrator can temporarily prevent all users from accessing a SharePoint Online site collection by locking the site collection (by using the **Set-SPOSite -LockState** command in SharePoint Online PowerShell). This will prevent users for accessing the site collection and any content or data that's located in the site. If you then determine that users should be able to access the site, the administrator can unlock the site. See [Set-SPOSite](#) for information about running this PowerShell cmdlet.

Preventing a user from signing in to Office 365

An IT admin can also prevent a user from signing into Office 365, which would prevent the user from accessing any Office 365 online service or processing any data stored in Office 365. See [Block a former employee's access to Office 365 data](#).

Part 2: Responding to DSRs with Respect to Insights Generated by Office 365

The Microsoft suite of Office 365 services includes online services that provide insights to users and organizations that have opted to use them.

- Delve and MyAnalytics provide insights to individual users
- Workplace Analytics provides insights to organizations.

These services are described in the following sections.

Delve

In Delve, users can manage their Office 365 profile and discover people and documents that may be relevant to them. Users can only see documents they have access to. For a series of helpful articles about Delve, see [Office Delve](#).

Access and export

Admins can't access or export a users' Delve data. This means that users have to access and export Delve data themselves. Most of the data types can be accessed and exported directly from Delve, but some data types are only available through other services.

Data available in the Delve user interface

- **Profile data.** This is the profile information from your organization's Global Address List in Azure Active Directory, as well as optional information that users have chosen to add about themselves. To access or export profile data in Delve, a user can click **Me > Update profile**. They can either copy the content directly from the page or take a screenshot.
- **Blog data.** This is blog posts published by a user. To access or export blog data, a user can click **Me > All posts**. They can either copy the content directly from the page or take a screenshot.
- **Recent people data.** These are the people in the organization that Delve has inferred are most relevant to the user at a given time. When a user clicks **Me > See all** in the "Click a person to see what they're working on" pane, Delve shows the most relevant people for a user at a given time.

Data available through an export link in Delve

- **People list data.** These are the people the user has viewed in Delve. The **People** list is shown in the left pane on the home page. Users can export the list of people they have most recently viewed in Delve.
- **Favorites data.** These are boards and documents that the user has marked as their favorite. The **Favorites** page shows boards and documents that the user has added to their favorites. Users can export a list of their current favorite boards and documents.
- **Feature settings data.** These are Delve configurations or actions that result from a user's use of Delve. Users can export a full list of these settings.

To access or export the above data, the user can click the gear icon in the upper-right corner in Delve, and then click **Feature settings > Export data**. Information is exported in JSON format.

Data that's available through other services

- **Popular documents data.** These are documents and email attachments that may be relevant to the user. Delve dynamically organizes these documents and email messages based on the user's activities and people they work with in Office 365. When a user opens Delve or clicks **Home**, Delve shows the most relevant documents or attachments for the user at a given time. To access or export the actual documents and attachments, the user can go to the Office 365 service through which the document or attachment was made available (such as Office.com, SharePoint Online, OneDrive for Business, or Exchange Online).
- **Recent documents and email attachments data.** These are the most recent documents and email attachments that the user has modified. When a user clicks **Me > See all** in the "Get back to your recent documents and email attachments" pane, Delve shows the latest documents and email attachments the user has modified at a given time. To access or export the actual documents and attachments, the user can go to the Office 365 service through which the document or attachment was made available; for example, Office.com, SharePoint Online, OneDrive for Business, or Exchange Online.
- **Documents from people around you data.** These are the documents that Delve has inferred are most relevant to the user at a given time. When a user clicks **Me > See all** in the "Discover documents from people around you" pane, Delve shows the most relevant documents for a user at a given time. To access or export the actual documents, the user can go to the Office 365 service through which the document or attachment was made available (e.g. Office.com, SharePoint Online, OneDrive for Business, or Exchange Online).

Rectify

Users can modify the following information in Delve:

- **Profile information.** A user can click **Me > Update profile** to update their information. Depending on your organization's settings in the Global Address List, users may not be able to modify all their profile information, such as their name or job title.
- **Feature settings.** A user can click the gear icon in the upper-right corner in Delve, and then click **Feature settings >** to change the desired settings.

Restrict

To restrict processing in Delve for your organization, you can turn off the Office Graph. Learn more [here](#).

Delete

Users can delete the following information in Delve:

- **Profile information.** To delete profile information, a user can click **Me > Update profile** and either delete free-form text. Depending on your organization's settings in the Global Address List, users may not be able to delete all their profile information, such as their name or job title.
- **Documents and email attachments.** To delete a document or attachment, users must go to the service where the document or attachment is stored (such as SharePoint Online, OneDrive for Business, or Exchange Online) and delete the document there.

MyAnalytics

MyAnalytics provides statistics to users to help them understand how they spend their time at work. To help your users better understand the data that is presented to them in their personal dashboard and how that data is calculated, direct your users to the [MyAnalytics personal dashboard](#) help topic.

Access and export

If your organization uses MyAnalytics, then Microsoft generates insights for all users – whether they have a MyAnalytics user license or not – to provide meaningful results to your licensed users. All MyAnalytics insights are derived from email and meeting headers in the user's mailbox. Microsoft provides you the ability to export data that MyAnalytics uses to generate these insights by using the DSR case tool in the Security & Compliance Center. For detailed instructions. See [Exporting Data from MyAnalytics and Office Roaming Service](#).

In addition to the insights data that you can export using the Security & Compliance Center, users with a MyAnalytics license can go to the [MyAnalytics dashboard](#) while signed in to their Office 365 account to view the insights that are generated about how they spend their time at work. They can take screenshots of MyAnalytics insights if they want to have permanent copies of their information.

Rectify

All insights generated by MyAnalytics are derived from the user's mail and calendar items. Therefore, there is nothing to rectify other than the source email or calendar items.

Restrict

To restrict processing for a specific user, you can opt them out of MyAnalytics. To see how, see [Configure MyAnalytics user settings](#).

Delete

All mailbox content, including MyAnalytics data, is purged when a user account is "hard-deleted" from Active Directory. For more information, see the [Deleting a user](#) section in this guide.

Workplace Analytics

Workplace Analytics allows organizations to augment Office 365 data with their own business data to gain insights about organizational productivity, collaboration patterns, and employee engagement. [This article](#) explains the control that your organization has over the data that Workplace Analytics processes and who has access to that data.

To assist you with DSRs in Workplace Analytics:

1. Determine whether your organization is using Workplace Analytics. For more information, see [Assign licenses to users in Office 365 for Business](#). If your organization is not using Workplace Analytics, there is no further action.
2. If your organization is using Workplace Analytics, then see who in your organization has been assigned to the role of Workplace Analytics administrator. You should also determine if the data subject's mailbox is licensed for Workplace Analytics. If necessary, have your Workplace Analytics administrator contact

Microsoft Support in handling the following DSR requests.

Access and export

Insights in Workplace Analytics reports created by you may or may not contain personal data of users that your organization licensed for Workplace Analytics, depending on the information that your organization used to supplement the Office 365 data. Your Workplace Analytics administrator will need to review those reports to determine if they contain a user's personal data. If a report does contain a user's personal data, then you will need to decide if you want to provide a copy of that report to the user. Workplace Analytics allows you to export the report.

Rectify

As explained above, Workplace Analytics uses Office 365 data in combination with the organizational data that you provide to generate reports of interest to you. The Office 365 data can't be rectified; it's based on a user's email and calendar activities. However, the organizational data that you have uploaded into Workplace Analytics to generate the report can be rectified. To do this, you will need to correct the source data, upload it, and rerun the report to generate a new Workplace Analytics report.

Restrict

To restrict processing for a specific user, you can remove their Workplace Analytics license.

Delete

If a data subject would like to be removed from a Workplace Analytics report or set of reports, you can delete the report. It is your responsibility to delete users from any organizational data that you used to generate the report, and reupload the data. All data about the user is removed when a user account is "hard-deleted" from Azure Active Directory.

To remove the personal data of a data subject, an Office 365 global administrator can take the following steps:

1. Remove the Workplace Analytics license from the data subject.
2. Delete the Azure Active Directory (AAD) entry for the data subject. (For more information, see [Delete a user](#).)
3. Contact support and have support open a ticket for a Data Subject Rights (DSR) user-delete request. In this ticket, identify the data subject by using their User Principal Name (UPN).
4. Export a copy of the HR data from the company's HR system (see [Export data](#)), remove the data subject's information from that HR data file, and then upload the edited HR data file in .csv format into Workplace Analytics (see [Upload organizational data](#)).

Part 3: Responding to DSRs for system-generated Logs

Microsoft also provides you with the ability to access, export, and delete system-generated logs that may be deemed personal under the GDPR's broad definition of "personal data." Examples of system-generated logs that may be deemed personal under GDPR include:

- Product and service usage data such as user activity logs
- User search requests and query data
- Data generated by product and services as a product of system functionality and interaction by users or other systems

Note that the ability to restrict or rectify data in system-generated logs is not supported. Data in system-generated logs constitutes factual actions conducted within the Microsoft cloud and diagnostic data, and modifications to such data would compromise the historical record of actions and increase fraud and security risks.

Accessing and exporting system-generated logs

Admins can access system-generated logs associated with a particular user's use of Office 365 services and applications. To access and export system-generated logs:

1. Go to the [Microsoft Service Trust Portal](#) and sign in using the credentials of an Office 365 global administrator.
2. In the **Privacy** drop-down list at the top of the page, click **Data Subject Request**.
3. On the **Data Subject Request** page, under **System Generated Logs**, click **Data Log Export**.

The **Data Log Export** is displayed. Note that a list of export data requests submitted by your organization is displayed.

4. To create a new request for a user, click **Create Export Data Request**.

After you create a new request, it will be listed on the **Data Log Export** page where you can track its status. After a request is complete, you can click a link to access the system-generated logs, which will be exported to your organization's Azure storage location within 30 days of creating the request. The data will be saved in common, machine-readable file formats such as JSON or XML. If you don't have an Azure account and Azure storage location, you'll need to create an Azure account and/or Azure storage location for your organization so that the Data Log Export tool can export the system-generated logs. For more information, see [Introduction to Azure Storage](#).

NOTE

When you create an Export Data Request, system-generated data for a few applications will not be exported through the Data Log Export tool. To export data for these applications, see [Additional steps to export system-generated log data](#).

The following summarizes accessing and exporting system-generated logs using the Data Log Export tool:

How long does the Microsoft Data Log Export tool take to complete a request? This can depend on several factors. In most cases it should complete in one or two days, but it can take up to 30 days.

What format will the output be in? The output will be structured machine-readable files such as XML, CSV, or JSON.

Who has access to Data Log Export tool to submit access requests for system-generated logs? Office 365 global administrators will have access to the GDPR Log Manager utility.

What data does the Data Log Export tool return? The Data Log Export tool returns system generated logs that Microsoft stores. Exported data will span across various Microsoft services including Office 365, Azure and Dynamics.

How is data returned to the user? Data will be exported to your organization's Azure storage location; it will be up to admins in your organization to determine how they will show/return this data to users.

What will data in system-generated logs look like? Example of a system-generated log record in JSON format:

```
[{"  
    "DateTime": "2017-04-28T12:09:29-07:00",  
    "AppName": "SharePoint",  
    "Action": "OpenFile",  
    "IP": "154.192.13.131",  
    "DevicePlatform": "Windows 1.0.1607"}]
```

NOTE

Some features will not allow for the export or deletion of system-generated logs with personal information to maintain the integrity of such information for security and audit reasons.

Product and service usage data for some of Microsoft's most often-used services, such as Exchange Online, SharePoint Online, Skype for Business, Yammer and Office 365 Groups can also be retrieved by searching the Office 365 audit log in the Security & Compliance Center. For more information, see [Use the Office 365 audit log search tool in DSR investigations](#) in Appendix A. Using the audit log may be of interest to you because it's possible to assign permissions to other people in your organization (such as your compliance officer) to search the audit log to access this data.

National clouds

A global IT admin will need to do the following to export system-generated log data in the following national clouds:

- Office 365 Germany - [Go to the Microsoft Service Trust Portal for Germany](#) and complete the steps outlined above.
- Office 365 US Government - [Go to the Office 365 admin portal](#) and submit a request to Microsoft Support.
- Office 365 operated by 21Vianet (China) - [Go to the Office 365 operated by 21Vianet admin portal](#) and then go to **Commerce** > **Subscription** > **Privacy** > **GDPR** and enter the required information.

Deleting system-generated logs

To delete system-generated logs retrieved through an access request, you must remove the user from the service and permanently delete their Azure Active Directory account. For instructions about permanently delete a user, see the [Deleting a user section](#) in this guide. It's important to note that permanently deleting a user account is irreversible once initiated.

Permanently deleting a user account will remove the user's data from system-generated logs for nearly all Office 365 services within 30 days. One exception to this is that the permanent deletion of the user account takes longer than 30 days in Exchange Online. Given the critical nature of Exchange Online content and prevent accidental data loss, this system has been engineered to intentionally place data in a holding state for up to 60 days after a user account has been permanently deleted. To permanently delete a user's Exchange Online data in a 30-day time frame, permanently delete the user account in Azure Active Directory and then contact [Microsoft Support](#) and request that the user's Exchange Online data be manually removed outside the scheduled delete process. For more information, see [Removing Exchange Online data](#), which was previously explained in this guide

Deleting a user's account will not remove system-generated logs for Yammer and Kaizala. To remove the data from these applications, see one of the following:

- Yammer - [Manage GDPR data subject requests in Yammer Enterprise](#)
- Kaizala - [Export or delete a user's organizational data in Kaizala](#)

National clouds

A global IT admin will need to do the following to delete system-generated logs in the following national clouds:

- Office 365 Germany - When the user account is permanently deleted, the system-generated logs will also be deleted.
- Office 365 US Government - Submit a request to Microsoft Support via the [Office 365 admin portal](#).
- Office 365 operated by 21Vianet (China) - Submit a request to Microsoft Support via the Office 365 admin portal at this [URL](#). Go to **Commerce** and then select **Subscription** -> **Privacy** -> **GDPR** and enter the required information.

Part 4: Additional resources to assist you with DSRs

DSR guides for other Microsoft enterprise services

This guide is dedicated to the topic of how to find and act on personal data to respond to DSRs when using Office 365 products, services and administrative tools. Go to the [Microsoft Service Trust Portal](#) to access similar guides for other Microsoft enterprise services.

Microsoft Support

"Support Data" is the data you and your users provide to Microsoft if your organization or your users engage with Microsoft to receive product support related to Office 365 or other Microsoft products and services (for example, to troubleshoot unexpected product behavior). Some of this data may contain personal data. For more information, see [Microsoft Support and Professional Services Data Subject Requests for the GDPR](#).

Product and services authenticated with an Org ID for which Microsoft is a data controller

Parts 1-3 of this guide cover products and services for which Microsoft is a data processor to your organization, and thus DSR capability is made available to your tenant administrator. There are a variety of circumstances where your organization's users may use their work or school account (also referred to as "Azure Active Directory ID" or "AAD") to sign in to Microsoft products and services for which Microsoft is a data controller. For all such products and services, your users will need to initiate their own data subject requests directly to Microsoft and Microsoft will fulfill the requests directly to the user. Note that, by design, products and services involving storage of user-authored content enable users to access, export, rectify, and delete their user-authored content as part of the inherent functionality of the products. Scenarios where this may apply include the following:

- **Optional connected online services** – Office 365 ProPlus makes certain optional connected online services available to the user. The list of such services and related user controls are listed [here](#). You can decide whether you would like to allow your end users to use these services. For more information, see [How admins can manage controller services in Office 365 ProPlus](#). To the extent that these optional services process personal data, Microsoft is a data controller for these services.
- **User feedback** – If your users elect to provide feedback on Microsoft products and services, Microsoft is a data controller for such feedback to the extent it contains personal data. Microsoft will fulfill any data subject requests for feedback collected by Microsoft (including feedback managed by Microsoft subprocessors) except in cases where Microsoft has instructed users to not include personal data during the feedback collection process. Exceptions: If Microsoft has instructed users to not include personal data during the feedback collection process, Microsoft will rely on that instruction and will assume that no personal data has been provided. Users who have created a separate account with third-party feedback service providers will need to fulfill their DSR directly with those providers.
- **Windows authenticated via work or school account** - If your organization has purchased Windows licenses, and your users authenticate to organization-provided Windows with their work or school account, Microsoft acts as a data controller. For more information, see the [Windows Data Subject Requests for the GDPR](#).
- **User-acquired products or services** - If you allow your users, acting in their individual capacity, to acquire Microsoft products or services that use AAD for authentication (for example, Office Add-Ons or applications available in a Microsoft Store), Microsoft may be a data controller. For any such Microsoft products or services, users will need to contact Microsoft directly to initiate a DSR.

IMPORTANT

If you delete a user as enabled via Azure Active Directory, your (former) user will lose the ability to sign in to any products or services for which he or she formerly relied upon for a work or school account. Additionally, Microsoft will no longer be able to authenticate the user in connection with a DSR request for products or services for which Microsoft is a data controller. If you wish to enable a user to initiate DSRs against such services, it is important you instruct your user to do so before you delete the user's AAD account.

Personal accounts

If your users have used Microsoft accounts (i.e. personal accounts) to acquire products and services from Microsoft

for their own use and for which Microsoft is a data controller, they may initiate DSR requests by using the [Microsoft privacy dashboard](#).

Third party products

If your organization, or your users acting in their individual capacity, have acquired products or services from third parties and use their Microsoft work or school account for authentication, any data subject requests should be directed to the applicable third party.

Appendix A: Preparing for DSR investigations

To help prepare your organization to undertake DSR investigations using Office 365 services, consider the following recommendations:

- Use the DSR eDiscovery case tool in the Office 365 Security & Compliance Center to manage DSR investigations
- Set up Compliance Boundaries to limit the scope of Content Searches
- Use the Office 365 audit log search tool in DSR investigations

Use the DSR case tool to manage DSR investigations

We recommend that you use the DSR case tool in Security & Compliance Center to manage DSR investigations.

By using the DSR case tool, you can:

- Create a separate case for each DSR investigation.
- Use the built-in to search for all content related to a specific data subject. When you create a new case and start the search, these content locations are searched:
 - All mailboxes in your organization (including the mailboxes associated with all Microsoft Teams and Office 365 Groups)
 - All SharePoint Online sites and OneDrive for Business accounts in your organization
 - All Microsoft Teams sites and Office 365 group sites in your organization
 - All public folders in Exchange Online
- Revise the default search query and re-run the search to narrow the search results.
- Control who has access to the case by adding people as members of the case; only members can access the case and they'll be able only see their cases in the list of cases on the DSR cases page in the Security & Compliance Center. Additionally, you can assign different permissions to different members of the same case. For example, you could allow some members to only view the case and the results of a Content Search and allow other members to create searches and export search results.
- Create export jobs to export the search results in response to a DSR export request. You can export all content returned by the Content Search. Additionally, other Office 365 data related to a data subject will also be exported.
- Create export jobs to export the search results in response to a DSR export request. You can export all content returned by the Content Search. Additionally, you can export system-generated logs for My Analytics and Office Roaming service.
- Delete cases when the DSR investigation process is complete. This will remove all the content searches and export jobs associated with the case.

To get started with using DSR cases, see [Manage GDPR data subject requests with the DSR case tool in the Office 365 Security & Compliance Center](#).

IMPORTANT

An eDiscovery Administrator can view and manage all DSR cases in your organization. For more information about the different roles related to eDiscovery, see [Assign eDiscovery permissions to potential case members](#).

Set up Compliance Boundaries to limit the scope of Content Searches

Compliance Boundaries are implemented by using the search permissions filtering functionality in the Security & Compliance Center. Compliance Boundaries create logical search boundaries within an organization that control/limit which content locations (for example Exchange Online mailboxes and SharePoint Online sites) that an IT admin or compliance officer can search. Compliance Boundaries are useful for multi-national organizations that need to respect geographical boundaries, governmental organizations that need to separate different agencies, and business organizations that segregated into business unit or department. For all these scenarios, Compliance Boundaries can be used in DSR investigations to limit which mailboxes and sites can be searched by people involved in the investigation.

You can use Compliance Boundaries together with eDiscovery cases to limit the content locations that can be searched in an investigation to those locations only within the agency or business unit.

Here's a high-level overview of how to implement Compliance Boundaries (together with eDiscovery cases) for DSR investigations.

1. Determine the agencies in your organization that will be designated as a compliance boundary.
2. Determine which user object attribute in Azure Active Directory will be used to define the compliance boundary. For example, you might choose the Country, CountryCode, or Department attribute, so that members of the admin role group that you create in the next step can only search the content locations of the users that have a specific value for that attribute. This is how you limit who can search for content in a specific agency.

NOTE

Currently, you must perform an additional step for OneDrive for Business and file a Microsoft Support request to have the attribute synchronized to OneDrive for Business accounts.

4. Create an admin role group in the Office 365 Security & Compliance Center for each compliance boundary. We recommend that you create these role groups by copying the built-in eDiscovery Manager role group and then removing any roles as necessary.
5. Add members to each of the specific role groups as eDiscovery Managers. Members will be the people responsible for investigating and responding to DSRs, and will typically consist of IT admins, data privacy officers, compliance managers, and human resource representatives.
6. Create a search permissions filter for each compliance boundary so that the members of the corresponding admin role group can only search mailboxes and sites for users within that agency/compliance boundary. The search permissions filter will allow members of the corresponding role group to search only the content locations with user object attribute value that corresponds to the agency/compliance boundary.

For step-by-step instructions, see [Set up compliance boundaries for eDiscovery investigations in Office 365](#).

Use the Office 365 audit log search tool in DSR investigations

IT admins can use the audit log search tool in the Security & Compliance Center to identify documents, files, and other Office 365 resources that users have created, accessed, changed, or deleted. Searching for this kind activity can be useful in DSR investigations. For example, in SharePoint Online and OneDrive for Business, auditing events are logged when users perform these activities:

- Accessed a file
- Modified a file
- Moved a file
- Uploaded or downloaded a file

You can search the audit log for specific activities, types of activities, activities performed by a specific user, and other search criteria. In addition to SharePoint Online and OneDrive for Business activities, you can also search for activities in Flow, Power BI, and Microsoft Teams. Note that auditing records are retained for 90 days. Therefore, you won't be able to search for user activities that occurred more than 90 days ago. For a complete list of audited activities and how to search the audit log, see [Search the audit log in the Office 365 Security & Compliance Center](#).

TIP

To work around the 90-day limitation discussed above and maintain a running history of your organization's auditing records, you could export all activities on a recurring schedule (for example, every 30 days) to have a continuous record of your organization's auditing records.

Appendix B: Change log

The following table lists the changes to the Office 365 DSR guide since its initial publication on May 25, 2018.

DATE	SECTION/APP	CHANGE
9/18/2018	Whiteboard	Whiteboard Preview is no longer in preview and has been released to general availability. Therefore, the section on Whiteboard Preview was renamed to "Whiteboard for PC, Surface Hub, and other platforms"; procedures to access, export, and delete data were removed from this section and replaced with a link to the Whiteboard support article.
11/08/2018	Workplace Analytics	Added step-by-step guidance to the Delete section about removing a data subject from Workplace Analytics and removing information about a data subject from a Workplace Analytics report.
11/12/2018	All	Fixed broken bookmarks and broken links to external topics.
1/9/2019	StaffHub	In the Delete section, updated the description of what happens when a user account is permanently deleted.

Azure Data Subject Requests for the GDPR

2/22/2019 • 19 minutes to read • [Edit Online](#)

Introduction to Data Subject Requests (DSRs)

The EU Data Protection Regulation (GDPR) gives rights to people (known in the regulation as *data subjects*) to manage the personal data that has been collected by an employer or other type of agency or organization (known as the *data controller* or just *controller*). Personal data is defined very broadly under the GDPR as any data that relates to an identified or identifiable natural person. The GDPR gives data subjects specific rights to their personal data; these rights include obtaining copies of personal data, requesting corrections to it, restricting the processing of it, deleting it, or receiving it in an electronic format so it can be moved to another controller. A formal request by a data subject to a controller to take an action on their personal data is called a *Data Subject Request* or DSR.

The guide discusses how to use Microsoft products, services and administrative tools to help our controller customers find and act on personal data to respond to DSRs. Specifically, this includes how to find, access, and act on personal data that reside in the Microsoft cloud. Here's a quick overview of the processes outlined in this guide:

1. **Discover**—Use search and discovery tools to more easily find customer data that may be the subject of a DSR. Once potentially responsive documents are collected, you can perform one or more of the DSR actions described in the following steps to respond to the request. Alternatively, you may determine that the request doesn't meet your organization's guidelines for responding to DSRs.
2. **Access**—Retrieve personal data that resides in the Microsoft cloud and, if requested, make a copy of it that can be available to the data subject.
3. **Rectify**—Make changes or implement other requested actions on the personal data, where applicable.
4. **Restrict**—Restrict the processing of personal data, either by removing licenses for various Azure services or turning off the desired services where possible. You can also remove data from the Microsoft cloud and retain it on-premises or at another location.
5. **Delete**—Permanently remove personal data that resided in the Microsoft cloud.
6. **Export**—Provide an electronic copy (in a machine-readable format) of personal data to the data subject.

Each section in this guide outlines the technical procedures that a data controller organization can take to respond to a DSR for personal data in the Microsoft cloud.

Terminology

The following provides definitions of terms that are relevant to this guide.

- **Controller**—The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- **Personal data and data subject**—Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **Processor**—A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

- *Customer Data*—All data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, a customer through use of the enterprise service. Customer Data includes both (1) identifiable information of end users (e.g., user names and contact information in Azure Active Directory) and Customer Content that a customer uploads into or creates in specific services (e.g., customer content in an Azure Storage account, customer content of an Azure SQL Database, or a customer's virtual machine image in Azure Virtual Machines).
- *System-Generated Logs*—Logs and related data generated by Microsoft that help Microsoft provide enterprise services to users. System-generated logs contain primarily pseudonymized data, such as unique identifiers – typically a number generated by the system that cannot on its own identify an individual person but is used to deliver the enterprise services to users. System-generated logs may also contain identifiable information about end users, such as a user name.

How to use this guide

This guide consists of two parts:

Part 1: Responding to Data Subject Requests for Customer Data — Part 1 of this guide discusses how to access, rectify, restrict, delete, and export data from applications in which you have authored data. This section details how to execute DSRs against both Customer Content and also identifiable information of end users.

Part 2: Responding to Data Subject Requests for System-Generated Logs — When you use Microsoft's enterprise services, Microsoft generates some information, known as System-Generated Logs, in order to provide the service. Part 2 of this guide discusses how to access, delete and export such information for Azure.

Understanding DSRs for Azure Active Directory and Microsoft Service Accounts

When considering services provided to enterprise customers, execution of DSRs must always be understood within the context of a specific Azure Active Directory (AAD) tenant. Notably, DSRs are always executed within a given AAD tenant. If a user is participating in multiple tenants, it is important to emphasize that a given DSR is *only* executed within the context of the specific tenant the request was received within. This is critical to understand as it means the execution of a DSR by one enterprise customer **will not** impact the data of an adjacent enterprise customer.

The same also applies for Microsoft Service Accounts (MSA) within the context of services provided to an enterprise customer: execution of a DSR against an MSA account *associated with an AAD tenant* **will only** pertain to data within the tenant. In addition, it is important to understand the following when handling MSA accounts within a tenant:

- If an MSA user creates an Azure subscription, the subscription will be handled as if it were an AAD tenant. Consequently, DSRs are scoped within the tenant as described above.
- If an Azure subscription created via an MSA account is deleted, **it will not affect** the actual MSA account. Again, as noted above, DSRs executing within the Azure subscription are limited to the scope of the tenant itself.

DSRs against an MSA account itself, **outside a given tenant**, are executed via the Consumer Privacy Dashboard. Please refer to the Windows Data Subject Request Guide for further details.

Part 1: DSR Guide for Customer Data

Executing DSRs against Customer Data

Microsoft provides the ability to access, delete, and export certain Customer Data through the Azure Portal and also directly via pre-existing application programming interfaces (APIs) or user interfaces (UIs) for specific services (also referred to as *in-product experiences*). Details regarding such in-product experiences are described in the respective services' reference documentation.

[Important]

Services supporting in-product DSRs require direct usage of the service's application programming interface (API) or user interface (UI), describing applicable CRUD (create, read, update, delete) operations. Consequently, execution of DSRs within a given service must be done in addition to execution of a DSR within the Azure Portal in order to complete a full request for a given data subject. Please refer to specific services' reference documentation for further details.

Step 1: Discover

The first step in responding to a DSR is to find the personal data that is the subject of the request. This first step - finding and reviewing the personal data at issue - will help you determine whether a DSR meets your organization's requirements for honoring or declining a DSR. For example, after finding and reviewing the personal data at issue, you may determine the request doesn't meet your organization's requirements because doing so may adversely affect the rights and freedoms of others.

After you find the data, you can then perform the specific action to satisfy the request by the data subject.

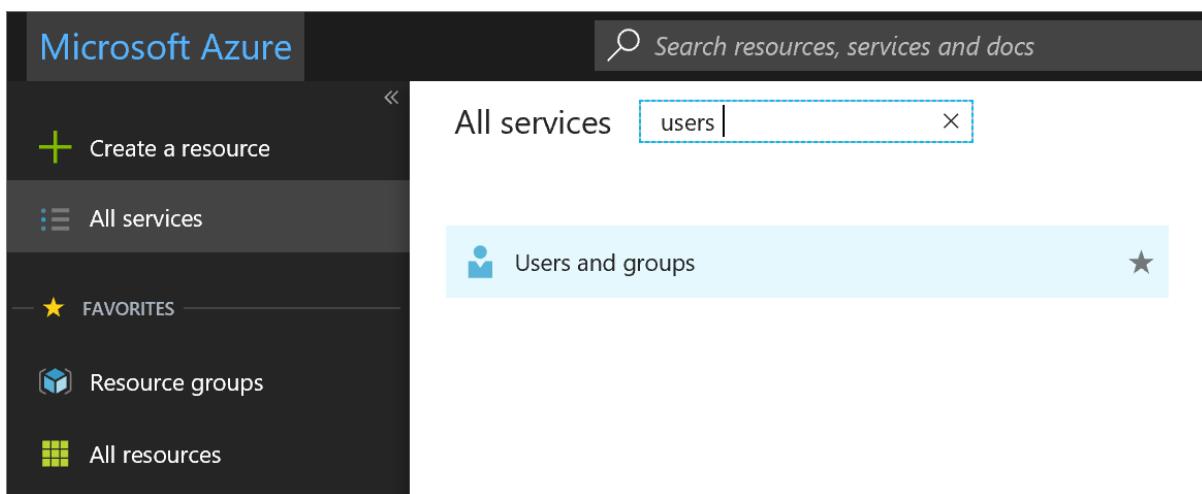
Azure Active Directory

[Azure Active Directory](#) is Microsoft's cloud-based, multi-tenant directory and identity management service. You can locate identifiable information of end users, such as customer and employee user profiles and user work information that contain personal data in your [Azure Active Directory](#) (AAD) environment by using the [Azure portal](#).

This is particularly helpful if you want to find or change personal data for a specific user. You can also add or change user profile and work information. You must sign in with an account that's a global admin for the directory.

How do I locate or view user profile and work information?

1. Sign in to the [Azure portal](#) with an account that's a global admin for the directory.
2. Select **All services**, enter **Users and groups** in the text box, and then select **Enter**.



3. On the **Users and groups** blade, select **Users**.

The screenshot shows the Azure portal interface for User management. On the left sidebar, there's a list of resources including Resource groups, All resources, Recent, App Services, Virtual machines (classic), Virtual machines, SQL databases, Cloud services (classic), Security Center, Subscriptions, User management, and Enterprise applications. Below this is a 'Browse >' link. The main content area has a title 'User management - Users f/128 Photography - PREVIEW'. It includes a search bar at the top. A navigation menu on the left lists GENERAL, RESOURCES, and CONFIGURATION sections. Under RESOURCES, the 'Users' option is selected and highlighted with a red box. Under CONFIGURATION, there are links for Groups, Domains, Azure AD Connect, Settings, and Password reset. The main pane displays a table of users with columns for NAME and USER NAME. Each user row includes a small profile picture, the user's name, their email address, and a three-dot ellipsis button. The table contains 20 entries, starting with Aaron Nicholls and ending with Amelia Casias.

NAME	USER NAME
Aaron Nicholls	tnich@f128.info
Abby Brennan	abrennan@f128.info
Adam Carlton	acarlton@f128.info
Adam Steenwyk	adam@f128.info
Adam Steenwyk	adam@f128.onmicrosoft.com
Adam Steenwyk (admin f128.onmicrosoft.com)	admin@f128.onmicrosoft.com
Adam Steenwyk (admin)	admin@f128.info
Adam Steenwyk (MSA)	ajamess_gmail.com#EXT#@f128.onmicrosoft.com
Adrian Martin	amartin@f128.info
Aidan Mitzner	amitzner@f128.info
Ajay Mokashi	amokashi@f128.info
Alain DuBois	adubois@f128.info
Alberto Bassani	abassani@f128.info
Alejandro Ruiz	aruiz@f128.info
Alex Grossman	agrossman@f128.info
Alice Gartner	alice@f128.info
Allison Hunter	ahunter@f128.info
Alvin Hwang	ahwang@f128.info
Amanda Baker	abaker@f128.info
Amanda Mackenzie	amackenzie@f128.info
Amelia Casias	acasias@f128.info

4. On the **Users and groups - Users** blade, select a user from the list, and then, on the blade for the selected user, select **Profile** to view user profile information that might contain personal data.

The screenshot shows the Microsoft 365 Admin Center interface. On the left, there is a list of users with their names, email addresses, and small profile pictures. One user, Angie Shannon, is highlighted with a blue selection bar. On the right, the 'User - Profile' page is displayed for Angie Shannon. The top navigation bar includes 'Save' and 'Discard' buttons. The main area is divided into sections: 'GENERAL' (Overview, Audit, Profile - which is selected and highlighted in blue), 'ACCESS' (Organizational Role, Groups, Sign ins, Azure Subscription Resources), 'Photo' (with a placeholder image and a 'Select a file' button), 'Object ID' (containing the value '3beb06c5 687e 4ae5 9c6b bdcbae438f33'), 'Source' (set to 'Azure Active Directory'), 'Settings' (Block sign in, Yes/No button, set to No), 'Usage location' (United States dropdown), 'Authentication contact info' (Authentication phone and Alternate authentication phone fields), and 'Last sign in' (with a timestamp).

- If you need to add or change user profile information, you can do so, and then, in the command bar, select **Save**.

Service-Specific Interfaces

Microsoft provides the ability to discover Customer Data directly via pre-existing application programming interfaces (APIs) or user interfaces (UIs) for specific services. Details are described in the respective services' reference documentation, describing applicable CRUD (create, read, update, delete) operations.

Step 2: Access

After you've found Customer Data containing personal data that is potentially responsive to a DSR, it is up to you and your organization to decide which data to provide to the data subject. You can provide them with a copy of the actual document, an appropriately redacted version, or a screenshot of the portions you have deemed appropriate to share. For each of these responses to an access request, you will have to retrieve a copy of the document or other item that contains the responsive data.

When providing a copy to the data subject, you may have to remove or redact personal information about other data subjects and any confidential information.

The following explains how to get a copy of data in response to a DSR access request.

Azure Active Directory

Microsoft offers both a portal and in-product experiences providing the enterprise customer's tenant administrator the capability to manage DSR access requests. DSR Access requests allow for access of the personal data of the user, including: (a) identifiable information about an end-user and (b) system-generated logs.

Service-Specific Interfaces

Microsoft provides the ability to discover Customer Data directly via pre-existing application programming interfaces (APIs) or user interfaces (UIs) for specific services. Details are described in the respective services'

reference documentation, describing applicable CRUD (create, read, update, delete) operations.

Step 3: Rectify

If a data subject has asked you to rectify the personal data that resides in your organization's data, you and your organization will have to determine whether it's appropriate to honor the request. Rectifying the data may include taking actions such as editing, redacting, or removing personal data from a document or other type or item. The most expedient way to do this for Microsoft Support and FastTrack data is provided below.

Azure Active Directory

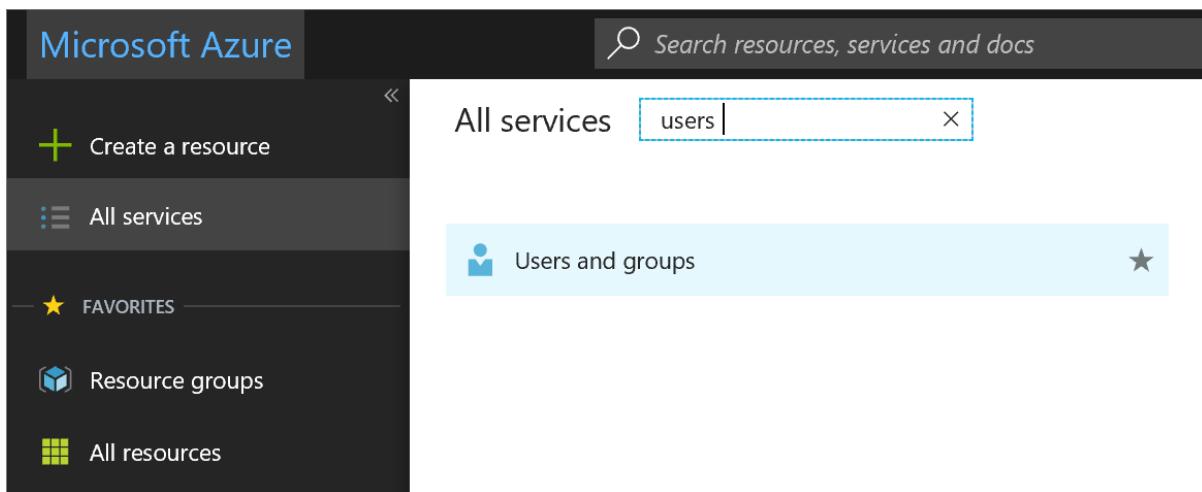
Enterprise customers have the ability to manage DSR rectify requests, including limited editing features per the nature of a given Microsoft service. As a data processor, Microsoft does not offer the ability to correct system-generated logs as it reflects factual activities and constitutes a historical record of events within Microsoft services. With respect to Azure Active Directory, limited editing features exist to rectify identifiable information about an end-user, as described further below.

Azure Active Directory: rectify/correct inaccurate or incomplete personal data

You can correct, update, or delete identifiable information about end users, such as customer and employee user profiles and user work information that contain personal data, such as a user's name, work title, address, or phone number, in your [Azure Active Directory](#) (AAD) environment by using the [Azure portal](#). You must sign in with an account that's a global admin for the directory.

How do I correct or update user profile and work information in Azure Active Directory?

1. Sign in to the [Azure portal](#) with an account that's a global admin for the directory.
2. Select **All services**, enter **Users and groups** in the text box, and then select **Enter**.



3. On the **Users and groups** blade, select **Users**.

The screenshot shows the Azure portal interface for User management. On the left sidebar, there's a list of resources including Resource groups, All resources, Recent, App Services, Virtual machines (classic), Virtual machines, SQL databases, Cloud services (classic), Security Center, Subscriptions, User management, and Enterprise applications. The 'User management' item is currently selected. The main content area is titled 'User management - Users' and shows a preview for 'f128 Photography'. It has tabs for General, Overview, Audit, Resources, Configuration, Domains, Azure AD Connect, Settings, and Password reset. Under 'Resources', the 'Users' tab is selected and highlighted with a red box. A search bar at the top says 'Search (Ctrl+ /)'. Below it, there's a table with columns 'NAME' and 'USER NAME'. The table lists 20 users, each with a small profile picture, their name, their email address, and a three-dot ellipsis button for more options. The users listed are: Aaron Nicholls (tnich@f128.info), Abby Brennan (abrennan@f128.info), Adam Carlton (acarlton@f128.info), Adam Steenwyk (adam@f128.info), Adam Steenwyk (admin f128.onmicrosoft.com) (admin@f128.onmicrosoft.com), Adam Steenwyk (admin) (admin@f128.info), Adam Steenwyk (MSA) (ajamess_gmail.com#EXT#@f128.onmicrosoft.com), Adrian Martin (amartin@f128.info), Aidan Mitzner (amitzner@f128.info), Ajay Mokashi (amokashi@f128.info), Alain DuBois (adubois@f128.info), Alberto Bassani (abassani@f128.info), Alejandro Ruiz (aruiz@f128.info), Alex Grossman (agrossman@f128.info), Alice Gartner (alice@f128.info), Allison Hunter (ahunter@f128.info), Alvin Hwang (ahwang@f128.info), Amanda Baker (abaker@f128.info), Amanda Mackenzie (amackenzie@f128.info), and Amelia Casias (acasias@f128.info).

NAME	USER NAME
Aaron Nicholls	tnich@f128.info
Abby Brennan	abrennan@f128.info
Adam Carlton	acarlton@f128.info
Adam Steenwyk	adam@f128.info
Adam Steenwyk	adam@f128.onmicrosoft.com
Adam Steenwyk (admin)	admin@f128.onmicrosoft.com
Adam Steenwyk (MSA)	ajamess_gmail.com#EXT#@f128.onmicrosoft.com
Adrian Martin	amartin@f128.info
Aidan Mitzner	amitzner@f128.info
Ajay Mokashi	amokashi@f128.info
Alain DuBois	adubois@f128.info
Alberto Bassani	abassani@f128.info
Alejandro Ruiz	aruiz@f128.info
Alex Grossman	agrossman@f128.info
Alice Gartner	alice@f128.info
Allison Hunter	ahunter@f128.info
Alvin Hwang	ahwang@f128.info
Amanda Baker	abaker@f128.info
Amanda Mackenzie	amackenzie@f128.info
Amelia Casias	acasias@f128.info

4. On the **Users and groups - Users** blade, select a user from the list, and then, on the blade for the selected user, select **Profile** to view the user profile information that needs to be corrected or updated.

The screenshot shows two windows side-by-side. On the left is a list of users with columns for Name and User Name. On the right is the 'User - Profile' blade for 'Angie Shannon - PREVIEW'. The 'Profile' tab is selected. The General section shows the user's name (Angie Shannon) and user name (angie@litwarecorp.com). There is a placeholder photo and a button to upload a new photo. The 'Object ID' is listed as 3beb06c5 687e 4ae5 9c6b bdcbae438f33. The 'Source' is set to Azure Active Directory. Under 'Settings', 'Block sign in' is set to 'No'. The 'Usage location' is United States. The 'Authentication contact info' section includes fields for 'Authentication phone' and 'Alternate authentication phone', both currently empty.

NAME	USER NAME
Abbie Spencer	aspencer@litwarecorp.com
AJ	tperkins_f128.info#EXT#@litware154.onmicrosoft.com
Al Vanover	avanover@litwarecorp.com
Alfred Borrego	alfred@litwarecorp.com
Alfred Geer	ageer@litwarecorp.com
Althea Spears	althea@litwarecorp.com
Amanda Dunlap	amanda@litwarecorp.com
Andy Pettis	andy@litwarecorp.com
Angie Shannon	angie@litwarecorp.com
Annabelle Ballard	annabelle@litwarecorp.com
Anne-Marie Johansen	annemarie@litwarecorp.com
Anthony Philip	anthony@litwarecorp.com
Arthur Theriot	arthur@litwarecorp.com
Audrey Bradley	audrey@litwarecorp.com
Aurel Cuza	aurel@litwarecorp.com
Austin Jin	austin@litwarecorp.com
Bhaanulata Mokkapati	bhaanulata@litwarecorp.com
Bryce Ault	bryce@litwarecorp.com
Cecill Noll	cnoll@litwarecorp.com
Cezar Spirlea	cezar@litwarecorp.com

5. Correct or update the information, and then, in the command bar, select **Save**.
6. On the blade for the selected user, select **Work Info** to view user work information that needs to be corrected or updated.

- Correct or update the user work information, and then, in the command bar, select **Save**.

Service-Specific Interfaces

Microsoft provides the ability to discover Customer Data directly via pre-existing application programming interfaces (APIs) or user interfaces (UIs) for specific services. Details are described in the respective services' reference documentation, describing applicable CRUD (create, read, update, delete) operations.

Step 4: Restrict

Data subjects may request that you restrict processing of their personal data. We provide both the Azure Portal and pre-existing application programming interfaces (APIs) or user interfaces (UIs). These experiences provide the enterprise customer's tenant administrator the capability to manage such DSRs through a combination of data export and data deletion. A customer may (1) export an electronic copy of the personal data of the user, including (a) account(s), (b) system-generated logs, and (c) associated logs, followed with (2) deletion of the account and associated data residing within Microsoft systems.

Step 5: Delete

The "right to erasure" by the removal of personal data from an organization's Customer Data is a key protection in the GDPR. Removing personal data includes removing all personal data and system-generated logs, except audit log information. When a user is **soft deleted** (see details below), the account is disabled for 30 days. If no further action is taken during this 30 day period, the user is **permanently deleted** (again, see details below). Upon a **permanent delete**, the user's account, personal data, and system-generated logs are expunged within an additional 30 days. If a tenant admin immediately issues a **permanent delete**, the user's account, personal data, and system-generated logs are expunged within 30 days of issuance.

[Important] You must be a tenant administrator to delete a user from the tenant.

Delete a user and associated data through the Azure portal

After you receive a delete request for a data subject, you can use the Azure portal to delete both a user and the associated personal information as well as system-generated logs.

Deleting this data also means deleting the user from the tenant. Users are initially soft-deleted, which means the account can be recovered by a tenant admin within 30 days of being marked for soft-delete. After 30 days, the account is automatically, and permanently, deleted from the tenant. Prior to that 30 days, you can manually delete a soft-deleted user from the recycle bin.

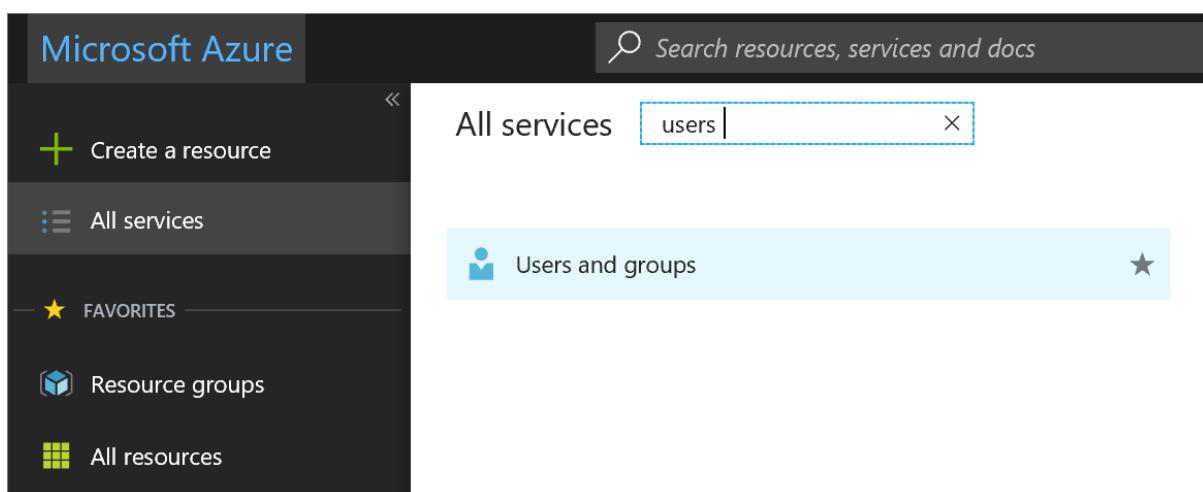
Here's the high-level process for deleting users from your tenant.

1. Go to the Azure portal and locate the user.
2. Delete the user. When you initially delete the user, the user's account is sent to the Recycle Bin.**At this point, the user is soft deleted, meaning the account is disabled, but not expunged from Azure Active Directory.**
3. Go to the Recently deleted users list and permanently delete the user.**At this point the user is permanently deleted (also known as hard deleted), meaning the account has been expunged from Azure Active Directory**

To delete a user from an Azure tenant

1. Open the Azure portal, select the **Azure Active Directory** blade, and then select **Users**.

The **Users – All users** blade appears.



2. Check the box next to the user you want to delete, select **Delete user**, and then select **Yes** in the box asking if you want to delete the user.

User management - Users
f128 Photography - PREVIEW

+ Add Columns Multi-Factor Au...

Resource groups
All resources
Recent
App Services
Virtual machines (classic)
Virtual machines
SQL databases
Cloud services (classic)
Security Center
Subscriptions
User management
Enterprise applications

Browse >

GENERAL

OVERVIEW

Audit

RESOURCES

Users (highlighted with a red box)

Groups

CONFIGURATION

Domains

Azure AD Connect

Settings

Password reset

NAME	USER NAME
Aaron Nicholls	tnich@f128.info
Abby Brennan	abrennan@f128.info
Adam Carlton	acarlton@f128.info
Adam Steenwyk	adam@f128.info
Adam Steenwyk	adam@f128.onmicrosoft.com
Adam Steenwyk (admin)	admin@f128.onmicrosoft.com
Adam Steenwyk (admin)	admin@f128.info
Adam Steenwyk (MSA)	ajamess_gmail.com#EXT#@f128.onmicrosoft.com
Adrian Martin	amartin@f128.info
Aidan Mitzner	amitzner@f128.info
Ajay Mokashi	amokashi@f128.info
Alain DuBois	adubois@f128.info
Alberto Bassani	abassani@f128.info
Alejandro Ruiz	aruiz@f128.info
Alex Grossman	agrossman@f128.info
Alice Gartner	alice@f128.info
Allison Hunter	ahunter@f128.info
Alvin Hwang	ahwang@f128.info
Amanda Baker	abaker@f128.info
Amanda Mackenzie	amackenzie@f128.info
Amelia Casias	acasias@f128.info

3. In the **Show** drop-down box, select **Recently deleted users**.

Home > contoso m365x764270 > Users - All users

Users - All users

contoso m365x764270 - Azure Active Directory

New user New guest user Reset password Delete user More

All users (highlighted with a blue box)

Deleted users

Password reset

User settings

ACTIVITY

Sign-ins

Audit logs

TROUBLESHOOTING + SUPPORT

Troubleshoot

New support request

Name

Show

All users

All users

Guest users only

Recently deleted users (highlighted with a blue box)

NAME	USER TYPE	SOURCE
Aarif Sherzai	Member	Azure Active Dir...
Achim Maier	Member	Azure Active Dir...
Adam Wallen	Member	Azure Active Dir...
Adele Vance	Member	Azure Active Dir...
Adriana Napolitani	Member	Azure Active Dir...
Aldo Muller	Member	Azure Active Dir...
Alex Wilber	Member	Azure Active Dir...
Alice Lucchese	Member	Azure Active Dir...
Alisha Guerrero	Member	Azure Active Dir...
Allan Deyoung	Member	Azure Active Dir...

4. Select the same user again, select **Delete permanently**, and then select **Yes** in the box asking if you're sure.

[Important]

Be aware that by clicking **Yes** you are permanently, and irrevocably, deleting the user and all associated data and system-generated logs. If you do this by mistake, you'll have to manually add the user back to the tenant.

The associated data and system-generated logs are non-recoverable.

The screenshot shows the 'Users - All users' page in the Azure Active Directory portal. On the left, there's a navigation sidebar with links like 'All users', 'Deleted users', 'Password reset', and 'User settings'. Below that are sections for 'ACTIVITY' (Sign-ins, Audit logs) and 'TROUBLESHOOTING + SUPPORT' (Troubleshoot, New support request). The main area has a search bar and buttons for 'Delete permanently', 'Restore user', 'Refresh', and 'Columns'. A modal dialog box is open, asking 'Permanently delete selected users? All data for this user will be irrevocably deleted.' with 'Yes' and 'No' buttons. A single user, 'Isabella Simonsen', is selected for deletion, with details like her name, email (isabella@M365x7642...), member status, and creation date (3/27/2018, 8:47:51 AM).

Service-Specific Interfaces

Microsoft provides the ability to discover Customer Data directly via pre-existing application programming interfaces (APIs) or user interfaces (UIs) for specific services. Details are described in the respective services' reference documentation, describing applicable CRUD (create, read, update, delete) operations.

Step 6: Export

The "right of data portability" allows a data subject to request a copy of their personal data in an electronic format (that's a "structured, commonly used, machine read-able and interoperable format") that may be transmitted to another data controller. Azure supports this by enabling your organization to export the data in the native JSON format, to your specified Azure Storage Container.

[Important] You must be a tenant administrator to export user data from the tenant.

Azure Active Directory

With respect to Customer Data, Microsoft offers both a portal and in-product experiences providing the enterprise customer's tenant administrator the capability to manage export requests for identifiable information about an end-user.

Service-Specific Interfaces

Microsoft provides the ability to discover Customer Data directly via pre-existing application programming interfaces (APIs) or user interfaces (UIs) for specific services. Details are described in the respective services' reference documentation, describing applicable CRUD (create, read, update, delete) operations.

Part 2: System-Generated Logs

Microsoft also provides you with the ability to access, delete and export certain system-generated logs associated with a user's use of Azure.

IMPORTANT

The ability to restrict or rectify system-generated logs is not supported. System-generated logs constitute factual actions conducted within the Microsoft cloud and diagnostic data, and modifications to such data would compromise the historical record of actions, increasing fraud and security risks.

Executing DSRs against System-Generated Logs

Microsoft provides the ability to access, delete, and export certain system-generated logs through the Azure Portal and also directly via programmatic interfaces or user interfaces for specific services. Details are described in the respective services' reference documentation.

IMPORTANT

Services supporting in-product DSRs require direct usage of the service's application programming interface (API) or user interface (UI). Consequently, execution of an in-product DSRs **must be done in addition to execution of a DSR within the Azure Portal in order to complete a full request for a given data subject. Please refer to specific services' reference documentation for further details.**

Step 1: Access

The tenant admin is the only person within your organization who can access system-generated logs associated with a particular user's use of Azure. The data retrieved for an access request will be provided in a machine-readable format and will be provided in files that will allow the user to know which services the data is associated with. As noted above, the data retrieved will not include data that may compromise the security of the service.

Azure Active Directory

Microsoft offers both a portal and in-product experiences providing the enterprise customer's tenant administrator the capability to manage access requests. Access requests will allow for access of the personal data of the user, including: (a) identifiable information about an end-user and (b) service-generated logs. The process is identical to that described in the Azure Active Directory section of Part 1, Step 2: Access.

Service-Specific Interfaces

Microsoft provides the ability to discover Customer Data directly via pre-existing application programming interfaces (APIs) or user interfaces (UIs) for specific services. Details are described in the respective services' reference documentation, describing applicable CRUD (create, read, update, delete) operations.

Step 2: Delete

The tenant admin is the only person within your organization who can execute a DSR delete request for a particular user within an Azure tenant.

Azure Active Directory

Microsoft offers both a portal and in-product experiences providing the enterprise customer's tenant administrator the capability to manage DSR delete requests. DSR delete requests follow the same as described in the Delete a user and associated data through the Azure portal section of Part 1, Step 5: Delete.

Service-Specific Interfaces

Microsoft provides the ability to discover Customer Data directly via pre-existing application programming interfaces (APIs) or user interfaces (UIs) for specific services. Details are described in the respective services' reference documentation, describing applicable CRUD (create, read, update, delete) operations.

Step 3: Export

The tenant admin is the only person within your organization who can access system-generated logs associated with a particular user's use of Azure. The data retrieved for an export request will be provided in a machine-readable format and will be provided in files that will allow the user to know which services the data is associated with. As noted above, the data retrieved will not include data that may compromise the security or stability of the service.

Export system-generated logs using the Azure portal

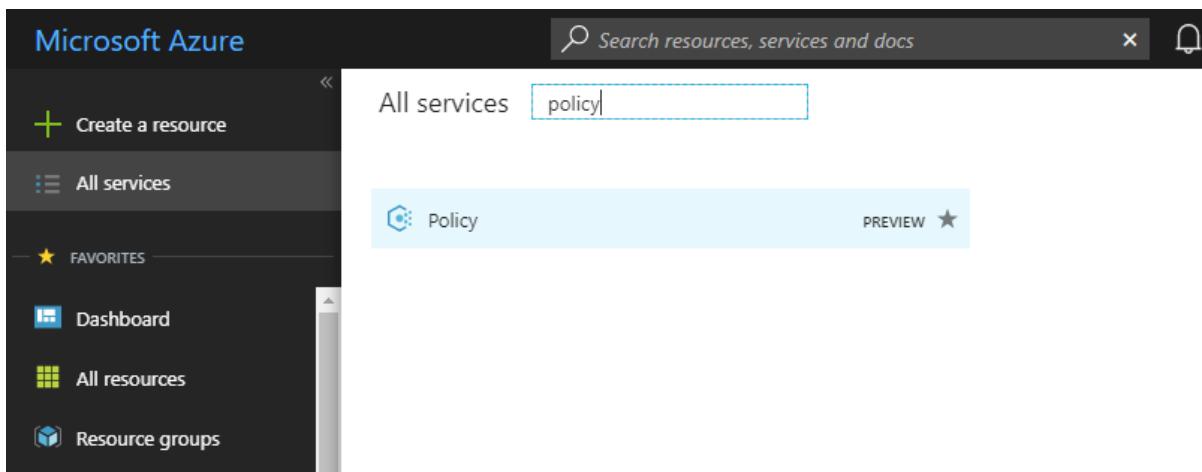
After you receive an export request for a data subject, you can use the Azure portal to export system-generated logs associated with a given user.

Here's the high-level process for exporting data from your tenant.

1. Go to the Azure portal and create an export request on behalf of the user.
2. Export the data and send file to user.

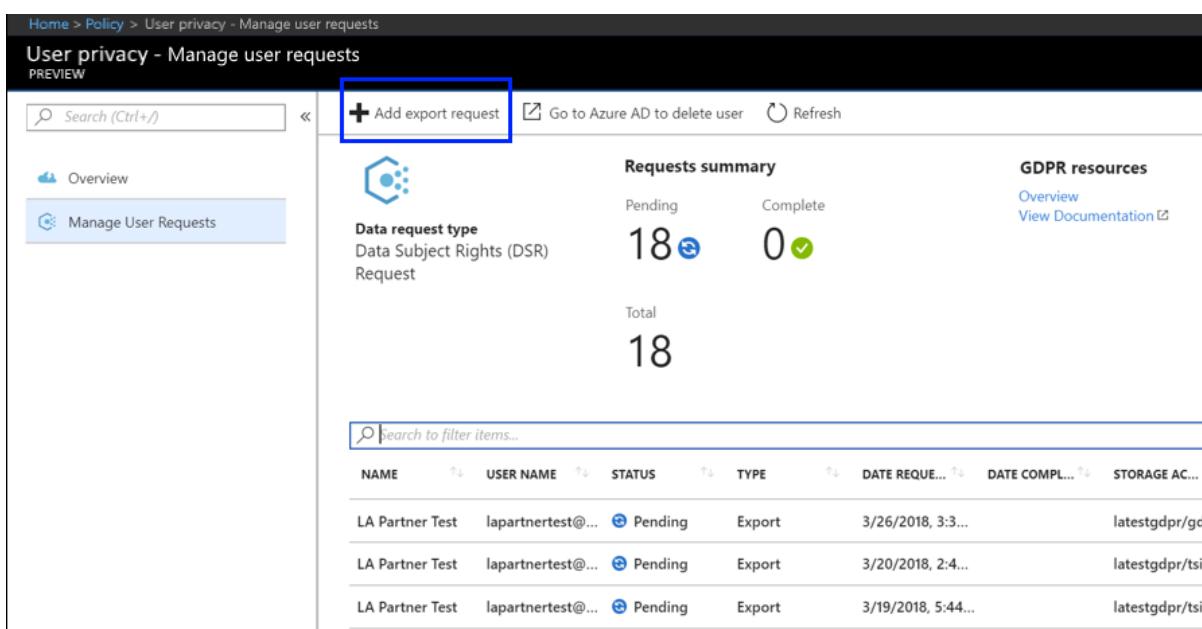
To export a user's info from an Azure tenant

1. Open the Azure portal, select **All services**, type *policy* into the filter, and then select **Policy**.



A screenshot of the Microsoft Azure portal. The left sidebar shows 'Create a resource', 'All services' (which is selected), 'FAVORITES' (Dashboard, All resources, Resource groups), and a preview of 'Policy'. The main search bar at the top has 'Search resources, services and docs' and contains the text 'policy'. Below the search bar, the 'All services' section is shown with a card for 'Policy' which includes a 'PREVIEW' button.

2. In the **Policy** blade, select **User privacy**, select **Manage User Requests**, and then select **Add export request**.



A screenshot of the 'User privacy - Manage user requests' blade in the Azure portal. The left sidebar shows 'Overview' and 'Manage User Requests' (which is selected). The main area has a 'Search (Ctrl+J)' bar, a 'Go to Azure AD to delete user' link, and a 'Refresh' button. A blue box highlights the '+ Add export request' button. To the right, there's a 'Requests summary' section with 'Pending' (18) and 'Complete' (0) counts, and a 'Total' count of 18. Below this is a table of user requests:

NAME	USER NAME	STATUS	TYPE	DATE REQUESTED	DATE COMPLETED	STORAGE AC...
LA Partner Test	lapartnerest@...	Pending	Export	3/26/2018, 3:3...		latestgdpr/gd...
LA Partner Test	lapartnerest@...	Pending	Export	3/20/2018, 2:4...		latestgdpr/tsit...
LA Partner Test	lapartnerest@...	Pending	Export	3/19/2018, 5:44...		latestgdpr/tsie...

3. Complete the **Export data request**:

New export data request

PREVIEW

Export all the data associated to a specific user from all subscriptions to a selected destination.

* User

Export destination
Select the subscription and storage account to export the data to

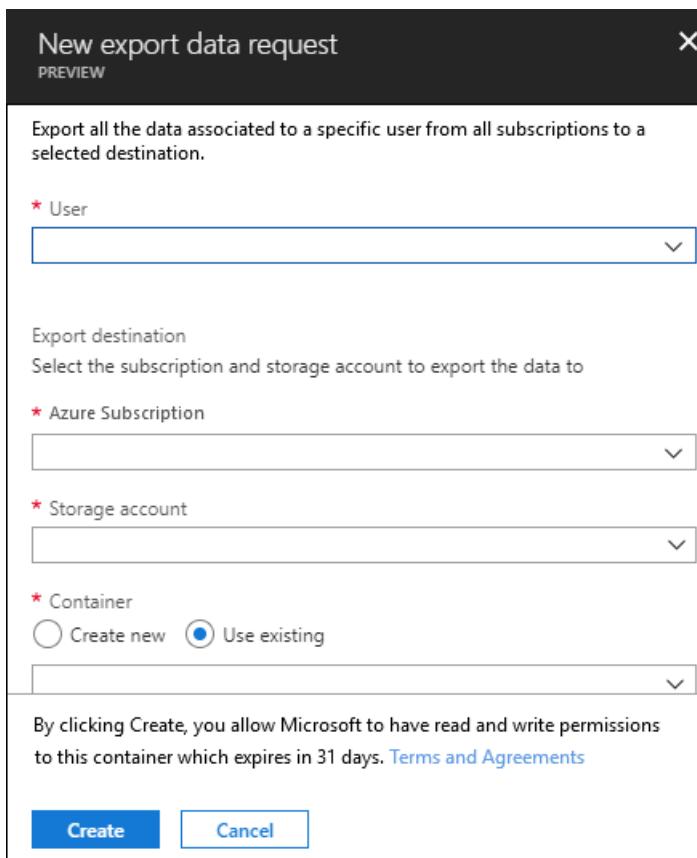
* Azure Subscription

* Storage account

* Container
 Create new Use existing

By clicking Create, you allow Microsoft to have read and write permissions to this container which expires in 31 days. [Terms and Agreements](#)

Create **Cancel**



- **User.** Type the email address of the Azure Active Directory user that requested the export.
- **Subscription.** Select the account you use to report resource usage and to bill for services. This is also the location of your Azure storage account.
- **Storage account.** Select the location of your Azure Storage (Blob). For more info, see the [Introduction to Microsoft Azure Storage – Blob storage](#) article.
- **Container.** Create a new (or select an existing) container as the storage location for the user's exported privacy data.

4. Select **Create**.

The export request goes into **Pending** status. You can view the report status on the **User privacy - Overview** blade.

[Important]

Because personal data can come from multiple systems, it's possible that the export process might take up to one month to complete.

Service-Specific Interfaces

Microsoft provides the ability to discover Customer Data directly via pre-existing application programming interfaces (APIs) or user interfaces (UIs) for specific services. Details are described in the respective services' reference documentation, describing applicable CRUD (create, read, update, delete) operations.

Notify about exporting or deleting issues

If you run into issues while exporting or deleting data from the Azure portal, go to the Azure portal **Help + Support** blade and submit a new ticket under **Subscription Management > Other Security and Compliance Request > Privacy Blade and GDPR Requests**.

[Learn more](#)

Intune Data Subject Requests for the GDPR

12/5/2018 • 9 minutes to read • [Edit Online](#)

The EU Data Protection Regulation (GDPR) gives rights to people (known in the regulation as *data subjects*) to manage the personal data that has been collected by an employer or other type of agency or organization (known as the *data controller* or just *controller*). Personal data is defined very broadly under the GDPR as any data that relates to an identified or identifiable natural person. The GDPR gives data subjects specific rights to their personal data; these rights include obtaining copies of personal data, requesting corrections to it, restricting the processing of it, deleting it, or receiving it in an electronic format so it can be moved to another controller. A formal request by a data subject to a controller to take an action on their personal data is called a *Data Subject Request* or DSR.

The guide discusses how to use Microsoft products, services, and administrative tools to help our controller customers find and act on personal data to respond to DSRs. Specifically, this includes how to find, access, and act on personal data that reside in the Microsoft cloud. Here's a quick overview of the processes outlined in this guide:

1. **Discover**—Use search and discovery tools to more easily find customer data that may be the subject of a DSR. Once potentially responsive documents are collected, you can perform one or more of the DSR actions described in the following steps to respond to the request. Alternatively, you may determine that the request doesn't meet your organization's guidelines for responding to DSRs.
2. **Access**—Retrieve personal data that resides in the Microsoft cloud and, if requested, make a copy of it that can be available to the data subject.
3. **Rectify**—Make changes or implement other requested actions on the personal data, where applicable.
4. **Restrict**—Restrict the processing of personal data, either by removing licenses for various Azure services or turning off the desired services where possible. You can also remove data from the Microsoft cloud and retain it on-premises or at another location.
5. **Delete**—Permanently remove personal data that resided in the Microsoft cloud.
6. **Export**—Provide an electronic copy (in a machine-readable format) of personal data to the data subject.

Each section in this guide outlines the technical procedures that a data controller organization can take to respond to a DSR for personal data in the Microsoft cloud.

Terminology

The following provides definitions of terms that are relevant to this guide.

- **Controller**—The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- **Personal data and data subject**—Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **Processor**—A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- **Customer Data**—All data, including all text, sound, video, or image files, and software, that are provided to

Microsoft by, or on behalf of, a customer through use of the enterprise service. Customer Data includes both (1) identifiable information of end users (e.g., user names and contact information in Azure Active Directory) and Customer Content that a customer uploads into or creates in specific services (e.g., customer content in an Azure Storage account, customer content of an Azure SQL Database, or a customer's virtual machine image in Azure Virtual Machines).

- **System-Generated Logs**—Logs and related data generated by Microsoft that help Microsoft provide enterprise services to users. System-generated logs contain primarily pseudonymized data, such as unique identifiers – typically a number generated by the system that cannot on its own identify an individual person but is used to deliver the enterprise services to users. System-generated logs may also contain identifiable information about end users, such as a user name.

How to use this guide

This guide consists of two parts:

Part 1: Responding to Data Subject Requests for Customer Data — Part 1 of this guide discusses how to access, rectify, restrict, delete, and export data from applications in which you have authored data. This section details how to execute DSRs against both Customer Content and also identifiable information of end users.

Part 2: Responding to Data Subject Requests for System-Generated Logs — When you use Microsoft's enterprise services, Microsoft generates some information, known as System-Generated Logs, in order to provide the service. Part 2 of this guide discusses how to access, delete and export such information for Azure.

Understanding DSRs for Azure Active Directory and Microsoft Intune

When considering services provided to enterprise customers, execution of DSRs must always be understood within the context of a specific Azure Active Directory (AAD) tenant. Notably, DSRs are always executed within a given AAD tenant. If a user is participating in multiple tenants, it is important to emphasize that a given DSR is *only* executed within the context of the specific tenant the request was received within. This is critical to understand as it means the execution of a DSR by one enterprise customer **will not** impact the data of an adjacent enterprise customer.

The same also applies for Microsoft Intune provided to an enterprise customer: execution of a DSR against an Intune account *associated with an AAD tenant* **will only** pertain to data within the tenant. In addition, it is important to understand the following when handling Intune accounts within a tenant:

- If an Intune user creates an Azure subscription, the subscription will be handled as if it were an AAD tenant. Consequently, DSRs are scoped within the tenant as described above.
- If an Azure subscription created via an Intune account is deleted, **it will not affect** the actual Intune account. Again, as noted above, DSRs executing within the Azure subscription are limited to the scope of the tenant itself.

DSRs against an Intune account itself, **outside a given tenant**, are executed via the Consumer Privacy Dashboard. Please refer to the Windows Data Subject Request Guide for further details.

Part 1: DSR Guide for Customer Data

Executing DSRs against Customer Data

Microsoft provides the ability to access, delete, and export certain Customer Data through the Azure Portal and also directly via pre-existing application programming interfaces (APIs) or user interfaces (UIs) for specific services (also referred to as *in-product experiences*). Details regarding such in-product experiences are described in the respective services' reference documentation.

IMPORTANT

Services supporting in-product DSRs require direct usage of the service's application programming interface (API) or user interface (UI), describing applicable CRUD (create, read, update, delete) operations. Consequently, execution of DSRs within a given service must be done in addition to execution of a DSR within the Azure Portal in order to complete a full request for a given data subject. Please refer to specific services' reference documentation for further details.

Step 1: Discover

The first step in responding to a DSR is to find the personal data that is the subject of the request. This first step - finding and reviewing the personal data at issue - will help you determine whether a DSR meets your organization's requirements for honoring or declining a DSR. For example, after finding and reviewing the personal data at issue, you may determine the request doesn't meet your organization's requirements because doing so may adversely affect the rights and freedoms of others.

After you find the data, you can then perform the specific action to satisfy the request by the data subject. For details, see the following:

- [Data collection](#)
- [Data storage and processing](#)
- [View personal data](#)

Step 2: Access

After you've found Customer Data containing personal data that is potentially responsive to a DSR, it is up to you and your organization to decide which data to provide to the data subject. You can provide them with a copy of the actual document, an appropriately redacted version, or a screenshot of the portions you have deemed appropriate to share. For each of these responses to an access request, you will have to retrieve a copy of the document or other item that contains the responsive data.

When providing a copy to the data subject, you may have to remove or redact personal information about other data subjects and any confidential information.

The following explains how to get a copy of data in response to a DSR access request.

Azure Active Directory

Microsoft offers both a portal and in-product experiences providing the enterprise customer's tenant administrator the capability to manage DSR access requests. DSR Access requests allow for access of the personal data of the user, including: (a) identifiable information about an end-user and (b) system-generated logs.

Service-Specific Interfaces

Microsoft Intune provides the ability to [discover Customer Data](#) directly via user interfaces (UIs) or pre-existing application programming interfaces (APIs).

Step 3: Rectify

If a data subject has asked you to rectify the personal data that resides in your organization's data, you and your organization will have to determine whether it's appropriate to honor the request. Rectifying the data may include taking actions such as editing, redacting, or removing personal data from a document or other type or item.

As a data processor, Microsoft does not offer the ability to correct system-generated logs as it reflects factual activities and constitutes a historical record of events within Microsoft services. With respect to Intune, admins can't update device or app specific information. If an end user wants to correct any personal data (like the device name), they must do so directly on their device. Such changes are synchronized the next time they connect to Intune.

Step 4: Restrict

Data subjects may request that you restrict processing of their personal data. We provide both the Azure Portal and pre-existing application programming interfaces (APIs) or user interfaces (UIs). These experiences provide the

enterprise customer's tenant administrator the capability to manage such DSRs through a combination of data export and data deletion. For details, see [Processing personal data](#).

Step 5: Delete

The "right to erasure" by the removal of personal data from an organization's Customer Data is a key protection in the GDPR. Removing personal data includes removing all personal data and system-generated logs, except audit log information. For details, see [Delete end user personal data](#).

Part 2: System-Generated Logs

Audit logs provide tenant admins with a record of activities that generate a change in Microsoft Intune. Audit logs are available for many manage activities and typically create, update (edit), delete, and assign actions. Remote tasks that generate audit events can also be reviewed. These audit logs may contain personal data from users whose devices are enrolled in Intune. Admins can't delete audit logs. For details, see [Audit personal data](#).

Notify about exporting or deleting issues

If you run into issues while exporting or deleting data from the Azure portal, go to the Azure portal **Help + Support** blade and submit a new ticket under **Subscription Management > Other Security and Compliance Request > Privacy Blade and GDPR Requests**.

[Learn more](#)

[Microsoft Trust Center](#)

Dynamics 365 Data Subject Requests for the GDPR

2/22/2019 • 28 minutes to read • [Edit Online](#)

The EU Data Protection Regulation (GDPR) gives rights to people (known in the regulation as *data subjects*) to manage the personal data that has been collected by an employer or other type of agency or organization (known as the *data controller* or just *controller*). Personal data is defined broadly under the GDPR as any data that relates to an identified or identifiable natural person. The GDPR gives data subjects specific rights to their personal data; these rights include obtaining copies of it, requesting changes to it, restricting the processing of it, deleting it, or receiving it in an electronic format so it can be moved to another controller. A formal request by a data subject to a controller to take an action on their personal data is called in this document a *Data Subject Rights Request* or DSR request.

The guide discusses how to use Microsoft's products, services and administrative tools to help our controller customers find and act on personal data to respond to DSR requests. Specifically, this includes how to find, access, and act on personal data that reside in Microsoft's cloud. Here's a quick overview of the processes outlined in this guide:

1. **Discover**—Use search and discovery tools to more easily find customer- data that may be the subject of a DSR request. Once potentially responsive documents are collected, you can perform one or more of the DSR actions described in the following steps to respond to the request. Alternatively, you may determine that the request doesn't meet your organizations guidelines for responding to DSR requests.
2. **Access**—Retrieve personal data that resides in the Microsoft cloud and, if requested, make a copy of it that can be available to the data subject.
3. **Rectify**—Make changes or implement other requested actions on the personal data, where applicable.
4. **Restrict**—Restrict the processing of personal data, either by removing licenses for various online services or turning off the desired services where possible. You can also remove data from the Microsoft cloud and retain it on-premises or at another location.
5. **Delete**—Permanently remove personal data that resided in Microsoft's cloud.
6. **Export**—Provide an electronic copy (in a machine-readable format) of personal data to the data subject.

Each section in this guide outlines the technical procedures that a data controller organization can take to respond to a DSR request for personal data in Microsoft's cloud

GDPR terminology

The following provides definitions of terms that are relevant to this guide:

- **Controller**—The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- **Personal data and data subject**—Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **Processor**—A natural or legal person, public authority, agency or other body which processes personal data

on behalf of the controller.

- *Customer Data* – All data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, a customer through use of the enterprise service, as defined in the Microsoft Online Services Terms.
- *System-Generated Logs* – Logs and related data generated by Microsoft that help Microsoft provide the enterprise services to users. System-generated logs contain primarily pseudonymized data, such as unique identifiers – typically a number generated by the system that cannot on its own identify an individual person but is used to deliver the enterprise services to users. System-generated logs may also contain identifiable information about end users, such as a user name.

How this guide can help you meet your controller responsibilities

The guide, divided into two parts, describes how to use Dynamics 365 products, services, and administrative tools to help you find and act on data in the Microsoft cloud in response to requests by data subjects who are exercising their rights under the GDPR. The first part addresses personal data that is included in Customer Data, followed by a part addressing other pseudonymized personal data captured in System-Generated Logs.

Part 1: Responding to Data Subject Rights (DSR) requests for Personal Data included in Customer Data.

Part 1 of this guide discusses how to access, rectify, restrict, delete, and export personal data from Dynamics 365 applications (software as a service), which is processed as part of the Customer Data you have provided to the online service.

Part 2: Responding to data subject rights requests for Pseudonymized Data. When you use Dynamics 365 enterprise services, Microsoft generates some information (referred to within this document as *system-generated logs*) to provide the service, which is limited to the usage footprint left behind by end users to identify their actions in the system. Although this data cannot be attributed to a specific data subject without the use of additional information, some of it may be deemed personal under the GDPR. Part 2 of this guide discusses how to access, delete, and export system-generated logs produced by Dynamics 365.

Preparing for data subject rights investigations

When data subjects exercise their rights and make requests, consider the following points:

- Properly identify the person and role—such as employee, customer, vendor—by using information that the data subject gave you as part of his or her request. This information might be a name, an employee ID or customer number, or other identifier.
- Record the data and time of the request. (You have 30 days to complete the request.)
- Affirm that the request meets your organization's requirements for honoring or declining a data subject's request. For example, you must make sure that executing the request doesn't conflict with any other legal, financial, or regulatory obligations that you have, or infringe on the rights and freedoms of others.
- Verify that you have the information that is related to the request.

Part 1: Responding to Data Subject Rights Requests for Personal Data Included in Customer Data

In the articles below, you'll find information to help you prepare for and respond to DSR requests for personal data included in Customer Data processed in Dynamics 365. It is important to note that personal data could be present in other categories of data processed by Microsoft during the course of the service of an online services subscription, such as administrator data or support data defined in the Microsoft Privacy Statement. This document is limited to assist you in the process of discovery and management of DSR requests affecting personal data present in the Customer Data that you have provided to Dynamics 365.

Dynamics 365 is an online service that offers multiple data processing capabilities as a software-as-a-service

(SaaS). As such, Dynamics 365 offers a broad array of functionality intended to process a diverse collection of data, which could vary by nature, purpose or other specific attributes, such as sales data, transactions, financials, HR information, etc. In light of this diversity, Dynamics 365 offers multiple forms, fields, schemas, end points, and logic to process Customer Data, which is also reflected in the multiple ways in which DSR requests could be addressed in each application. When Dynamics 365 applications offer several ways to address specific DSR requests, we will note those in this guide by pointing to the technical descriptions offered by each application.

Microsoft Dynamics 365

Finding customer data

The first step in responding to a data subject rights request is to search for and identify the Customer Data that is the subject of the request.

Classifying Customer Data appropriately is the cornerstone of working with personal data in Microsoft Dynamics 365 Customer Engagement. Dynamics 365 for Customer Engagement offers flexibility to build out an application extension around data classification. Proper classification enables you to identify information as personal data, thereby making it possible to locate and retrieve it when responding to requests from a data subject. It can also help enable compliance with legislative and regulatory requirements for collecting and managing personal data.

Microsoft provides capabilities that can assist you in responding to data subject rights requests, and thereby accessing Customer Data. However, it is your responsibility to ensure that personal data is located and classified appropriately.

Dynamics 365 for Customer Engagement provides multiple methods for you to search for personal data within records such as: Advanced Find Search, Relevance Search, and Search for Records. These functions all enable you to identify (find) personal data.

- [Advanced Find Search](#)
- [Relevance Search](#), which can be saved for future reference using dashboards Relevance search, which can be saved for future reference using dashboards
- [Search for Records](#) across multiple record types

In Dynamics 365 for Marketing, you have the following additional capabilities:

1. [Build Power BI reports](#) in order to filter and identify customer data.
2. Utilize the Insight Views on contacts and objects of marketing execution to identify additional data points that may contain customer data.

Dynamics 365 Finance and Operations provides several ways for you to search for Customer Data. You as a Tenant Admin can perform the following actions to search for Customer Data:

- Organize your Customer Data in a way that serves the purpose of rapidly discovering personal data, see [how to classify data inventory](#) for this purpose.
- Use the [Person search report](#) to find and collect personal data.
- [Extend the Person search report](#) by authoring a new entity or extending an existing entity.
- Use search and filter features to find specific personal data and export that data by using the Microsoft Office Export functionality or print that information to a .pdf using browser extensions.
- Author a custom form that locates and exports personal data.
- Author an external portal or website that allows an authenticated customer to see his or her personal data.

Dynamics for Business Central provides several ways for you to search for Customer Data. For details, see [Searching, filtering, and sorting data](#).

Dynamics 365 for Talent provides advanced search and filter features to find specific personal data and Microsoft Office Export functionality to export or print that information to a .pdf using browser extensions.

- Use the [Person search report](#) to find and collect Customer Data.
- Extend the [Person search report](#) by authoring a new entity or extending an existing entity.

Providing a copy of customer data

Customer Data in **Dynamics 365 for Customer Engagement** can be exported using the comprehensive entity export capabilities. Customer data can be exported to a static Excel file to facilitate a data portability request. Using Excel, you can then edit the personal data to be included in the portability request and then save as a commonly used, machine-readable format such as .csv or .xml.

Additionally, for Dynamics 365 for Marketing a [dedicated API](#) is provided that allows customer to build extensions that retrieve additional records of captured customer interactions that may contain personal data. The API loads all the relevant information from the back-end system and assembles it into a single, portable document.

Customer Data in **Dynamics 365 for Finance and Operations** can be exported using the comprehensive entity export capabilities. Using [Data management and integration entities](#), the Tenant Admin may utilize provided entities, create new, or extend existing, entities for a repeatable personal data export to Excel or a number of other common formats using [Data import and export jobs](#). Alternatively, many lists can be exported to a static Excel file to facilitate a data portability request. When customer data is exported to Excel, you can then edit the personal data to be included in the portability request and then save the file as a commonly used, machine-readable format such as .csv or .xml. You may also consider using the *Person Search Report *to provide the data subject with data that you've classified as personal data.

In **Dynamics 365 Business Central**, you can make use of two features to provide a copy of Customer Data to a data subject:

You can export Customer Data to an Excel file. In Excel, you can then edit the Customer Data to be included in the portability request, and save it in a commonly used, machine-readable format, such as .csv or .xml. For details, see [Exporting your business data to Excel](#).

In **Dynamics 365 for Talent**, you may use [Extend the Person search report](#) to gather information in support of a request for a copy of the data subject's personal data.

Rectifying customer data

Dynamics 365 for Customer Engagement gives you following methods for correcting inaccurate or incomplete customer data, or erasing customer data:

- Search for Customer Data using the capabilities mentioned in "Finding Customer Data" and directly edit data in Customer Engagement Forms. Edits can be done at a single row level or multiple rows can be modified directly.
- Bulk editing multiple Customer Engagement records, you can utilize the Microsoft Office add-in to export data to Microsoft Excel, make your changes, and then import that modified data from Excel into Dynamics 365 for Customer Engagement.

Additionally, for Dynamics 365 for Marketing you can also:

- Update-my-data landing page, by editing single or multiple rows directly
- Prepare a [subscription centers](#) page that has as many editable contact fields that can be included. This enables an end user to update their own information as much as possible.

In **Dynamics 365 for Finance and Operations**, you may also use of [customization tools](#), but the decision and implementation is your responsibility.

Dynamics 365 Business Central offers two ways to correct inaccurate or incomplete Customer Data.

To quickly bulk-edit multiple Business Central records, you can export lists to Excel using the [Business Central Excel Add-in](#) to correct multiple records, and then publish the modified data from Excel in Business Central. For details, see [Exporting your Business Data to Excel](#).

- You can change Customer Data stored in any field—such as information about a customer in the Customer card —by manually editing the data element containing the target personal data. For details, see [Entering data](#).

Brief note about modifying entries in business transactions

Transactional records, such as general, customer, and tax ledger entries, are essential to the integrity of an enterprise resource planning system. Personal data that is part of a financial or other transaction is kept "as is" for compliance with financial laws (for example, tax laws), prevention of fraud (such as security audit trail), or compliance with industry certifications. Therefore, Dynamics 365 for Finance and Operations and Dynamics 365 Business Central restrict modifying data in such records.

If you store personal data in business transaction records, the only way to correct, delete, or restrict processing of personal data to honor a data subject's request is to use the Dynamics 365 Business Central [customization capabilities](#). The decision to honor a modification data subject request and implementation thereof is your responsibility.

Restricting the processing of Customer Data

When you receive a request from a data subject to restrict processing of Customer Data, you can easily extract the affected Customer Data from the online service and store it in a separate container (i.e. on-premise storage or separate web service with data isolation capabilities) isolated from the processing functions offered by any cloud application.

Alternative mechanism such as data processing block is offered by **Dynamics 365 Business Central**, where users are offered the ability to block specific data subject's record. For details, see [Restrict data processing for a data subject](#). When a record is marked as blocked, Dynamics 365 Business Central will discontinue processing the Customer Data of that data subject. You cannot create new transactions that use a blocked record; for example, you cannot create a new invoice for a customer, when either the customer or salesperson is blocked.

Deleting customer data

When a data subject asks you to delete their Customer Data, there are several ways to do so:

- Bulk editing multiple Dynamics 365 records, you can utilize the Microsoft Office add-in to export data to Microsoft Excel, make your changes, and then import that modified data from Excel back into the online service.
- You can delete Customer Data stored in any field by locating the data you want to delete and then manually deleting the data element containing the target customer data, for example like employing a hard delete on the contact record representing the data subject and other records that contain personal data

Additionally, For Dynamics 365 Marketing, deletion of a contact will assure that interaction data with personal information will be removed as well. For any custom fields or entities, you must customize your system to make sure it deletes all Customer Data from related records and/or unlinks them from the contact record so that all personal information is removed. More information: [Developer Guide \(Marketing\)](#).

Alternatively, in **Dynamics 365 for Finance and Operations** you may use [customization tools](#) to erase/modify Customer Data.

In **Dynamics 365 Business Central**, when a data subject asks you to delete their personal data which happens to be included in your Customer Data, there are several ways to address this request:

- To quickly bulk-edit multiple Business Central records, you can export data to Excel using the [Business Central Excel Add-in](#) to delete multiple records, and then publish these changes from Excel back in Business

Central. For details, see [Exporting your Business Data to Excel](#).

- You can delete Customer Data stored in any field by manually deleting the data element containing the target Customer Data. For details, see [Entering data](#).
- You can directly delete Customer Data, for example by deleting a contact and then running the Delete Canceled Interaction Log Entries batch job to delete interactions for that contact.
- You can [delete documents](#) containing Customer Data—for example, memos and posted sales and purchase invoices.

Besides bulk or individual deletion of discrete records, please note that only terminated workers can be fully deleted from **Dynamics 365 for Talent**. Follow these steps to delete terminated workers.

Exporting customer data

To respond to a data portability request, Customer Data in **Dynamics 365 for Customer Engagement** can be exported using the comprehensive entity export capabilities. Customer data can be exported to a static Excel file to facilitate a data portability request. Using Excel, you can then edit the personal data to be included in the portability request and then save as a commonly used, machine-readable format such as .csv or .xml.

Additionally, for Dynamics 365 for Marketing a [dedicated API](#) is provided that allows customer to build extensions that retrieve additional records of captured customer interactions that may contain personal data. The API loads all the relevant information from the back-end system and assembles it into a single, portable document.

Dynamics 365 for Finance and Operations offers [Data management and integration entities](#) which enables provided entities, newly created entities, or extended entities for a repeatable personal data export to Excel or a number of other common formats using [Data import and export jobs](#). Alternatively, many lists can be exported to a static Excel file to facilitate a data portability request. When Customer Data is exported to Excel in this fashion, you can then edit the personal data to be included in the portability request and then save the file as a commonly used, machine-readable format such as .csv or .xml.

Both Dynamics 365 for Finance and Operations and **Dynamics 365 for Talent** offer Person Search Report to provide the data subject with data that you've classified as personal data.

- **Dynamics 365 Business Central** offers the following features,
- You can export Customer Data to an Excel file. In Excel, you can then edit the Customer Data to be included in the portability request, and save it in a commonly used, machine-readable format, such as .csv or .xml. For details, see [Exporting your business data to Excel](#).

You can export Customer Data to an Excel file. In Excel, you can then edit the Customer Data to be included in the portability request, and save it in a commonly used, machine-readable format, such as .csv or .xml. For details, see [Exporting your business data to Excel](#).

Microsoft Social Engagement

As Microsoft Social Engagement processes personal data which could be found in Customer Data and Social Content, this application offers a unique way to address DSR requests as it relates to personal data retrieved from social networks. Social Content is publicly-available content collected from social media networks (such as Twitter, Facebook and YouTube) and data indexing or data aggregation services in response to Customer's search queries executed in Microsoft Social Engagement. Social Content is not Customer Data. Further restrictions on processing, usage and storage of Social Content are described in the Microsoft Online Service Terms.

Finding personal data

The first step in responding to a data subject's request is to search for and identify the personal data that is the subject of that request. Microsoft Social Engagement stores following data:

For social media users

- Social media user data (referred to as *author* in Social Engagement) that Social Engagement acquires from social platforms. It could include the name, user name, profile picture, location, website, and bio if it is provided by the author.
- Author tags used by Social Engagement employees to group and classify authors—for example, as influencers, competitors, or fans.

For employees

- User profiles that include employee name, contact information, and profile picture and are managed in Office 365.
- Email addresses provided by employees who have created post alerts and trend alerts.
- Social media accounts (referred to as *social profiles* in Social Engagement) that are authenticated in Social Engagement by employees to engage with others on a social platform. They may be owned by an employee or by the organization and include data that employees provide when they register an account on a social platform. These profiles represent the organization on social media and are used to interact with posts on the organization's behalf from within the Social Engagement application.
- User names in Power BI if your organization uses the [Social Engagement content pack](#) for Power BI to analyze team performance on social media.

This first step—finding and reviewing the personal data at issue—will help you determine whether the data subject's request meets your organization's requirements for honoring or declining it. For example, after finding and reviewing the personal data, you may determine the request doesn't meet your organization's requirements because doing so may adversely affect the rights and freedoms of others.

Social media users (authors)

- To find their personal data, follow the first four steps in [Find and delete an author](#).
- Employees can create Social Engagement rules that search on social platforms for certain defined content; these search rules may contain author names. To make sure that you find these rules, review the social account search rules for the appropriate account such as [Twitter](#), [Instagram](#), and [YouTube](#).
- To find author tags for an author, first [filter posts by author](#), and then [view author tags](#).

Your employees

To find:

- A user profile, go to the [Office 365 admin center](#). In the **Admin center**, select **Users**. On the **Active Users** page, search for the user on the list.
In Social Engagement, go to **Settings > User management** to see information that is automatically synced from Office 365.
- The recipient of an alert, follow the first two steps in [Manage alert recipients as administrator](#).
- Social profile data that has been entered by employees, go to **Settings > Social profiles**. (For more information, see [Manage social profiles](#).)
- User names in Power BI, open the Social Engagement Power BI dashboard and filter by the employee name.

Providing a copy of personal data

The GDPR gives data subjects the right to get a copy of personal data upon request. After you've found customer content containing data that is potentially responsive to the request, it is up to you and your organization to decide whether to provide the data subject with a copy.

Social media users (authors)

- To export personal data of authors, follow the steps in [Export author information](#) to export the data to an Excel file.

- To extract the author tags that were added to a specific author, you can [export author tag data](#).

Your employees

To export:

- Customer Data from user profiles, go to the [Office 365 admin center](#). In the **Admin center**, select **Users**. On the **Active Users** page, search for the user whose data you wish to export. Delete all users except the target user, and then select **Export** to export the data to a .csv file where you can use Excel to view the information.
- Email addresses of an alert recipient (the only Customer Data in an alert). follow the steps in [Manage alert recipients as administrator](#). Then select **Export** to download an Excel list of the alerts that include this recipient.
- User names from Power BI: [Engagement reporting](#) shows user names in reports of team performance on social media. To export this data, filter by the user in the PowerBI dashboard or [report](#), and [export the data](#).

Rectifying personal data

To correct inaccurate or incomplete personal data:

Social media users (authors)

- You must ask the data owner (author) to make the change on the social platform (such as Twitter, WordPress, or Tumblr). The data subject owns the data in the social media account, so they are the only ones who can change it. Once the author makes the change, Social Engagement syncs the revised details automatically.
- Author tags, follow the steps in [Change author tags](#).

Your employees

- User profiles: To make changes to the Customer Data in a user profile, see [Change a user name and email address in Office 365](#) and [Add your profile photo to Office 365](#). These changes are synced automatically in Social Engagement. To find them, go to **Settings > User management**.
- Alert recipients: You can [change an alert](#).

Restricting the processing of personal data

Social media users (authors)

To stop processing the Customer Data of authors in Social Engagement, [delete the author](#).

This will block future processing of the data of this data subject and any future posts, as well as delete all data about and by this author. Whenever Social Engagement acquires new posts, it automatically checks if the author was deleted earlier and discards posts from deleted authors. This has no effect on the user's account on the social platform.

Your employees

- To stop processing the Customer Data of employees, you can [remove their license](#) in Office 365. This deletes all Social Engagement-related items such as user roles and profiles, all related user-defined custom settings, alerts, activity maps, and streams. Search topics and social profiles are not deleted; however, administrators inherit ownership of the social profiles of deleted users and can delete them on request.
- To restrict sending alert email messages, you can remove an email address from all the alerts it's been added to by following the steps in [Manage alert recipients as an administrator](#).

Deleting personal data

GDPR gives data subjects the right to request from the controller the deletion of personal data in certain circumstances. The "right to be forgotten" by removing such data from an organization is a key protection in the GDPR.

Social media users (authors)

To permanently delete all of an author's personal data in Social Engagement, delete the complete social profile of this author. See [Delete an author](#).

Once you do this, there is no way to undo it. This will delete all data about and by this author on Social Engagement, and will block future processing of their data and any future posts. Whenever Social Engagement acquires new posts, it automatically checks if the author was deleted earlier and discards posts from deleted authors. This has no effect on the user's account on the social platform.

To delete author tags, see [Remove author tags](#).

[Note] If you are asked to remove information about a specific author, we recommend that you first confirm the identity of that author to validate the request. To confirm their identity, you can request a private message from the author from their social media account.

Social Engagement has implemented compliance feeds from several social platforms (such as Twitter, WordPress, Tumblr) to act on signals like post deletions that were triggered on the social platforms directly. This feature is automatically activated with every Social Engagement installation and does not require any user interaction. Additionally, Social Engagement provides a mechanism that allows services (like Dynamics 365 for Customer Engagement) that build on social content from Social Engagement to inherit these signals.

Your employees

To permanently delete all of an employee's Customer Data, you can [remove their license](#) in Office 365.

- This deletes all Social Engagement-related items such as user roles and profiles, all related user-defined custom settings, alerts, activity maps, and streams. Search topics and social profiles are not deleted. (Administrators inherit ownership of the social profiles of deleted users and can delete them on request.)
- These changes are synced automatically in Social Engagement. To find them, go to **Settings > User management**.
- The employee entries in a PowerBI engagement report are anonymized when their personal data is deleted.

You can [delete a social profile](#).

To delete an email address from all alerts it's been added to, follow the steps in [Manage alert recipients as an administrator](#).

Exporting personal data

You can provide data subjects with their personal data in an electronic format.

Social media users (authors)

To export the personal data of authors, follow the steps in [Export author information](#) to export the data to an Excel file.

To extract the author tags that were added to a specific author, you can [export author tag data](#).

Your employees

To export:

- Customer Data from user profiles, go to the [Office 365 admin center](#). In the **Admin center**, select **Users**. On the **Active Users** page, search for the user whose data you wish to export. Delete all users except the target user, and then select **Export** to export the data to a .csv file where you can use Excel to view the information.
- Email addresses of an alert recipient (the only personal data in an alert). Follow the steps in [Manage alert recipients as administrator](#). Then select **Export** to download an Excel list of the alerts that include this recipient.
- User names from Power BI: [Engagement reporting](#) shows user names in reports of team performance on social media. To export this data, filter by the user in the PowerBI dashboard or [report](#), and [export the data](#)

Part 2: Responding to DSRs for system-generated logs

Microsoft also provides you with the ability to access, export, and delete system-generated logs that may be deemed personal under the GDPR's broad definition of "personal data." Examples of system-generated logs that may be deemed personal under GDPR include:

- Product and service usage data such as user activity logs
- User search requests and query data
- Data generated by product and services as a product of system functionality and interaction by users or other systems

Note that the ability to restrict or rectify data in system-generated logs is not supported. Data in system-generated logs constitutes factual actions conducted within the Microsoft cloud and diagnostic data, and modifications to such data would compromise the historical record of actions and increase fraud and security risks.

Accessing and exporting system-generated logs

Admins can access system-generated logs associated with a particular user's use of Dynamics 365 services and applications. To access and export system-generated logs:

1. Go to the [Microsoft Service Trust Portal](#) and sign in using the credentials of an Dynamics 365 global administrator.
2. In the **Privacy** drop-down list at the top of the page, click **Data Subject Request**.
3. On the **Data Subject Request** page, under **System Generated Logs**, click **Data Log Export**.

The **Data Log Export** is displayed. Note that a list of export data requests submitted by your organization is displayed.

4. To create a new request for a user, click **Create Export Data Request**.

After you create a new request, it will be listed on the **Data Log Export** page where you can track its status. After a request is complete, you can click a link to access the system-generated logs, which will be exported to your organization's Azure storage location within 30 days of creating the request. The data will be saved in common, machine-readable file formats such as JSON or XML. If you don't have an Azure account and Azure storage location, you'll need to create an Azure account and/or Azure storage location for your organization so that the Data Log Export tool can export the system-generated logs.

Azure supports this by enabling your organization to export the data in the native JSON format, to your specified Azure Storage Container. [Introduction to Microsoft Azure Storage – Blob storage](#) article.

Important: You must be a tenant administrator to export user data from the tenant.

The following table summarizes accessing and exporting system-generated logs:

How long does the Microsoft Data Log Export tool take to complete a request?	This can depend on several factors. In most cases it should complete in one or two days, but it can take up to 30 days.
What format will the output be in?	The output will be structured machine-readable files such as XML, CSV, or JSON.
What data does the Data Log Export tool return?	The Data Log Export tool returns system generated logs that Microsoft stores. Exported data will span across various Microsoft services including Office 365, Azure and Dynamics.

Who has access to Data Log Export tool to submit access requests for system-generated logs?	Dynamics 365 global administrators will have access to the GDPR Log Manager utility.
How is data returned to the user?	Data will be exported to your organization's Azure storage location; it will be up to admins in your organization to determine how they will show/return this data to users.
What will data in system-generated logs look like?	<p>Example of a system-generated log record in JSON format:</p> <pre>[{ "DateTime": "2017-04-28T12:09:29-07:00", "AppName": "SharePoint", "Action": "OpenFile", "IP": "154.192.13.131", "DevicePlatform": "Windows 1.0.1607" }]</pre>

[Note] Some features will not allow for the export or deletion of system-generated logs with personal information to maintain the integrity of such information for security and audit reasons.

Deleting system-generated logs

To delete system-generated logs retrieved through an access request, you must remove the user from the service and permanently delete their Azure Active Directory account. For instructions about permanently delete a user, see the [Deleting a user](#) section in this guide. It's important to note that permanently deleting a user account is irreversible once initiated.

Permanently deleting a user account will remove the user's data from system-generated logs for nearly all Dynamics 365 services within 30 days.

[Learn more](#)

[Microsoft Trust Center](#)

Visual Studio Family Data Subject Requests for the GDPR

2/8/2019 • 10 minutes to read • [Edit Online](#)

The European Union [General Data Protection Regulation \(GDPR\)](#) gives rights to people (known in the regulation as *data subjects*) to manage their personal data. Personal data is defined very broadly under the GDPR as any data that relates to an identified or identifiable natural person. The GDPR gives data subjects specific rights to their personal data; these rights include obtaining copies of personal data, requesting corrections to it, restricting the processing of it, deleting it, or receiving it in an electronic format. A formal request by a data subject to a data controller (an employer or other type of agency or organization that has control over personal data) to take an action on that data subject's personal data is called a *data subject request* or DSR. For general information about GDPR, see the [GDPR section of the Service Trust portal](#).

Products covered by this guide

This guide discusses how to use Microsoft tools to export or delete personal data collected during authenticated (signed-in) session usage of Visual Studio and Visual Studio for Mac and Microsoft extensions to them and to Visual Studio Code. This guide also covers how to make data subject requests for personal data collected when using Visual Studio Developer Community, NuGet.org, and the ASP.NET website. These products may enable use of non-Microsoft tools and extensions, and Microsoft is not a data processor or controller for these tools and extensions. Users should contact the tool or extension provider to understand the personal data and collection policies for these tools and extensions.

Additional privacy information

The Microsoft Software License Terms accompanying the products, the [Microsoft Privacy Statement](#), and [Microsoft's GDPR Commitments](#) describe our data processing practices.

Visual Studio, Visual Studio for Mac, and Visual Studio Code

Personal data we collect

As a data processor under the GDPR, Microsoft collects the data we need from users to provide experiences for and improve Visual Studio and Visual Studio for Mac and Microsoft extensions to them and to Visual Studio Code. There are two categories of data: customer data and system-generated logs. Customer data includes user-identifiable transactional and interactional data that these products need to perform the service they provide. For example, to provide users with personalized experiences such as roaming settings, we need to collect user account information and settings data. System-generated logs are usage or diagnostic data that are used to help identify and troubleshoot problems and improve our products and services, and may also contain identifiable information about end users, such as a user name. System-generated logs are retained for no more than 18 months. As an example, system-generated logs are aggregated for each day of product usage and include the usage date, the product used (for example, "Visual Studio 2017"), the action you took (for example, "vs/core/packagecostsummary/solutionload"), and the number of times the action was taken, as shown in this sample:

```
{Time:"2/23/2018 12:00:00 AM", "AppName": "Visual Studio  
2017", "Action": "vs/core/packagecostsummary/solutionload", "Target": "1 times",  
"DevicePlatform": "Windows 10 Enterprise", "IP": null, "InputMethod": null,  
"SearchTerm": null, "SearchResult": null}  
  
{Time:"2/23/2018 12:00:00 AM", "AppName": "Visual Studio  
2017", "Action": "vs/ide/connected/accountmanagement/account", "Target": "1 times",  
"DevicePlatform": "Windows 10 Enterprise", "IP": null, "InputMethod": null,  
"SearchTerm": null, "SearchResult": null}  
  
{"Time": "2/27/2018 12:00:00 AM", "AppName": "Visual Studio  
2017", "Action": "vs/core/perf/satellitepagefileusage", "Target": "23 times",  
"DevicePlatform": "Windows 10 Enterprise", "IP": null, "InputMethod": null,  
"SearchTerm": null, "SearchResult": null}
```

For more information, see [System-generated logs collected by Visual Studio](#).

Only personal data that is attached to authenticated identities can be serviced by a DSR. So, for example, because Visual Studio Code does not support sign-in, system-generated logs from it are not attached to an authenticated identity and cannot be serviced. However, some Microsoft extensions for Visual Studio Code may provide authenticated data, and this data can be serviced by a DSR. For more information, see [GDPR and Visual Studio Code](#). In general, we do not store data for Visual Studio 2013 and earlier; however, certain extensions and components may provide data attached to authenticated identities and can be serviced by a DSR as outlined below.

How users can control personal data

Visual Studio 2015 and later, Visual Studio for Mac, and Visual Studio Code provide the following means for your users to stop data collection, and for you as controller to export, or delete data that has already been gathered.

In-app settings

Users can control the privacy settings for these products. For more information, see the following

- [How to manage privacy settings in Visual Studio](#).
- [How to manage privacy settings in Visual Studio for Mac](#).
- [How to disable telemetry reporting in Visual Studio Code](#).

Exporting or deleting data

Controllers can manage customer data and system-generated logs collected from their data subjects by one of two methods, depending upon how their Visual Studio Family product or Microsoft extensions were registered. In some cases, both methods must be used. Both methods allow Controllers to download a copy of their activity history managed by that method. Closure of an AAD or MSA account deletes associated Visual Studio customer data, and anonymizes personally identifiable data in system-generated logs pertaining to these products.

Anonymized system-generated logs are retained for no more than 18 months.

- Users that have registered a Visual Studio Family product by using an account that is backed by an Azure tenant—for example, AAD account or MSA account associated with an Azure subscription—can follow the instructions in [Azure Data Subject Requests for the GDPR](#).
- Users that have registered a Visual Studio Family product without an account that is backed by an Azure tenant—for example many accounts using a Microsoft Account (MSA)—can use [the web-based Microsoft Privacy Response Center](#) available through their Microsoft account to view, control, and delete activity data tied to their Microsoft account across multiple Microsoft services. In this scenario, the user is a controller for their own personal data.

NOTE

When an MSA account holder deletes their account, all their personally identifiable data pertaining to these products is deleted, whether the account is backed by an Azure tenant or not, and system-generated logs are anonymized.

For Visual Studio 2013, the data we collect is anonymized. For Visual Studio 2012 and prior releases, we immediately delete the data upon receipt. In both cases, there is nothing to view, export, or delete at a later time.

Visual Studio Developer Community

We support [General Data Protection Regulation \(GDPR\)](#) requests through the [Developer Community](#) website. You can View, Export, or Delete your feedback data.

Personal data we collect

Microsoft collects data to help us reproduce and troubleshoot issues you report with Visual Studio Family products. This data includes personal data and public feedback. Personal data includes:

- Your [Developer Community](#) profile information;
- Preferences and notifications;
- Attachments and system-generated logs you provided by [reporting a problem in Visual Studio](#) or through [Developer Community](#);
- Your votes.

Public feedback includes: reported problems, comments, and solutions.

How users can control personal data

View

To View your feedback-related data, follow these steps:

1. Sign into [Developer Community](#). From the top right corner, click on your profile and select **Profile and Preferences**.
2. Click on any of the **Profile**, **Notifications**, **Activity**, and **Attachments** tabs to view the data submitted to the feedback systems.
 - a. **Profile** refers to your [Developer Community](#) profile, including user name, email address, about, etc.
 - b. **Notifications** is how you control the email notifications you receive.
 - c. **Activity** will give you the feedback items you have been active on (posted, commented, etc.), and the activities performed.
 - d. **Attachments** is a list of your attachment history in a format like

FileName was attached to the problem "ProblemName" Tue, Apr 10, 18 2:27 PM.

Export

You can export your feedback data as part of DSR. We will create one or more .zip archives that will include:

- Your [Developer Community](#) profile information;
- Preferences and notification settings;
- Attachments you provided by [reporting a problem in Visual Studio](#) or through [Developer Community](#).

NOTE

We will exclude the following public feedback you have provided from your archive: comments, solutions, reported problems.

To start an Export, follow these steps:

1. Sign into [Developer Community](#). From the top right corner, click on your profile and select **Profile and Preferences**.
2. Click the **Privacy** tab, and then click **Create an archive** to request exporting your data.
3. The **Archive Status** will update to show that we are preparing the data. The length of time before the data is available depends on the amount of data we need to export.
4. Once the data is ready, we will send you an email.
5. Click **Download Archive** in the email, or go back to the Privacy tab to download your data.

NOTE

- We will not send email if you chose not to receive notifications in the Notifications tab.
- If you request Export again, we will remove your old archive and create a new one.

Delete

Deleting will remove the following information about you from [Developer Community](#):

- Profile information;
- Preferences and notification settings;
- Attachments you provided by [reporting a problem in Visual Studio](#) or through [Developer Community](#).
- Your votes

NOTE

We will not delete, but will anonymize, the following public information: your comments, your solutions, problems that you reported.

IMPORTANT

Delete of an AAD or MSA account triggers the Delete process for [Developer Community](#).

To initiate a Delete, follow these steps:

1. Sign into [Developer Community](#). From the top right corner, click on your profile and select **Profile and Preferences**.
2. Click the **Privacy** tab, and then click **Delete your data and account** to start deleting your data.
3. A confirmation screen will appear.
4. Type "delete" in the box, and then click **Delete my account**.

Once you click **Delete my account**:

- We will sign you out.
- We will delete your [Developer Community](#) account, your personal data, and attachments.
- We will anonymize your public feedback. Your public feedback will remain available on Developer Community, and will be indicated as reported by an Anonymous user.
- We won't email you after we delete your account, because you will no longer be present in the system.
- If you report a new problem or log into [Developer Community](#), you will be identified as a new user.
- If you delete your account from [Developer Community](#), we will not delete it from other Microsoft services.

Xamarin Forums and Bugzilla

Personal Data We Collect

Through the [Xamarin Forums](#) user community and [Xamarin Bugzilla](#) bug reporting websites, Microsoft collects data you provide to help us reproduce and troubleshoot issues you may have with Microsoft products and services. This data includes personal data and public feedback. The personal data we collect is user account data (for example, user names and email addresses associated with your Xamarin Forums or Bugzilla accounts), and the public feedback we collect includes bugs, problems, comments, and solutions you provide via the Xamarin Forums or Xamarin Bugzilla bug reporting website.

How You Can Control Your Data

Xamarin Forums

[View](#)

Users with active Xamarin Forums accounts may view their personal data and public feedback (for example, all of their posted threads and posts) from their Xamarin Forums account page. Users may also edit their personal data through their account page.

[Export](#)

Xamarin Forums are hosted by a third party, Vanilla Forums. To request export of your public data, users should contact forums@xamarin.com (monitored by the Xamarin team). We will then work directly with Vanilla Forums to process this request.

[Delete](#)

Xamarin Forums are hosted by a third party, Vanilla Forums. To request deletion of your personal and public data, users should contact forums@xamarin.com (monitored by the Xamarin team). We will then manually service the user's personal data deletion request.

Bugzilla for Xamarin

[View](#)

Users with active Xamarin Bugzilla accounts can view all bugs they've reported and all comments they've added to bugs by clicking the appropriate links on the Xamarin Bugzilla home page.

[Export](#)

Exporting of personal data is not supported.

[Delete](#)

To request deletion of personal data used in connection with Xamarin's Bugzilla bug reporting website, users can close their Xamarin Bugzilla account by going to the [user preferences page](#) and choosing the **Close Account tab**. Enter your Bugzilla password and check the box confirming that you understand that this will permanently delete your account. Public feedback (for example, bugs, problems, comments, and solutions) that users have posted to the Xamarin Bugzilla will not be deleted after receipt of a delete request. Public feedback will instead be anonymized by removing the name and email address associated with any public feedback created by the user submitting the delete request.

NuGet

For more information on DSR for NuGet.org, see [NuGet User Data Requests](#).

ASP.NET

For information on DSR for the ASP.NET website, see [The ASP.NET Website and GDPR Data Subject Request processing](#).

IIS.NET

For information on DSR for the IIS.NET website, see [The IIS.NET Website and GDPR Data Subject Request processing](#).

Other Visual Studio Family Services

SurveyMonkey

From time to time, we invite customers to provide feedback on these products via SurveyMonkey. This data is deleted within 28 days. When servicing data subject requests for these products, if we have authenticated survey responses we include them in export and delete data subject requests.

UserVoice

We invite customers to provide product suggestions at UserVoice.com sites for these products. These sites are independently operated by UserVoice, and data subject requests are managed by UserVoice.

- <https://visualstudio.uservoice.com/>
- <https://aspnet.uservoice.com/>
- <https://xamarin.uservoice.com/>

For data subject requests on this data, see the UserVoice guidance on [how to export your data](#) or on [how to delete your data](#).

Learn more

- [Microsoft's GDPR Commitments to Customers of our Generally Available Enterprise Software Products](#)
- [Microsoft Trust Center](#)
- [Service Trust portal](#)
- [Microsoft Privacy Dashboard](#)
- [Microsoft Privacy Response Center](#)
- [Azure Data Subject Requests for the GDPR](#)

Azure DevOps Services Data Subject Requests for the GDPR

12/5/2018 • 3 minutes to read • [Edit Online](#)

The European Union [General Data Protection Regulation \(GDPR\)](#) gives rights to people, known in the regulation as *data subjects*, to manage the personal data that's collected by a *data controller*. A data controller, or just *controller*, is an employer or other type of agency or organization. Personal data is defined broadly under the GDPR as any data that relates to an identified or identifiable natural person. The GDPR gives data subjects specific rights to their personal data. These rights include obtaining copies of personal data, requesting corrections to it, restricting the processing of it, deleting it, or receiving it in an electronic format so it can be moved to another controller. A formal request by a data subject to a controller to take an action on their personal data is called a *Data Subject Request*, or DSR.

For general information about GDPR, see the [GDPR section of the Service Trust portal](#).

This guide discusses how to use Microsoft tools to export or delete personal data collected during an authenticated (signed-in) session of Azure DevOps Services (formerly known as Visual Studio Team Services).

Additional privacy information

The [Microsoft Privacy Statement](#), [Online Services Terms \(OST\)](#), and [Microsoft's GDPR Commitments](#) articles describe our data processing practices.

Personal data we collect

Microsoft collects data from users to operate and improve Azure DevOps Services. Azure DevOps Services collects two categories of data—customer data and system-generated logs. Customer data includes user-identifiable transactional and interactional data that Azure DevOps Services needs to operate the service. System-generated logs include service usage data that is aggregated for each product area and feature.

Delete Azure DevOps data

The first step to delete associated Azure DevOps Services customer data and to anonymize personally identifiable data found in system-generated logs is to close your Azure Active Directory (AAD) identity account or Microsoft Account (MSA). Azure DevOps Services is relied upon as a system of record with strict integrity, traceability, and audit rules. These existing obligations affect our delete and retention obligations for GDPR. Closing the identity account does not alter, remove, or change artifacts and records associated with the individual identity in the Azure DevOps organization. We have ensured that when an entire Azure DevOps organization is deleted, all associated personally identifiable data and system-generated logs found in that organization are removed from our system (after the requisite Azure DevOps organization 30-day soft-delete period).

Export Azure DevOps data

Controllers can export customer data and system-generated logs collected from their data subjects by one of two methods, depending upon the identity provider (MSA or AAD) used to sign in to the Azure DevOps service.

- Users that authenticate using an account that is backed by an Azure tenant, for example, AAD account or MSA account associated with an Azure subscription, can follow the instructions in [Azure Data Subject Requests for the GDPR](#).

- Users that authenticate using an MSA identity can use this [Privacy Request site](#) to view activity data tied to their MSA identity across multiple Microsoft services. In this scenario, the user is a controller for their own personal data.

Export or delete issues

For AAD identities, if you run into issues while exporting or deleting data from the Azure portal, go to the Azure portal **Help + Support** blade and submit a new ticket under **Subscription Management > Other Security and Compliance Request > Privacy Blade and GDPR Requests**.

For MSA identities, if you run into issues while exporting data from the Privacy Request site, log on to the [Privacy Request site](#) and submit a request for help from the Microsoft Privacy team via the request webform.

Learn more

Microsoft is committed to ensuring that your Azure DevOps Services data remains secure and private, without exception. Visit the [Azure DevOps Services data protection overview](#) whitepaper to learn more about how we protect your Azure DevOps Services data.

See also

- [Microsoft's GDPR commitments to customers of our generally available enterprise software products](#)
- [Microsoft Trust center](#)
- [Service Trust portal](#)
- [Microsoft privacy dashboard](#)
- [Microsoft privacy response center](#)
- [Azure Data Subject Requests for the GDPR](#)

Microsoft Support and Professional Services Data Subject Requests for the GDPR

2/22/2019 • 21 minutes to read • [Edit Online](#)

Introduction to Microsoft Professional Services

Microsoft Professional Services includes a diverse group of technical architects, engineers, consultants, and support professionals dedicated to delivering on the Microsoft mission of empowering customers to do more and achieve more. Our Professional Services team includes more than 21,000+ total consultants, Digital Advisors, Premier Support, engineers, and sales professionals working across 191 countries, supporting 46 different languages, managing several million engagements per month, and engaging in customer and partner interactions through on-premise, phone, web, community and automated tools. The organization brings broad expertise across the Microsoft portfolio, leveraging an extensive network of partners, technical communities, tools, diagnostics and channels that connect us with our enterprise customers.

Find out more about Microsoft Professional Services here

(https://www.microsoft.com/microsoftservices/professional_services.aspx) and by going to the Microsoft Professional Services section on the Microsoft Trust Center

(<https://www.microsoft.com/trustcenter/cloudservices/commercialsupport>). Microsoft Professional Services takes its obligations under the General Data Protection Regulation (GDPR) seriously. The information in this document is designed to answer customer questions about how Microsoft's support and consulting offerings will respond to and assist customers in responding to Data Subject Request (DSR) obligations under GDPR.

Introduction to DSRs

The GDPR gives rights to people (known in the regulation as *data subjects*) to manage the personal data that has been collected by an employer or other type of agency or organization (known as the *data controller* or just *controller*). Personal data is defined very broadly under the GDPR as any data that relates to an identified or identifiable natural person. The GDPR gives data subjects specific rights to their personal data; these rights include obtaining copies of it, requesting changes to it, restricting the processing of it, and deleting it. A formal request by a data subject to a controller to take an action on their personal data is called a *Data Subject Request* or DSR. Additionally, it obligates companies working on behalf of a controller (known as the *data processor* or just *processor*) to reasonably assist the controller in fulfilling DSRs.

This guide discusses how to find, access, and act on personal data that reside in Microsoft IT systems that may have been collected to provide Support and other Professional Services offerings.

In developing a response for DSRs, it is important for Microsoft's customers to understand that Support and Consulting Data is separate from Customer Data in the Online Services or other data that they or their data subjects may have provided to Microsoft. Tools and processes provided for Online Services, the Microsoft Privacy Dashboard, or other Microsoft systems for responding to DSRs cannot be used to respond to DSRs for personal data held by Microsoft Support or other Professional Services.

All requests must be made through a support representative, as described below. Currently there is no self-serve tool for customers gain access to personal data within the Professional Services organizations.

Overview of the processes outlined in this guide

Discover. Find personal data that may be the subject of a DSR. Once potentially responsive material is collected, perform one or more of the DSR actions described in the following steps to respond to the DSR request. Alternatively, determine that the request doesn't meet organizational guidelines for responding to DSRs.

Access. Retrieve personal data that resides in the Microsoft cloud and, if requested, make a copy of it available to

the data subject.

Rectify. Make changes or implement other requested actions on the personal data.

Restrict. Restrict the processing of personal data by halting activity on an engagement.

Delete. Permanently remove personal data that reside in Microsoft IT Systems.

Export. Provide a copy of personal data to the customer or data subjects.

Terminology

Below are the relevant definitions of terms from the GDPR for this guide:

- **Controller.** The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- **Personal data and data subject.** Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **Processor.** A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Additional terms and definitions that may helpful in understanding this guide

- **Support and Consulting Data** is all data, including all text, sound, video, image files, or software, that are provided to Microsoft by, or on behalf of, Customer (or that Customer authorizes Microsoft to obtain from an Online Service) through an engagement with Microsoft to obtain Support or Professional Services. To clarify, this does not include data collected where Microsoft is the data controller including Customer Contact Data.
- **Customer Contact** is personal data that may be part of your business relationship with Microsoft, such as personal data contained within your customer contact information. This may include your name, e-mail, or phone number of the Premier Contract Service Manager (CSM), the Global or IT Administrator for an Online Service, or similar roles.
- **Pseudonymized Data** When you use Microsoft support for Microsoft's enterprise products and services, Microsoft generates some information linked to a Microsoft numeric identifier to provide the support. This is often referred to as "Pseudonymized Data", Although this data cannot be attributed to a specific data subject without the use of additional information, some of it may be deemed personal under GDPR's broad definition for personal data. Within Professional Services, requests to fulfill or assist in fulfilling DSRs will always automatically include addressing pseudonymized data.

How to use this guide

This guide covers four scenarios a customer may encounter if they have utilized Microsoft Professional Services.

DSR for a Customer Contact Engaging Microsoft

Explanation for how Microsoft will respond to requests from a customer contact or IT administrator to exercise their data subject rights.

DSR for an End User Engaging Microsoft

Explanation for how Microsoft will respond to requests from a customer's employees or other data subjects to

exercise their rights.

DSR for Customer Provided Data: Commercial Support

Explanation for how to receive assistance from Microsoft when a customer has received a request from their employee or other data subjects to exercise their rights, and that data subject's personal data was collected by Microsoft Support during a support engagement.

DSR for Customer Provided Data: Consulting Services including FastTrack Migration Services

Explanation for how to receive assistance from Microsoft when a customer has received a request from their employee or other data subjects to exercise their rights, and that data subject's personal data was collected by Microsoft during a consulting engagement.

DSR for a Customer Contact Engaging Microsoft

How Microsoft responds to requests by a customer contact or IT admin to exercise their data subject rights.

When a customer engages with Microsoft to receive support or consulting services, Microsoft Support automatically collects or retrieves from account records the personal data of the Customer Contact (e.g. Premier CSM, Global Admin, IT Admin). This likely includes the name, email, phone and other personal data of the individual seeking support or consulting services.

The Customer Contact's personal data is part of Microsoft's business relationship with the customer, and Microsoft is the data controller. Microsoft will respond to DSRs from the Customer Contact around their personal data, regardless of whether they are still with the organization.

Customers should understand that the DSR only covers the personal data of the Customer Contact, and no changes or deletions will be made to any of the customer's data submitted as part of engagements (e.g. transcripts, case descriptions, files, work product), since Microsoft is the data processor. Additionally, to maintain the engagement's historical record no changes at all will be made to closed engagements, including the record of who opened an engagement.

Upon receiving an inquiry from a Customer Contact regarding a DSR, Microsoft personnel will refer a customer contact to [Microsoft Privacy Support](#). This is Microsoft's primary input mechanism for privacy inquiries and complaints. Upon receiving an inquiry, the Microsoft Privacy Team will identify that this is part of a commercial or organizational account and respond accordingly.

To maintain customer's business continuity, Microsoft will also not process a DSR associated with an engagement until a replacement contact is confirmed. Upon confirmation of a new contact, Microsoft will swap out the old contact with the new one in open engagements.

Customers may choose to make changes to their data collected during Professional Services engagements through normal support or consulting channels, separate from this DSR. For instance, Microsoft can assist in expunging support engagements, on request (see below in *DSR Guide for Customer Provided Data* section).

Example for Illustration Purposes Only

John is an IT Admin for an O365 enterprise customer, with one open support engagement and two closed engagements. Now John is leaving his company and wants his data deleted. John contacts the PRC, who identifies him as the IT Admin. John is informed his name cannot be deleted from the prior (closed) engagements or from any data within the open engagements. However, the PRC will replace John as the contact on the current open ticket if he will identify a replacement contact. John lets Microsoft know that Jane will be his replacement contact, and Microsoft makes the change across all support systems.

DSR for an End User Engaging Microsoft

How Microsoft responds to requests from a customer's employees or other data subjects to exercise their rights.

If a customer's employee or other data subject contacts Microsoft to exercise their rights over data that Microsoft has collected as the data processor, then that data subject will be informed that they need to contact Microsoft's customer, as the data controller, to exercise those rights. Microsoft will take no further action.

If the data subject has also contacted Microsoft about exercising their rights for data Microsoft has collected in situations where Microsoft is the data controller (e.g. consumer support, commercial customer contact) then Microsoft will separately respond to the individual's data subject right request for that personal data.

Example for Illustration Purposes Only

Jane is an employee of an Enterprise customer, Contoso, that has given her a Dynamics 365 account. She contacts Microsoft to have all her data deleted and is referred to the Privacy Response Center. Jane fills out the request form. The Privacy Response Center identifies her as an enterprise end-user and lets her know she needs to work through Contoso for the deletion of her enterprise data. They also identify her as a Microsoft X-Box user and delete her data out of her consumer Microsoft account.

DSR for Customer Provided Data: Commercial Support

How to receive assistance from Microsoft when a customer has received a request from their employee or other data subjects to exercise their rights, and that data subject's personal data was collected by Microsoft Support during a support engagement.

When a customer engages with Microsoft Support, Microsoft collects Support Data from the customer to resolve any issues that required a support engagement. This Support Data includes Microsoft's interaction with the customer (e.g. chat, phone, email, web submission) plus any content files the customer sends to Microsoft or Microsoft has, with customer's permission, extracted from the customer's IT environment or Online Services tenancy to resolve the support issue. In the case of Premier support, this would also include any data we collect from you to proactively prevent future issues. However, this excludes Customer Contact information or other information from Microsoft's business relationship with the customer (e.g. billing records).

For all Support Data, Microsoft is the data processor. As such, Microsoft's will not respond to direct requests from data subjects regarding Support Data provided when they were associated with a Microsoft commercial customer. Microsoft will work with the customer through their normal support channels to assist them in responding to DSRs.

Step 1: Discover

The first step in obtaining Microsoft's assistance in responding to a DSR is to find the personal data that is the subject of the DSR. This first step - finding and reviewing the personal data at issue - will help a customer determine whether a DSR meets the organization's policies for honoring a data subject request.

After the customer finds the data, the customer can then perform the specific action to satisfy the request by the data subject. Depending on what the customer is trying to do will determine what level of discovery the customer needs to engage in.

Where Microsoft assists a customer with the resolution of a DSR then this is a business function, and the request is made through your regular support channel and not through a request to the Microsoft Privacy Team.

In discovering relevant data and obtaining Microsoft's assistance, a customer has several options for how to approach the DSR:

Option A – Cross-Microsoft Support Customer DSR. Apply the DSR to all the customer's support data across Microsoft's support environment. To do this, a customer can just ask Microsoft to apply the DSR to all Support

Data collected.

Option B – Specific Customer Engagements. Use online systems to review tickets, then identify specific engagements containing the relevant personal data and report them Microsoft. Microsoft will attempt to provide assistance to perform a search if the customer does not have the ability to search across engagements (tickets).

**Once engagements are identified, request to apply the DSR to either a specific part of the record or everything related to that engagement across Microsoft. **

To identify specific engagements, customers need to search across their engagements. For Premier customers, the Contract Service Manager ("CSM") for a customer has visibility across all Support Requests (SRs) that are created under that Contract Schedule. For Non-Premier, equivalent support engagement portals are available, such as through Online Services support areas.

Searching in SMC

1 Users can create Support Requests, search for requests, or get more details from a specific request.

Support Requests

+ New support request

Number	Status	Title	Severity	Last Updated
116061614299181	Closed	test asdf	C	7/22/2016
116072014438622	Closed	TEST	C	7/19/2016
116062914352555	Closed	test	C	6/30/2016
116062414330722	Closed	test	C	6/29/2016
116041913980936	Closed	test case	C	6/28/2016

Show more

The CSM can go to the portal at Support.Microsoft.Com (<https://support.microsoft.com/<local language code>/premier>) ("SMC") and select and review Support Requests. (Note: In the URL, please substitute for your local language code).

[Important Note Regarding DTM] In addition to the case history in SMC, customers may also have personal data of an end user in files that was collected by Microsoft (or, with customer's permission, removed from the Online Service) during a support engagement. Examples may include copies of customer's exchange mailboxes, Azure VMs, or databases. This personal data may or may not be mentioned in the case history (i.e. ticket) for a particular engagement. To review that data, the Customer Contact must be a specific authenticated (via AAD or MSA) Support Request contact that has received a URL for a workspace in Microsoft Support Data Transfer and Management tool (DTM). A Customer Contact will have access to the files, but no global view is available, and SMC will not indicate if files exist.

Once customers have identified all the relevant data in the selected support tickets, customers can decide whether to request the deletion of everything related to a ticket or selectively apply the DSR to individual instances of personal data.

Step 2: Access

After a customer has found Support Data containing personal data that is potentially responsive to a DSR, it is up to the customer to decide which personal data to include in the response. For example, the customer may choose to remove personal data about other data subjects and any confidential information.

Response to the DSR may include a copy of the actual document, an appropriately redacted version, or a screenshot of the portions the customer has deemed appropriate to share. For each of these responses to an access request, the customer will have to retrieve a copy of the document or other item that contains the responsive data.

Access to the personal data of an end user may be from a mention or notation in the various types of content documentation. Since customers may access the engagement ticket and the content they can provide a summary of personal data themselves without further assistance from Microsoft.

In rare cases, customer may have need to obtain copies of support interaction data (e.g. emails, transcribed copies of phone recordings; chat transcripts) between a Microsoft Representative and the Customer's Representative. To the extent required, Microsoft may provide redacted copies of these transcripts based on need, sensitivity, and difficulty.

Step 3: Rectify

If a data subject has asked the customer to rectify the personal data that resides in their organization's Support Data, the customer will have to determine whether it's appropriate to honor the request. If the customer chooses to honor the request, then the customer may request that Microsoft make the change. Microsoft may rectify data or may delete customer's data from the support systems and request that the customer resubmit it to Microsoft in corrected format.

Step 4: Restrict

The customer may at any time close an engagement or contact Microsoft and request the engagement be closed. A closed engagement will prevent any work from being performed.

For extra assurance, customer may contact Microsoft and request a note be placed in the engagement ticketing system instructing that the case should not be re-opened for any reason absent the customer's permission.

Note: Engagements (tickets) will also be deleted according on a retention and deletion schedule, based on the sensitivity of data, service, and system. If customer requires a copy of data, they should ensure they have extracted data prior to deletion.

Step 5: Delete

The "right to erasure" by the removal of personal data from an organization's Support Data is a key protection in the GDPR. Removing personal data includes deleting entire engagements, documents or files or deleting specific data within an engagement, document or file.

As a customer investigates or prepares to delete personal data in response to a DSR, here are a few important things to understand about how deletion works for Microsoft Support.

All data at Microsoft has a retention and deletion policy applied to it, which will vary depending on risk and other factors.

Customers requesting the deletion of a data subject's personal data universally cross Support systems may do that through your TAM or by filing a Support Request (SR) in SMC or equivalent system. You *must* indicate that this is a request to assist with a DSR under GDPR.

Option A - Cross-Microsoft Support Customer DSR. For a cross system DSR, customer must provide the personal data that Microsoft needs to identify the required data (e.g. email address; phone number). Microsoft will not correlate or research records and will only search directly on identifiers provided by the customer. When data is found, Microsoft will delete all engagements and all associated data. **Important Note:** this may result in loss of historical records that are important to customer's organization.

Option B – Specific Customer Engagements. For specific engagements that the customer has identified and wants deleted, do not delete tickets out of SMC. This will result in personal data remaining in logs and downstream systems that may not be deleted within the needed timeframe. Instead, identify the ticket or personal data within the ticket that must be deleted, and contact Microsoft Support to assist you in deleting that data.

Microsoft Support Data Transfer and Management tool (DTM) instructions

For all these searches, Microsoft will not search across DTM due to the potential sensitivity of content in files. However, if the customer desires, Microsoft will delete all files contained in DTM associated with the customer's account. Due to the potential for serious customer impact, Microsoft requires a separate request from customer specifying the deletion of DTM files.

- For open cases, the Customer Contact can go into DTM and delete files.
- For cases closed less than 90 days, a request must be made to a TAM or in an SR to have the files removed.
- For cases closed after than 90 days, files have already been automatically deleted.
- Even if the personal data was only located within a file that has been deleted, customers must still have Microsoft run a check across systems for the personal data as some data may have been removed from DTM in the course of providing support.

Step 6: Export

The "right of data portability" allows a data subject to request a copy of their personal data in an electronic format and request that your organization transmit it to another controller. In the case of Support Data, any usable information that Microsoft has would be in the form of engagement information or files that can be returned to you for re-communication or uploading to another controller.

Note: Exported data may not include Microsoft's intellectual property or any data that may compromise the security or stability of the service.

Example for Illustration Purposes Only

John is a Premier CSM for an Enterprise customer, Contoso, that uses O365 for its employee e-mail and Azure to host a Contoso SQL database. Contoso has multiple open and closed tickets. Recently, Microsoft Support, with Contoso's permission, moved a copy of the SQL database into DTM for support and troubleshooting.

John receives a DSR from Jane asking that all her data be deleted. John goes into SMC and searches across engagements to identify that Jane had email account issues and so was referenced in two tickets by name and email address. He contacts his TAM, provides the TAM with Jane's name and e-mail address as an identifier, and requests that those two tickets be deleted, along with all downstream data that may have been generated out of those tickets.

He also suspects he was engaged in a chat conversation with support personnel where he mentions Jane, so he requests that chat log to be deleted.

He also knows that Jane's personal data is in the SQL Database. Since the SQL VM was moved into DTM less than 90 days ago, he asks his TAM separately to assist in the immediate deletion of the database out of DTM.

Lastly, since he knows that data may have been removed from the DTM file during providing support, he asks Microsoft to run a check across IT systems for Jane's personal data from the SQL database.

Microsoft Support performs all these deletions and, based on customer request, the TAM provides him with an attestation statement that the required data has been deleted.

DSR Guide for Customer Provided Data in Consulting Services including Migration Services

How to receive assistance from Microsoft when a customer has received a request from their employee or other data subjects to exercise their rights, and that data subject's personal data was collected by Microsoft during a consulting engagement.

Microsoft Consulting Services

For Microsoft Consulting Services engagements contracted where the Microsoft Professional Services Data Protection Addendum (<http://aka.ms/professionalservicesdpa>) applies.

Microsoft is the data controller for Customer Contacts working with the engagement team. Those individuals should contact [Microsoft Privacy Support](#) to fulfill data subject rights.

Microsoft is the data processor for a DSR located within data provided during a consulting engagement. The customer should contact the engagement manager to build in a plan to assist in responding to a DSR based on the data collected and then specific type of consulting services provided. To the extent your request constitutes a level of effort typically seen within a Microsoft Consulting Services engagement, there may be an additional work order required. Additionally, personal data will be deleted after each consulting engagement within a timeframe dependent on the type of consulting engagement. Customer can request data to be deleted sooner and request an attestation of deletion.

Microsoft FastTrack Services

[Microsoft FastTrack](#) provides IT consulting services to organizations to help them onboard and use Microsoft cloud services such as Microsoft 365, Azure and Dynamics 365.

Microsoft is the data controller for Customer Contacts working with the FastTrack team. If Customer Contacts wish to access, revise or remove contact information from Microsoft's FastTrack records, customers can have the data subject send the request directly to Office 365 FastTrack GDPR Request inbox <o365ftgdpr@microsoft.com>.

For FastTrack migration services, Microsoft is the data processor. In accordance with our Fast Track additional privacy disclosure statement, all data in migration is considered "migration data." If you need to execute DSRs while your organization is engaged in a FastTrack migration project, special care is required.

If you need to process any access, rectify, or export DSR requests while a user's data is being processed through FastTrack migration systems, it will be the customer's responsibility to fulfill such DSRs through your existing source systems in which the user data is stored. Once the user's migration is complete and the data has been migrated to the destination Microsoft cloud service, the guidance provided by Microsoft on how customers can use Microsoft products, services and administrative tools to find and act on personal data to respond to data subject request will then apply. To view this guidance see [Data Subject Requests for the GDPR](#).

If you need to delete an Office 365 user account in response to a DSR delete request while your organization is engaged in an ongoing FastTrack migration project, you should be aware that migration systems may retain a copy of user migration data for a period of time following completion of the user's migration and deleting the Office 365 user account will not automatically delete such user migration data stored in FastTrack migration systems. If you would like the Microsoft FastTrack team to delete user migration data, you can [submit a request](#). In the ordinary course of business, Microsoft FastTrack will delete all data copies once your organization's migration is complete.

Other Consulting Services

Customer receiving other Professional Services through Microsoft should work through the engagement team for fulfillment of all GDPR requirements. If the engagement team is not able to provide clear instructions on GDPR DSR fulfillment, customers may contact [Microsoft Privacy Support](#) for assistance.

Breach Notification under the GDPR

2/22/2019 • 2 minutes to read • [Edit Online](#)

Microsoft takes its obligations under the General Data Protection Regulation (GDPR) seriously. For information about how Microsoft services protect against a personal data breach and how we respond and notify you if a breach occurs, see the following topics:

- [Office 365](#)
- [Azure](#)
- [Dynamics 365](#)
- [Microsoft Support and Professional Services](#)

For more information about how Microsoft detects and responds to a breach of personal data, see [Data Breach Notification Under the GDPR](#) in the Service Trust Portal.

Learn more

[Microsoft Trust Center](#)

Office 365 Breach Notification Under the GDPR

2/22/2019 • 7 minutes to read • [Edit Online](#)

As a data processor, Office 365 will ensure that our customers are able to meet the GDPR's breach notification requirements as data controllers. To that end, we are committed to the following:

- Providing customers with an ability to specify a dedicated privacy contact who will be notified in the event of a breach. Customers will be able to specify this contact in Azure Active Directory (AAD)
- Notifying customers of a personal data breach within 72 hours of a breach being declared. Notification will be done by e-mail to the contact specified by the customer
- Initial notification will include, at the least, a description of the nature of the breach, approximation of user impact, and mitigation steps (if applicable). If our investigation is not complete at the time of initial notification, we will indicate next steps and timelines for subsequent communication in our initial notification

Microsoft recognizes that data controllers are responsible for conducting risk assessments and determining whether a breach requires notification of the customer's DPA, and our notification to customers will provide the information needed to make that assessment. Microsoft will therefore notify customers of any personal data breach, except for those cases where personal data is confirmed to be unintelligible (for example, strongly encrypted data where integrity of the keys is confirmed).

Office 365 Investments in Data Security

In addition to our commitment to provide timely notification of breach, Office 365 strongly invests in systems, processes, and personnel to reduce the likelihood of personal data breach and to quickly detect and mitigate consequence of breach if it does occur.

Here is a description of some of our investments in this space:

- **Access Control Systems.** Office 365 maintains a "zero-standing access" policy, which means that engineers do not have access to the service unless it is explicitly granted in response to a specific incident that requires elevation of access. Whenever access is granted it is done under the principle of least privilege: permission granted for a specific request only allow for a minimal set of actions required to service that request. To do this, Office 365 maintains strict separation between "elevation roles", with each role only allowing certain pre-defined actions to be taken. The "Access to Customer Data" role is distinct from other roles that are more commonly used to administer the service and is scrutinized most heavily before approval. Taken together, these investments in access control greatly reduce the likelihood that an engineer in Office 365 inappropriately accesses customer data.
- **Security Monitoring Systems and Automation:** Office 365 maintains robust, real-time security monitoring systems. Among other issues, these systems raise alerts for attempts to illicitly access customer data, or for attempts to illicitly transfer data out of our service. Related to the points about access control mentioned above, our security monitoring systems maintain detailed records of elevation requests that are made, and the actions taken for a given elevation request. Office 365 also maintains automatic resolution investments that automatically act to mitigate threats in response to issues we detect, and dedicated teams for responding to alerts that cannot be resolved automatically. To validate our security monitoring systems, Office 365 regularly conducts red-team exercises in which an internal penetration testing team simulates attacker behavior against the live environment. These exercises lead to regular improvements to our security monitoring and response capabilities.
- **Personnel and Processes:** In addition to the automation described above, Office 365 maintains processes

and teams responsible for both educating the broader organization about privacy and incident management processes, and for executing those processes during a breach. For example, a detailed privacy breach Standard Operating Procedure (SOP) is maintained and shared with teams throughout the organization. This SOP describes in detail the roles and responsibilities both of individual teams within Office 365 and centralized security incident response teams. These span both what teams need to do to improve their own security posture (conduct security reviews, integrate with central security monitoring systems, and other best practices), and what teams would need to do in the event of an actual breach (rapid escalation to incident response, maintain and provide specific data sources that will be used to expedite the response process). Teams are also regularly trained on data classification, and correct handling and storage procedures for personal data.

The major takeaway is that Office 365 strongly invests in reducing the likelihood and consequences of personal data breach impacting our customers. If personal data breach does occur, we are committed to rapidly notifying our customers once that breach is confirmed.

What to Expect in the Event of Breach

The section above describes the investments Office 365 makes to reduce the likelihood of data breach. In the unlikely event that breach does occur, customers should expect a predictable experience in terms of the following:

- Consistent incident response lifecycle within Office 365. As described above, Office 365 maintains detailed incident response SOPs describing how teams should prepare for breach and how they should operate if a breach does occur. This ensures that our protections and processes apply throughout the service.
- Consistent criteria for notifying customers. Our notification criteria focus on Confidentiality, Integrity, and Availability of customer data. Office 365 will directly notify customers if either the confidentiality or integrity of customer data is impacted. That is, we will notify customers if their data is accessed without proper authorization, or if there is inappropriate destruction or loss of data. Office 365 will also report issues impacting data availability, although this is usually done through the Service Health Dashboard (SHD).
- Consistent notification details. When Office 365 does communicate regarding data breach, customers can expect specific details to be communicated: at minimum, we will provide the following details:
 - Timing of the breach and timing of breach awareness
 - The approximate number of users impacted
 - The type of user data that was breached
 - Actions needed to mitigate the breach, either by the controller or by the processor

Customers should also note that Office 365, as a data processor, will not determine the risk of data breach. Whenever personal data breach is detected, we will notify our customers and provide them with the details they need to accurately determine risk to impacted users and to decide whether further reporting to regulatory authorities is required. To that end, data controllers are expected to determine the following:

- Breach severity (that is, risk determination)
- Whether end users need to be notified
- Whether regulators (DPAs) need to be notified
- Specific steps that will be taken by the controller to mitigate the consequences of breach

Contacting Microsoft

In some scenarios, a customer may become aware of a breach and may wish to notify Microsoft. The current protocol is for customers to notify Microsoft Support, which will then interface with engineering teams for more

information. In this scenario, Microsoft engineering teams are similarly committed to providing the information customers need, through their support contact, in a timely fashion.

Call to Action for Customers

As noted above, Office 365 is committed to notifying customers within 72 hours of breach declaration. The customer's tenant administrator will be notified. Additionally, Office 365 recommends that customers designate a Global Privacy Contact alias, which can be done in the Azure Active Directory (AAD) portal. In the event of personal data breach, this alias may be e-mailed in addition to the notification that will be sent to administrators.

The customer's privacy contact can be an individual within the organization, a distribution list (DL), or someone entirely outside of the organization. Office 365 only asks that customers provide an e-mail address for this contact, and customers will be able to specify this in the AAD portal, under the "Global Privacy Contact" field. Note that this field is related to, but distinct from, the existing "Technical Contact" field in AAD. If customers choose to specify a DL for this contact, they should ensure that the DL is configured to enable receipt of messages from external senders.

To summarize, Office 365 asks customers to do the following to receive the benefits of our breach notification processes:

- Decide on a contact to receive e-mail notifications regarding personal data breach. This contact should be aware of the controller's requirements under GDPR and should be prepared to interface with the organization's DPO and potentially the DPA shortly after receiving notification. Tenant administrators will also receive breach notifications and should similarly be aware of the controller's requirements under GDPR.
- Enter the privacy contact's e-mail address into the AAD portal. If no Global Privacy Contact information is provided, Microsoft will only notify the tenant administrator
-

Azure and Breach Notification Under the GDPR

2/22/2019 • 9 minutes to read • [Edit Online](#)

Microsoft Azure takes its obligations under the General Data Protection Regulation (GDPR) seriously. Microsoft Azure takes extensive security measures to protect against data breaches. These include both physical and logical security controls, as well as automated security processes, comprehensive information security and privacy policies, and security and privacy training for all personnel.

Security is built into Microsoft Azure from the ground up, starting with the [Security Development Lifecycle](#), a mandatory development process that incorporates privacy-by-design and privacy-by-default methodologies. The guiding principle of Microsoft's security strategy is to "assume breach," which is an extension of the defense-in-depth strategy. By constantly challenging the security capabilities of Azure, Microsoft can stay ahead of emerging threats. For more information on Azure security, please review these [resources](#).

Microsoft has a global, 24x7 incident response service that works to mitigate the effects of attacks against Microsoft Azure. Attested by multiple security and compliance audits (e.g. [ISO/IEC 27018](#)), Microsoft employs rigorous operations and processes at its data centers to prevent unauthorized access, including 24x7 video monitoring, trained security personnel, smart cards, and biometric controls.

Detection of Potential Breaches

Due to the nature of modern cloud computing, not all data breaches occurring in a customer cloud environment involve Microsoft Azure services. Microsoft employs a shared responsibility model for Azure services to define security and operational accountabilities. Shared responsibility is particularly important when discussing security of a cloud service, because both the cloud services provider and the customer are accountable for portions of cloud security.

Microsoft does not monitor for or respond to security incidents within the customer's realm of responsibility. A customer-only security compromise would not be processed as an Azure security incident and would require the customer tenant to manage the response effort. Customer incident response may involve collaboration with Microsoft Azure [customer support](#), given appropriate service contracts. Microsoft Azure also offers various services (e.g., [Azure Security Center](#)) that customers can utilize for developing and managing security incident response.

Azure responds to a potential data breach according to the security incident response process, which is a subset of the Microsoft Azure incident management plan. Azure's security incident response is implemented using a five-stage process: Detect, Assess, Diagnose, Stabilize, and Close. The Security Incident Response Team may alternate between the diagnose and stabilize stages as the investigation progresses. An overview of the security incident response process is below:

	STAGE	DESCRIPTION
1	Detect	First indication of a potential incident.
2	Assess	An on-call incident response team member assesses the impact and severity of the event. Based on evidence, the assessment may or may not result in further escalation to the security response team.

	STAGE	DESCRIPTION
3	Diagnose	<p>Security response experts conduct the technical or forensic investigation, identify containment, mitigation, and workaround strategies.</p> <p>If the security team believes that customer data may have become exposed to an unlawful or unauthorized individual, execution of the Customer Incident Notification process begins in parallel.</p>
4	Stabilize and Recover	<p>The incident response team creates a recovery plan to mitigate the issue. Crisis containment steps such as quarantining impacted systems may occur immediately and in parallel with diagnosis. Longer term mitigations may be planned which occur after the immediate risk has passed.</p>
5	Close and Post-Mortem	<p>The incident response team creates a post-mortem that outlines the details of the incident, with the intention to revise policies, procedures, and processes to prevent a reoccurrence of the event.</p>

The [Microsoft Azure Security Response in the Cloud](#) white paper further details how Microsoft investigates, manages, and responds to security incidents within Azure.

The detection processes used by Microsoft Azure are designed to discover events that risk the confidentiality, integrity, and availability of Azure services. Several events can trigger an investigation:

- Automated system alerts via internal monitoring and alerting frameworks. These alerts could come in the way of signature-based alarms such as antimalware, intrusion detection or via algorithms designed to profile expected activity and alert upon anomalies.
- First party reports from Microsoft Services running on Microsoft Azure and Azure Government.
- Security vulnerabilities are reported to the [Microsoft Security Response Center \(MSRC\)](#) via secure@microsoft.com. MSRC works with partners and security researchers around the world to help prevent security incidents and to advance Microsoft product security.
- Customer reports via the [Customer Support Portal](#) or Microsoft Azure and Azure Government Management Portal, that describe suspicious activity attributed to the Azure infrastructure (as opposed to activity occurring within the customer's scope of responsibility).
- Security [Red Team and Blue Team](#) activity. This strategy uses a highly-skilled Red Team of offensive Microsoft security experts to uncover and attack potential weaknesses in Azure. The security response Blue Team must detect and defend against the Red Team's activity. Both Red and Blue Team actions are used to verify that Azure security response efforts are effectively managing security incidents. Security Red Team and Blue Team activities are operated under rules of engagement to help ensure the protection of customer data.
- Escalations by operators of Azure Services. Microsoft employees are trained to identify and escalate

potential security issues.

Azure's Data Breach Response

Microsoft assigns the investigation appropriate priority and severity levels by determining the functional impact, recoverability, and information impact of the incident. Both the priority and severity may change over the course of the investigation, based on new findings and conclusions. Security events involving imminent or confirmed risk to customer data are treated as high severity and worked around the clock to resolution. Microsoft Azure categorizes the information impact of the incident into the following breach categories:

CATEGORY	DEFINITION
None	No information was exfiltrated, changed, deleted, or otherwise compromised.
Privacy Breach	Sensitive personal data of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated.
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated.
Integrity Loss	Sensitive or proprietary information was changed or deleted.

The Security Response Team works with Microsoft Azure Security Engineers and SMEs to classify the event based on factual data from the evidence. A security event may be classified as:

- **False Positive:** An event that meets detection criteria but is found to be part of a normal business practice and may need to be filtered. The service team will identify the root cause for false positives and will address them in a systematic way leveraging detection sources and fine-tuning them as needed.
- **Security Incident:** An incident where unlawful access to any Customer Data or Support Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data or Support Data has occurred.
- **Customer-Reportable Security Incident (CRSI):** An unlawful or unauthorized access to or use of Microsoft's systems, equipment, or facilities resulting in disclosure, modification, or loss of customer data.
- **Privacy Breach:** A subtype of Security Incident involving personal data. Handling procedures are no different than a security incident.

For a CRSI to be declared, Microsoft must determine that unauthorized access to customer data has or has very likely occurred and/or that there is a legal or contractual commitment that notification must occur. It is desired, but not required, that specific customer impact, resource access, and repair steps be known. An incident is generally declared a CRSI after the conclusion of the Diagnose stage of a security incident; however, the declaration may happen at any point that all pertinent information is available. The security incident manager must establish evidence beyond reasonable doubt that a reportable event has occurred to begin execution of the Customer Incident Notification Process.

Throughout the investigation, the security response team works closely with global legal advisors to help ensure that forensics are performed in accordance with legal obligations and commitments to customers. There are also significant restrictions on system and customer data viewing and handling in various operating environments. Sensitive or confidential data, as well as Customer Data, are not transferred out of the production environment without explicit written approval from the Incident Manager recorded in the corresponding incident ticket.

Microsoft verifies that customer and business risk is successfully contained, and that corrective measures are implemented. If necessary, emergency mitigation steps to resolve immediate security risks associated with the event are taken.

Microsoft also completes an internal post-mortem for data breaches. As a part of this exercise, sufficiency of response and operating procedures are evaluated, and any updates that may be necessary to the Security Incident Response SOP or related processes are identified and implemented. Internal post-mortems for data breaches are highly confidential records not available to customers. Post-mortems may, however, be summarized and included in other customer event notifications. These reports are provided to external auditors for review as part of Azure's routine audit cycle.

Customer Notification

Microsoft Azure notifies customers and regulatory authorities of data breaches as required. Microsoft relies on heavy internal compartmentalization in the operation of Azure. Data flow logs are also robust. As a benefit of this design, most incidents can be scoped to specific customers. The goal is to provide impacted customers with an accurate, actionable, and timely notice when their data has been breached.

After the declaration of a CRSI, the notification process takes place as expeditiously as possible while still considering the security risks of moving quickly. Generally, the process of drafting notifications occurs as the incident investigation is ongoing. Customer notices are delivered in no more than 72 hours from the time we declared a breach *except* for the following circumstances:

- Microsoft believes the act of performing a notification will increase the risk to other customers. For example, the act of notifying may tip off an adversary causing an inability to remediate.
- Other unusual or extreme circumstances vetted by Microsoft's legal department Corporate External and Legal Affairs (CELA) and the Executive Incident Manager.

Microsoft Azure provides customers with detailed information enabling them to perform internal investigations and assisting them in meeting end user commitments, while not unduly delaying the notification process.

Notification of a personal data breach will be delivered to the customer by any means Microsoft selects, including via email. Notification of a data breach will be delivered to the list of security contacts provided in Azure Security center, which can be configured by following the [implementation guidelines](#). If contact information is not provided in Azure Security Center, the notification will be sent to one or more administrator in an Azure subscription. To ensure that notification can be successfully delivered, it is the customer's responsibility to ensure that the administrative contact information on each applicable subscription and online services portal is correct.

The Microsoft Azure or Azure Government team may also elect to notify additional Microsoft personnel such as Customer Service (CSS) and the customer's Account Manager(s) (AM) or Technical Account Manager(s) (TAM). These individuals often have close relationships with the customer and can facilitate faster remediation

Microsoft InTune Data Breach

Microsoft Intune is key component of the Microsoft Enterprise Mobility and Security Suite cloud service offering. To support the data governance strategy, all Microsoft cloud services are developed with the Microsoft Privacy and Security by Design and Privacy and Security by Default methodologies.

As such Microsoft Intune's cloud service offering follows the same Technical and Organizational measures the Microsoft Azure service team(s) take for securing against data breach processes. Therefore, any information documented in the "Microsoft Azure Data Breach" notification document here is analogous to the Microsoft Intune service as well. For example, Microsoft Intune has the same Security Incident Response Process and Lifecycle (Stage 1: Detect thru Stage 5: Close and Postmortem) and also the same Customer Security Incident Notification process. In addition, Microsoft Intune also fulfills its obligations for Breach Notification for any Microsoft O365 customers using Intune by working directly with the Microsoft O365 team.

For more information about how Microsoft detects and responds to a breach of personal data, see [Data Breach Notification Under the GDPR](#) in the Service Trust Portal.

Learn more

[Microsoft Trust Center](#)

Dynamics 365 and Breach Notification Under the GDPR

2/22/2019 • 9 minutes to read • [Edit Online](#)

Dynamics 365 takes its obligations under the General Data Protection Regulation (GDPR) seriously. Microsoft Dynamics 365 Data Breach

Microsoft works continuously to provide highly secure, enterprise-grade services for Dynamics 365 customers. The information in this section provides a summary of how Microsoft Dynamics 365 protects against security incident/data breach and the process we follow to respond and notify our customers.

Microsoft Dynamics 365 Built-In Security Features

Microsoft Dynamics 365 takes advantage of the cloud service infrastructure and built-in security features to keep data safe using security measures and mechanisms to protect data. In addition, Dynamics 365 provides efficient data access and collaboration with data integrity and privacy in the following areas: [secure identity, data protection, role based security and threat management](#).

Incident Response Training

Each employee working on Microsoft Dynamics 365 is provided with training regarding security incidents and response procedures that are appropriate to their role. Every Microsoft Dynamics 365 employee receives training upon joining, and annual refresher training every year thereafter. The training is designed to provide the employee with a basic understanding of Microsoft's approach to security so that upon completion of training, all employees understand:

- The definition of a security incident;
- The responsibility of all employees to report security incidents;
- How to escalate a potential security incident to Dynamics 365 Security Incident Response team;
- How the Dynamics 365 Security incident Response team responds to security incident;
- Special concerns regarding privacy, particularly customer privacy;
- Where to find additional information about security and privacy, and escalation contacts.

How does Microsoft Dynamics 365 define Security Incident/ Potential Breaches

A security incident/ data breach refers to events such as unlawful access to customer's data stored on Microsoft equipment or in Microsoft facilities, or unauthorized access to such equipment or facilities that has the potential to result in the loss, disclosure or alteration of customer data. Microsoft's goal when responding to security incidents/ data breach is to protect customer data and Dynamics 365 services. Microsoft's approach to managing a security incident conforms to the [National Institute of Standards and Technology](#) (NIST) Special Publication (SP) [800-61](#).

Microsoft does not monitor for or respond to security incidents within the customer's realm of responsibility. A customer-only security compromise would not be processed as a Dynamics 365 security incident and would require the customer tenant to manage the response effort. Customer incident response may involve collaboration with Microsoft Dynamics 365 customer support, given appropriate service contracts.

Detection of Potential Breaches

Dynamics 365 responds to a potential data breach according to the security incident response process, which is a subset of the Microsoft Dynamics 365 incident management plan. Dynamics 365 security incident response is implemented using a five-stage process: Detect, Assess, Diagnose, Stabilize, and Close. The Security Incident Response Team may alternate between the diagnose and stabilize stages as the investigation progresses. An

overview of the security incident response process is below:

	STAGE	DESCRIPTION
1	Detect	First indication of an event investigation.
2	Assess	An on-call incident response team member assesses the impact and severity of the event. Based on evidence, the assessment may or may not result in further escalation to the security response team.
3	Diagnose/ Investigate	Security response experts conduct the technical or forensic investigation, identify containment, mitigation, and workaround strategies. If the security team believes that customer data may have become exposed to an unlawful or unauthorized individual, parallel execution of the Customer Incident Notification process begins in parallel.
4	Stabilize and Recover	The incident response team creates a recovery plan to mitigate the issue. Crisis containment steps such as quarantining impacted systems may occur immediately and in parallel with diagnosis. Longer term mitigations may be planned which occur after the immediate risk has passed.
5	Close and Post-Mortem	The incident response team creates a post-mortem that outlines the details of the incident, with the intention to revise policies, procedures, and processes to prevent a reoccurrence of the event.

The [Dynamics Security Incident Management](#) white paper further details how Microsoft investigates, manages, and responds to security incidents within Dynamics 365.

The detection processes used by Microsoft Dynamics 365 are designed to discover events that risk the confidentiality, integrity, and availability of Dynamics 365 services. Several events can trigger an investigation:

- Automated system alerts via internal monitoring and alerting frameworks. These alerts could come in the way of signature-based alarms such as antimalware, intrusion detection or via algorithms designed to profile expected activity and alert upon anomalies.
- First party reports running Microsoft Dynamics 365 services deployed in Public Cloud and Microsoft Dynamics 365 services deployed in Sovereign Cloud.
- Security vulnerabilities are reported to the [Microsoft Security Response Center \(MSRC\)](#) via secure@microsoft.com. MSRC works with partners and security researchers around the world to help prevent security incidents and to advance Microsoft product security.
- Customer reports that describe suspicious activity attributed to the Microsoft Dynamics 365 Services (as

opposed to activity occurring within the customer's scope of responsibility).

- Security [Red Team and Blue Team](#) activity. This strategy uses a highly-skilled Red team of offensive security experts to uncover and attack potential weaknesses in Microsoft Dynamics 365 services. The security response Blue team must detect and defend against the Red Team's activity. Both Red and Blue Team actions are used to verify that Microsoft Dynamics 365 security response efforts are effectively managing security incidents. Security Red Team and Blue Team activities are operated under requirements of responsibility to help ensure the protection of customer data.
- Escalations by operators of Microsoft Dynamics 365 services. Microsoft employees are trained to identify and escalate potential security issues.

Microsoft Dynamics 365 Data Breach Response

Microsoft assigns the investigation appropriate priority and severity levels by determining the functional impact, recoverability, and information impact of the incident. Both the priority and severity may change over the course of the investigation, based on new findings and conclusions. Security events involving imminent or confirmed risk to customer data are treated as high severity and worked around the clock to resolution. Microsoft Dynamics 365 defines privacy breach as a breach of "personal data of an online service end user or Microsoft employees."

The Security Response Team works with Microsoft Dynamics 365 Security Engineers and Subject Matter Experts (SMEs) to classify the event based on factual data from the evidence. A security event may be classified as:

- **False Positive:** An event that meets detection criteria but is found to be part of a normal business practice and may need to be filtered. The service team will identify the root cause for false positives and will address them in a systematic way leveraging detection sources and fine-tuning them as needed.
- **Security Incident:** An incident where unlawful access to any Customer Data or Support Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data or Support Data has occurred.
- **Customer-Reportable Security Incident (CRSI):** Unlawful or unauthorized access to or use of Microsoft's systems, equipment, or facilities resulting in disclosure, modification, or loss of customer data.
- **Privacy Incident:** A subtype of Security Incident involving personal data. Handling procedures are no different than a security incident.

For a CRSI to be declared, Microsoft must determine that unauthorized access to customer data has or has very likely occurred and/or that there is a legal or contractual commitment that notification must occur. It is desired, but not required, that specific customer impact, resource access, and repair steps be known. An incident is generally declared CRSI after the conclusion of the Diagnose stage of a security incident; however, the declaration may happen at any point that all pertinent information is available. The security incident manager must establish evidence beyond reasonable doubt that a reportable event has occurred to begin execution of the Customer Incident Notification Process.

Throughout the investigation, the security response team works closely with global legal advisors to help ensure that forensics are performed in accordance with legal obligations and commitments to customers. There are also significant restrictions on system and customer data viewing and handling in various operating environments. Sensitive or confidential data, as well as Customer Data, are not transferred out of the production environment without explicit written approval from the Incident Manager recorded in the corresponding incident ticket.

Microsoft verifies that customer and business risk is successfully contained, and that corrective measures are implemented. If necessary, emergency mitigation steps to resolve immediate security risks associated with the event are taken.

Microsoft also completes an internal post-mortem for data breaches. As a part of this exercise, sufficiency of response and operating procedures are evaluated, and any updates that may be necessary to Microsoft's internal security policies or related processes are identified and implemented. Internal post-mortems for data breaches are

highly confidential records not available to customers. Post-mortems may, however, be summarized and included in other customer event notifications. These reports are provided to external auditors for review as part of Dynamics 365 routine audit cycle.

Customer Notification

Microsoft Dynamics 365 notifies customers and regulatory authorities of data breaches as required. Microsoft relies on heavy internal compartmentalization in the operation of Dynamics 365 services. Data flow logs are also robust. As a benefit of this design, most incidents can be scoped to specific customers. The goal is to provide impacted customers with an accurate, actionable, and timely notice when their data has been breached.

The notification process upon a declared CRSI will occur as expeditiously as possible while still considering the security risks of moving quickly. Generally, the process of drafting notifications occurs as the incident investigation is ongoing. Customer notices are delivered promptly from the time we declared a breach *except* for the following circumstances:

- Microsoft believes the act of performing a notification will increase the risk to other customers. For example, the act of notifying may tip off an adversary causing an inability to remediate.
- Other unusual or extreme circumstances vetted by Microsoft's legal department and the Executive Incident Manager.

Microsoft Dynamics 365 provides customers with detailed information enabling them to perform internal investigations and assisting them in meeting end user commitments, while not unduly delaying the notification process.

Notification of a personal data breach will be delivered to the customer by any means Microsoft selects, including via email. Notification of a data breach will be delivered to the list of customer contacts/ admins (only affected tenants) provided in Office Security Center, which is configurable by the customer/ tenant admin. To ensure that notification can be successfully delivered, it is the customer's responsibility to ensure that the administrative contact information on each applicable subscription and online services portal is correct.

The Microsoft Dynamics 365 team may also elect to notify additional Microsoft personnel such as Customer Service (CSS) and the customer's Account Manager(s) (AM) or Technical Account Manager(s) (TAM). These individuals often have close relationships with the customer and can facilitate faster remediation.

Learn more

[Microsoft Trust Center](#)

Microsoft Support and Professional Services and Breach Notification Under the GDPR

2/22/2019 • 7 minutes to read • [Edit Online](#)

Microsoft Support and Professional Services takes its obligations under the General Data Protection Regulation (GDPR) seriously.

Microsoft Professional Services includes a diverse group of technical architects, engineers, consultants, and support professionals dedicated to delivering on the Microsoft mission of empowering customers to do more and achieve more. Our Professional Services team includes more than 21,000+ total consultants, Digital Advisors, Premier Support, engineers, and sales professionals working across 191 countries, supporting 46 different languages, managing several million engagements per month, and engaging in customer and partner interactions through on-premise, phone, web, community and automated tools. The organization brings broad expertise across the Microsoft portfolio, leveraging an extensive network of partners, technical communities, tools, diagnostics and channels that connect us with our enterprise customers.

The drive for Microsoft Professional Services' global data protection incident response team is to (a) employ rigorous operations and processes to prevent data protection incidents from occurring, (b) manage them professionally and efficiently when they do occur, and (c) learn from these data protection incidents through regular post-mortem and program improvements. Microsoft's Professional Services data protection incident response team's processes and results are reviewed and attested to by multiple security and compliance audits (e.g., ISO/IEC 27001).

Data Protection Incident Response Overview

Microsoft Professional Services is committed to protecting its customers and takes considerable measures to prevent data protection incidents from occurring as a means of maintaining customer trust. A data protection incident in the Professional Services organization is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, or Support or Consulting Data, while processed by Microsoft. For Commercial customers that have purchased Premier Support, Unified Support or Microsoft Consulting Services, you should refer to your data protection incident response language in the Professional Services Data Protection Addendum located at <http://aka.ms/professionalservicesdpa/>.

Scope & Limits of Data Protection Incident Response Process

Our personal data breach notification process begins when we declare that a [personal data breach] has occurred.

To be declared, the Microsoft data protection incident response team must determine that a data protection incident as defined above has or has very likely occurred. Declaration will occur as soon as all pertinent information is available to determine that a data protection incident has occurred.

Due to the nature of professional services, some events that seem like Microsoft data protection incidents are not because they occurred through customer's actions or on customer's systems. Microsoft does not monitor for or respond to data protection incidents within the customer's realm of responsibility. However, when Microsoft becomes aware of a customer-driven data protection incident we will classify this as a customer-driven data protection incident, which the data protection incident response team calls an "event," inform the customer of our observation, and as requested will assist them on their response effort, to the extent required by their interaction with Microsoft. Some examples of customer-driven data protection incidents include inadvertent sending Microsoft the customer's passwords and other sensitive data to Microsoft, requests to delete data and being the victim of fraud.

Some actions are out of scope for this process completely, including general questions about our data protection

policies or standards, data subject right requests, opt-out requests, product wish lists or bug reports not related to data protection, data protection incidents not involving customer's data, and fraud against Microsoft.

Types of Data Protection Incidents

The data protection incident response team has identified a set of scenarios that may occur in professional services. While adhering to the basic data protection incident response framework, procedures have been developed and customized to expedite the response process. For instance, a misdirected email may require little investigation. On the other hand, identifying malicious personnel may require a complete forensic investigation due to the surreptitious nature of an offender's activities. This set of scenarios may provide insight into the data protection incident response process for professional services.

Data Protection Incident Response Process

When Microsoft Professional Services identifies a data protection incident, a triage process occurs that (a) assesses the event, (b) determines whether it is in-scope for this process, (c) determines whether it was malicious, (d) performs a preliminary investigation and assigns a severity level, and (e) alerts and coordinates with appropriate stakeholders within Microsoft. The team also begins recording details for tracking purposes and the post-mortem exercise.

Detection

Microsoft Professional Services continuously monitors for emerging data protection incidents across all data stores containing personal data—both online and offline. We use different methods to detect data protection incidents, including automated alerts, customer reports, reports from external parties, observation of anomalies, and indications of malicious or hacker activity.

The detection processes used by Microsoft Professional Services are designed to discover data protection incidents and trigger investigations. For example:

- Security vulnerabilities are reported to the Microsoft-wide reporting system for referral or reported directly to the Professional Services data protection incident response team.
- Customers submit reports via the [Customer Support Portal](#) that describe suspicious activity.
- Professional Services personnel submit escalations. Microsoft employees are trained to identify and escalate potential security issues.
- For tools and systems used in the process of providing Professional Services, the operations teams use automated system alerts via internal monitoring and alerting frameworks. These alerts could come in the way of signature-based alarms such as antimalware, intrusion detection or via algorithms designed to profile expected activity and alert upon anomalies.

Data Protection Incident Response Drills, Testing of Data Protection Incident Response Plan

In addition to ongoing training, each year Professional Services executes drills in partnership with appropriate internal departments to communicate the data protection incident escalation procedures, roles, and responsibilities to all stabilization team members. This prepares key stakeholders for real-world data protection incidents—whether security, physical, or privacy in nature. This includes exercises with representatives of the data protection incident response team, security team, legal teams and communications team.

After the exercises, we document the outcome and remediation methods we have decided to use.

Data Protection Incident Response Training

A key component of data protection incident response is personnel training to identify and report data protection incidents. Personnel in the Professional Services organization are required to take training that covers privacy fundamentals, GDPR regulations, and best practices on how to identify and report data protection incidents.

Regular online training is available, and completion is mandatory for all personnel. The training program employs testing, ongoing surveys, awareness, and follow-up designed to ensure that training is being understood and retained.

Process

When Microsoft Professional Services organization identifies a data protection incident, it follows a documented industry standard response plan, beginning with determination that the data protection incident criteria are met. Where a data protection incident occurs, it is generally declared immediately after Triage but, depending on complexity, the declaration may happen at any point when a level of necessary information is available, including after the investigation stage. On the other hand, the team has discretion to declare a data protection incident based only on reasonable suspicion of occurrence. The team may also alternate between the various stages as the investigation progresses.

Microsoft also completes an internal post-mortem for data protection incidents. As a part of this exercise, sufficiency of response and operating procedures are evaluated, and any updates that may be necessary to the *Data Protection Incident Response Standard Operating Procedure* or related processes are identified and implemented. Internal post-mortems for data breaches are highly confidential records not available to customers. Post-mortems may, however, be summarized and included in customer event notifications. As part of a routine audit cycle, post-mortem processes are reviewed by external auditors to ensure follow-up occurs.

Notification

When Microsoft Professional Services declares a data protection incident under the GDPR, we target notification to our customers within 72 hours. This 72-hour notice obligation is a policy commitment of Professional Services—not a legal requirement under the GDPR.

After the declaration of an data protection incident, the notification process takes place as expeditiously as possible while still considering the security risks of moving quickly. To ensure that notification can be successfully delivered, it is the customer's responsibility to ensure that the administrative contact information on each applicable account, subscription and online services portal is correct. While the goal is to provide impacted customers with an accurate, actionable, and timely notice, to achieve the 72-hour notification commitment the initial notification may not include complete details as all details may not be available during the early stages of an data protection incident. In addition, Microsoft may need to withhold some details due to the circumstances of the data protection incident. For instance, it may be necessary to withhold details if the act of providing notification increases risk to other customers or interferes with Microsoft's or law enforcement's ability to catch a malicious actor.

In its capacity as a data processor, Microsoft recognizes that customers are responsible for determining whether notification is appropriate and, if so, notifying the competent Data Protection Authority (DPA) and the customer's own data subjects of any personal data breach. Microsoft Professional Services will work to provide customers the information needed to proceed with notice in these circumstances.

When providing notice to customers of a personal data breach, Microsoft will include the following information, if applicable and known:

- Nature of the breach
- Mitigation measures Microsoft is taking or proposing
- Product, service, application involved
- Length of time personal data was exposed, if known
- Volume of affected/exposed personal data records, if known
- Sub-processor/supplier details, if one is involved in the breach

Learn more

Find out more about [Microsoft Professional Services](#) and by going to the Microsoft Professional Services section on the Microsoft Trust Center (<https://www.microsoft.com/trustcenter/cloudservices/commercialsupport>).

Data Protection Impact Assessments

2/22/2019 • 2 minutes to read • [Edit Online](#)

Under the General Data Protection Regulation (GDPR), data controllers are required to prepare a Data Protection Impact Assessment (DPIA) for processing operations that are “likely to result in a high risk to the rights and freedoms of natural persons.” There is nothing inherent in Microsoft Azure or Dynamics 365 that would necessarily require the creation of a DPIA by a Data Controller using it. Rather, whether a DPIA is required will be dependent on the details and context of *how* the data controller deploys, configures each product.

The purpose of this document is to provide data controllers with information that will help them to determine whether a DPIA is needed and, if so, what details to include.

- [Office 365](#)
- [Azure](#)
- [Dynamics 365](#)
- [Microsoft Support and Professional Services](#)

For more information about GDPR compliance Microsoft data protection, see [Compliance](#) in the ***Service Trust Portal***.

Learn more

[Microsoft Trust Center](#)

Data Protection Impact Assessments: Guidance for Data Controllers Using Microsoft Office 365

2/22/2019 • 12 minutes to read • [Edit Online](#)

Under the General Data Protection Regulation (GDPR), data controllers are required to prepare a Data Protection Impact Assessment (DPIA) for processing operations that are "likely to result in a high risk to the rights and freedoms of natural persons." There is nothing inherent in Microsoft Office 365 that would necessarily require the creation of a DPIA by a data controller using it. Rather, whether a DPIA is required will be dependent on the details and context of how the data controller deploys, configures, and uses Office 365.

The purpose of this document is to provide data controllers with information about Office 365 that will help them to determine whether a DPIA is needed and if so, what details to include. It applies to Office 365 applications and services, including but not limited to Exchange Online, SharePoint Online, OneDrive for Business, Yammer, Skype for Business, and Power BI. (See, for example, Tables 1 and 2 of the Office 365 Data Subject Request Guide.)

Part 1 – Determining Whether a DPIA is Needed

Article 35 of the GDPR requires a data controller to create a Data Protection Impact Assessment "[w]here a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons." It further sets out particular factors that would indicate such a high risk, which are discussed in the following table. In determining whether a DPIA is needed, a data controller should consider these factors, along with any other relevant factors, in light of the controller's specific implementation(s) and use(s) of Office 365.

Table 1 - Risk factors and relevant information about Office 365

Risk Factor	Relevant Information about Office 365
A systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person	<p>Depending upon the data controller's configuration, Office 365 may perform certain automated processing of data, such as the analysis performed by Workplace Analytics that allows the data controller to derive insights on how people collaborate within an organization based on email and calendar header information from user's mailboxes.</p> <p>Office 365 is not designed to perform automated processing as the basis for decisions that produce legal or similarly significant effects on individuals. However, because Office 365 is a highly-customizable service, a data controller could potentially use it for such processing.</p>
Processing on a large scale ¹ of special categories of data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation), or of personal data relating to criminal convictions and offences	<p>Office 365 is not specifically designed to process special categories of personal data.</p> <p>However, a data controller could use Office 365 to process the enumerated special categories of data. Office 365 is a highly-customizable service that enables the customer to track or otherwise process any type of personal data, including special categories of personal data. Any such use is relevant to a controller's determination of whether a DPIA is needed. But as the data processor, Microsoft has no control over such use and typically would have little or no insight into such use.</p>

Processing on a large scale* of special categories of data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation), or of personal data relating to criminal convictions and offences	Office 365 is not specifically designed to process special categories of personal data. However, a data controller could use Office 365 to process the enumerated special categories of data. Office 365 is a highly-customizable service that enables the customer to track or otherwise process any type of personal data, including special categories of personal data. Any such use is relevant to a controller's determination of whether a DPIA is needed. But as the data processor, Microsoft has no control over such use and typically would have little or no insight into such use.
A systematic monitoring of a publicly accessible area on a large scale	Office 365 is not designed to conduct or facilitate such monitoring. However, a data controller could use it to process data collected through such monitoring

[*] With respect to the criteria that the processing be on a "large scale," Recital 91 of the GDPR clarifies that: "The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory."

Part 2 – Contents of a DPIA

Article 35(7) mandates that a Data Protection Impact Assessment specify the purposes of processing and a systematic description of the envisioned processing. In Microsoft's DPIAs, such systematic description includes factors such as the types of data processed, how long data is retained, where the data is located and transferred, and what third parties may have access to the data. In addition, the DPIA must include:

- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of natural persons; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

The table below provides key information from Microsoft that can help with your DPIA drafting. It contains information about Office 365 that is relevant to each of the required elements of a DPIA. As in Part 1, data controllers must consider the details provided below, along with the details of its own specific implementation(s) and use(s) of Office 365.

Table 2 - Elements of and relevant factors about Office 365

Risk Factors	Relevant Information About Office 365
--------------	---------------------------------------

Purpose(s) of processing	<p>The purpose(s) of processing data using Office 365 is determined by the controller that implements, configures, and uses it.</p> <p>As specified by the Online Services Terms, Microsoft, as a data processor, processes Customer Data only to provide the requested services to our customer, the data controller, including purposes compatible with providing those services. Microsoft will not use Customer Data or information derived from it for any advertising or similar commercial purposes.</p>
Categories of personal data processed	<p>[Customer Data]</p> <p>This is all data, including text, sound, video, or image files and software, that customers provide to Microsoft or that is provided on customers' behalf through their use of Microsoft online services. It includes data that customers upload for storage or processing, as well as customizations. Examples of Customer Data processed in Office 365 include email content in Exchange Online, and documents or files stored in SharePoint Online or OneDrive for Business.</p> <p>[System-generated Log Data]</p> <p>This is data that Microsoft generates to run the service, such as use or performance data. Most of these data contain pseudonymous identifiers generated by Microsoft.</p> <p>[Support Data]</p> <p>This is data provided to Microsoft by or on behalf of Customer (or that Customer authorizes Microsoft to obtain from an Online Service) through an engagement with Microsoft to obtain technical support for Online Services.</p> <p>Customer Data, System-generated Log Data, and Support Data do not include administrator and billing data, such as customer administrator contact information, subscription information, and payment data, which Microsoft collects and processes in its capacity as a data controller and which is outside the scope of this document.</p>

<p>Data retention</p>	<p>[Customer Data],</p> <p>As set out in the Data Protection Terms in the Online Services Terms, Microsoft will retain Customer Data for the duration of the customer's right to use the service and until all Customer Data is deleted or returned in accordance with the customer's instructions or the terms of the Online Services Terms.</p> <p>At all times during the term of the customer's subscription, the customer will have the ability to access, extract, and delete Customer Data stored in the service, subject in some cases to specific product functionality intended to mitigate the risk of inadvertent deletion (e.g., Exchange recovered items folder), as further described in product documentation.</p> <p>Except for free trials and LinkedIn services, Microsoft will retain Customer Data stored in the Online Service in a limited function account for 90 days after expiration or termination of the customer's subscription so that the customer may extract the data. After the 90-day retention period ends, Microsoft will disable the customer's account and delete the Customer Data.</p> <p>[System-generated Log Data]</p> <p>This data is retained for a default period of up to 180 days from collection, subject to longer retention periods where required for security of the services or to meet legal or regulatory obligations.</p> <p>For further information about service capability that enable the customer to delete personal data maintained in the service at any time, see the Office 365 Data Subject Requests Guide.</p>
<p>Location and transfers of personal data</p>	<p>As described in the Data Protection Terms of the Online Services Terms, if Customer provisions its instance of Office 365 in Australia, Canada, the European Union, France, India, Japan, South Korea, the United Kingdom, or the United States, Microsoft will store the following Customer Data at rest only within that location: (1) Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments), (2) SharePoint Online site content and the files stored within that site, (3) files uploaded to OneDrive for Business, and (4) project content uploaded to Project Online.</p> <p>For other types of personal data from the European Economic Area and Switzerland, Microsoft will ensure that transfers of personal data to a third country or an international organization are subject to appropriate safeguards as described in Article 46 of the GDPR. In addition to Microsoft commitments under the Standard Contractual Clauses for processors and other model contracts, Microsoft is certified to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks and the commitments they entail.</p>

Data sharing with third-party subprocessors	<p>Microsoft shares data with third parties acting as our subprocessors to support functions such as customer and technical support, service maintenance, and other operations. Any subcontractors to which Microsoft transfers Customer Data or Support Data will have entered into written agreements with Microsoft that are no less protective than the Data Protection Terms of the Online Services Terms. All third-party subprocessors with which Customer Data from Microsoft's Core Online Services is shared are included in the Online Services Subcontractor list. All third-party subprocessors that may access Support Data (including Customer Data that customers choose to share during their support interactions) are included in the Microsoft Commercial Support Contractors list.</p>
Data sharing with independent third-parties	<p>Some Office 365 products include extensibility options that enable, at the controller's election, sharing of data with independent third parties. For example, Exchange Online is an extensible platform that allows third-party add-ins or connectors to integrate with Outlook and extend Outlook's feature sets. These third-party providers of add-ins or connectors act independently of Microsoft, and their add-ins or connectors must be enabled by the users or enterprise administrators, who authenticates with their add-in or connector account.</p> <p>Microsoft will not disclose Customer Data or Support Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Customer Data or Support Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose Customer Data or Support Data to law enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.</p> <p>Upon receipt of any other third-party request for Customer Data or Support Data, Microsoft will promptly notify Customer unless prohibited by law. Microsoft will reject the request unless required by law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from the customer.</p>
Data subject rights	<p>When operating as a processor, Microsoft makes available to customers (data controllers) the personal data of its data subjects and the ability to fulfill data subject requests when they exercise their rights under the GDPR. We do so in a manner consistent with the functionality of the product and our role as a processor. If we receive a request from the customer's data subjects to exercise one or more of its rights under the GDPR, we redirect the data subject to make its request directly to the data controller.</p> <p>The Office 365 Data Subject Requests Guide provides a description to the data controller on how to support data subject rights using the capabilities in Office 365.</p>

<p>An assessment of the necessity and proportionality of the processing operations in relation to the purposes</p>	<p>Such an assessment will depend on the controller's needs and purposes of processing.</p> <p>With regard to the processing carried out by Microsoft, such processing is necessary and proportional for the purpose of providing the services to the data controller.</p>
<p>An assessment of the risks to the rights and freedoms of data subjects</p>	<p>The key risks to the rights and freedoms of data subjects from the use of Office 365 will be a function of how and in what context the data controller implements, configures, and uses it.</p> <p>However, as with any service, personal data held in the service may be at risk of unauthorized access or inadvertent disclosure. Measures Microsoft takes to address such risks are discussed below.</p>
<p>The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned</p>	<p>Microsoft is committed to helping protect the security of Customer's information. In compliance with the provisions of Article 32 of the GDPR, Microsoft has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Customer Data and Support Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction.</p> <p>Further, Microsoft complies with all other GDPR obligations that apply to data processors, including but not limited to, data protection impact assessments and record keeping.</p>

Learn more

[Microsoft Trust Center](#)

Data Protection Impact Assessments: Guidance for Data Controllers Using Microsoft Azure

2/25/2019 • 10 minutes to read • [Edit Online](#)

Under the General Data Protection Regulation (GDPR), data controllers are required to prepare a Data Protection Impact Assessment (DPIA) for processing operations that are "likely to result in a high risk to the rights and freedoms of natural persons." There is nothing inherent in Microsoft Azure itself that would necessarily require the creation of a DPIA by a data controller using it. Rather, whether a DPIA is required will be dependent on the details and context of *how* the data controller deploys, configures, and uses Microsoft Azure.

The purpose of this document is to provide data controllers with information about Microsoft Azure that will help them to determine whether a DPIA is needed and, if so, what details to include.^[^1]

Part 1 – Determining Whether a DPIA is Needed

Article 35 of the GDPR requires a data controller to create a Data Protection Impact Assessment (DPIA) "[w]here a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons." It further sets out particular factors that would indicate such a high risk, which are discussed in the following table. In determining whether a DPIA is needed, a data controller should consider these factors, along with any other relevant factors, in light of the controller's specific implementation(s) and use(s) of Microsoft Azure.

Table 1 - Azure DPIA risk factors

High Risk Factor	Relevant Information about Microsoft Azure
A systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.	Microsoft Azure does not provide capabilities to perform certain automated processing of data. <i>However, because Azure is a highly-customizable service, a data controller could potentially configure it to be used for such processing.</i> Controllers should make this determination based on their usage of Azure.

<p>Processing on a large scale of special categories of data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation), or of personal data relating to criminal convictions and offences.</p>	<p>Microsoft Azure is not specifically designed to process special categories of personal data and the usage of Azure does not increase the inherent risk of a controller's processing.</p> <p><i>However, a data controller could use Microsoft Azure to process the enumerated special categories of data.</i> Microsoft Azure is a highly-customizable service that enables the customer to track or otherwise process any type of data, including special categories of personal data. But as the data processor, Microsoft has no control over such use and has little or no insight into such use. It is incumbent upon the data controller to determine appropriate uses of the data controller's data.</p>	
<p>A systematic monitoring of a publicly accessible area on a large scale.</p>	<p>Microsoft Azure is not designed to conduct or facilitate such monitoring.</p> <p><i>However, a data controller could use Azure to process data collected through such monitoring.</i> Microsoft Azure is a highly-customizable service that enables the customer to track or otherwise process any type of data, including monitoring data. But as the data processor, Microsoft has no control over such use and has little or no insight into such use. It is incumbent upon the data controller to determine appropriate uses of the data controller's data.</p>	

Part 2 – Contents of a DPIA

Article 35(7) mandates that a Data Protection Impact Assessment specify the purposes of processing and a systematic description of the envisioned processing. A systematic description of a comprehensive DPIA might include factors such as the types of data processed, how long data is retained, where the data is located and transferred, and what third parties may have access to the data. In addition, the DPIA must include:

- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of natural persons; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

The table below contains information about Microsoft Azure that is relevant to each of those elements. As in Part 1, data controllers must consider the details provided below, along with any other relevant factors, in the context of the controller's specific implementation(s) and use(s) of Microsoft Azure.

Table 2 - Azure DPPIA elements

Element of a DPPIA	Relevant Information About Microsoft Azure
Purpose(s) of processing	<p>The purpose(s) of processing data using Microsoft Azure is determined by the controller that implements, configures, and uses it.</p> <p>As specified by the Online Services Terms (OST), Microsoft, as a data processor, processes Customer Data only to provide the requested services to our customer, the data controller. Microsoft will not use Customer Data or information derived from it for any advertising or similar commercial purposes.</p>

Categories of personal data processed

Customer Data - All data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, a customer through use of the enterprise service. Customer Data includes both (1) identifiable information of end users (e.g., user names and contact information in Azure Active Directory) and customer content that a customer uploads into or creates in specific services (e.g., customer content in an Azure Storage account, customer content of an Azure SQL Database, or a customer's virtual machine image in Azure Virtual Machines).

System-Generated Logs - Logs and related data generated by Microsoft that help Microsoft provide enterprise services to users. System-generated logs contain primarily pseudonymized data, such as unique identifiers generated by the system, that cannot on their own identify an individual person but are used to deliver the enterprise services to users. System-generated logs may also contain identifiable information about end users, such as a user name.

Support Data - This is data provided to Microsoft by or on behalf of Customer (or that Customer authorizes Microsoft to obtain from an Online Service) through an engagement with Microsoft to obtain technical support for Online Services.

For additional details regarding data processed by Azure, see the [Online Services Terms](#), as well as [Microsoft Trust Center](#).

Data retention	<p>Microsoft will retain and process Customer Data for the duration of the Customer's right to use the Online Service and until all Customer Data is retrieved by Customer or deleted in accordance with the terms of the OST.</p> <p>At all times during the term of Customer's subscription, the Customer will have the ability to access and extract Customer Data stored in each Online Service. Except for free trials and LinkedIn services, Microsoft will retain Customer Data stored in the Online Service in a limited function account for 90 days after expiration or termination of Customer's subscription so that Customer may extract the data. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data. The customer can delete personal data pursuant to a Data Subject Request using the capabilities described in the Azure Data Subject Request GDPR Documentation.</p>	
Location and transfers of personal data	<p>Customers have the ability to provision Customer Data at rest within specified geographic regions, subject to certain exceptions as set out in the OST.</p> <p>Additional details regarding service deployments and data residency can also be found at the Azure Global Infrastructure webpage.</p> <p>For personal data from the European Economic Area and Switzerland, Microsoft will ensure that transfers of Personal Data to a third country or an international organization are subject to appropriate safeguards as described in Article 46 of the GDPR. In addition to Microsoft's commitments under the Standard Contractual Clauses for processors and other model contracts, Microsoft is certified to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks and the commitments they entail.</p>	

Data sharing with third parties	<p>Microsoft shares data with third parties acting as our subprocessors (i.e., subcontractors which process personal data) to support functions such as customer and technical support, service maintenance, and other operations. Any subcontractors to which Microsoft transfers Customer Data or Support Data will have entered into written agreements with Microsoft that are no less protective than the Data Protection Terms of the Online Services Terms. All third-party subcontractors with which Customer Data or Support Data is shared are included in the Lists of subcontractors (see "We limit access by subprocessors").</p> <p>Information regarding Microsoft's response to law enforcement and third party requests for Customer Data and Support Data is located in the Online Services Terms. Unless Microsoft is legally prohibited from doing so, Microsoft will attempt to redirect the law enforcement agency or third party directly to the Customer.</p>	
Data subject rights	<p>When operating as a processor, Microsoft makes available to the customer (a.k.a. the data controller) the personal data of its data subjects and the ability to fulfill data subject requests when they exercise their rights under the GDPR. Microsoft does so in a manner consistent with the functionality of the product and its role as a data processor. If Microsoft receives a request from the customer's data subjects to exercise one or more of its rights under the GDPR, the request will be redirected to the data controller.</p> <p>The Azure Data Subject Request GDPR Documentation provides a description of how to support data subject rights using the capabilities in Azure.</p>	
An assessment of the necessity and proportionality of the processing operations in relation to the purposes	<p>Such an assessment will depend on the data controller's needs and purposes of processing.</p> <p>With regard to the processing carried out by Microsoft, such processing is necessary and proportional for the purpose of providing the services to the data controller. Microsoft makes this commitment in the OST.</p>	

<p>An assessment of the risks to the rights and freedoms of data subjects</p>	<p>The key risks to the rights and freedoms of data subjects from the use of Microsoft Azure will be a function of how and in what context the data controller implements, configures, and uses Microsoft Azure.</p> <p>However, as with any service, personal data held in the service may be at risk of unauthorized access or inadvertent disclosure. Measures Microsoft takes to address such risks are discussed in the OST, as further detailed below.</p>	
<p>The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned</p>	<p>Microsoft is committed to helping protect the security of Customer Data. The security measures Microsoft takes are described in detail in the OST.</p> <p>Microsoft complies with strict security standards and industry-leading data protection methodology. Microsoft is continually improving its systems to deal with new threats. More information regarding cloud governance and privacy practices is available at Trust Center's Cloud Governance & Privacy page.</p> <p>Microsoft takes reasonable and appropriate technical and organizational measures to safeguard the personal data that it processes. These measures include, but are not limited to, internal privacy policies and practices, contractual commitments, and international and regional standard certifications. More information is available at Trust Center's Privacy Standards page.</p> <p>Microsoft provides significant, transparent customer facing security and privacy materials to help explain Microsoft's use and processing of personal data. Customers are encouraged to contact Microsoft with questions.</p> <p>Further, Microsoft complies with all other GDPR obligations that apply to data processors, including but not limited to, data protection impact assessments and record keeping.</p>	

[^1]: Microsoft is not providing any legal advice in this document. This document is being provided for informational purposes only. Customers are encouraged to work with their privacy officers and legal counsel to

determine the necessity and content of any DPIAs related to their use of Microsoft Azure or any other Microsoft online service.

Learn more

[Microsoft Trust Center](#)

Data Protection Impact Assessments: Guidance for Data Controllers Using Dynamics 365

2/22/2019 • 10 minutes to read • [Edit Online](#)

Under the General Data Protection Regulation (GDPR), data controllers are required to prepare a Data Protection Impact Assessment (DPIA) for processing operations that are "likely to result in a high risk to the rights and freedoms of natural persons." There is nothing inherent in Dynamics 365 that would necessarily require the creation of a DPIA by a Data Controller using it. Rather, whether a DPIA is required will be dependent on the details and context of *how* the data controller deploys, configures, and uses Dynamics 365.

The purpose of this document is to provide data controllers with information about Dynamics 365 that will help them to determine whether a DPIA is needed and, if so, what details to include.

Part 1 – Determining Whether A DPIA is Needed

Article 35 of the GDPR requires a data controller to create a Data Protection Impact Assessment "[w]here a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons." It further sets out particular factors that would indicate such a high risk, which are discussed in the following table. In determining whether a DPIA is needed, a data controller should consider these factors, along with any other relevant factors, in light of the controller's specific implementation(s) and use(s) of Dynamics 365.

Table 1 - High risk factors in Dynamics 365

Risk Factor	Relevant Information about Dynamics 365
A systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;	Dynamics 365 does perform certain automated processing of data, such as lead or opportunity scoring (e.g. predicting how likely a sale is to occur). But it is not designed to perform processing on which decisions are based that produce legal or similarly significant effects on individuals. However, because Dynamics 365 is a highly-customizable service, a data controller could potentially configure it to be used for such processing, such as scoring for employment decisions or credit applications.

<p>Processing on a large scale[^1] of special categories of data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation), or of personal data relating to criminal convictions and offences;</p>	<p>Dynamics 365 is not specifically designed to process special categories of personal data. However, a data controller <i>could</i> use Dynamics 365 to process the enumerated special categories of data. For instance, Dynamics 365 offers healthcare industry templates which could be used to process personal data associated with a health condition. Further, Dynamics 365 is a highly-customizable service that enables the customer to track or otherwise process any type of personal data, including special categories of personal data. But as the data processor, Microsoft has no control over such use and typically would have little or no insight into such use.</p>	
<p>A systematic monitoring of a publicly accessible area on a large scale</p>	<p>Dynamics 365 is not designed to conduct or facilitate such monitoring. However, a data controller could use it to process data collected through such monitoring.</p>	

Part 2 – Contents of a DPIA

Article 35(7) mandates that a Data Protection Impact Assessment specify the purposes of processing and a systematic description of the envisioned processing. A systematic description of a comprehensive DPIA might include factors such as the types of data processed, how long data is retained, where the data is located and transferred, and what third parties may have access to the data. In addition, the DPIA must include:

- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of natural persons; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

The table below contains information about Dynamics 365 that is relevant to each of those elements. As in Part 1, data controllers must consider the details provided below, along with any other relevant factors, in the context of the controller's specific implementation(s) and use(s) of Dynamics 365.

Table 2 - Contents of a DPIA

Elements of a DPIA	Relevant Information About Dynamics 365	
Purpose(s) of processing	The purpose(s) of processing data using Dynamics 365 is determined by the controller that implements, configures,	

and uses it.

Dynamics 365 is an online platform for processing that is made up of several discrete online services, each of which has distinct purposes of processing. Below are the types of services offered by Dynamics 365:

Customer Engagement at its core is a customer relationship management service. It includes the following online services: Dynamics 365 for Sales, Dynamics 365 for Marketing, Dynamics 365 for Customer Service, Dynamics 365 for Project Service, and Dynamics 365 for Field Service.

Dynamics 365 for Finance and Operations, Enterprise edition (D365FOEE) is an enterprise resource planning suite offered as a software as a service (SaaS), that is provided primarily to enterprise customer management of Sales, Service, Finance and Operations, Manufacturing and Human Resources.

Dynamics 365 for Retail (D365FR) is offered as a software as a service (SaaS) with integrated on-premise point-of-sale solutions for enterprise retailers and distributors.

Dynamics 365 Lifecycle Services (LCS) is an ancillary online service, used primarily by enterprise customers in the deployment, management, and maintenance of the customer's D365FOEE, D365FR implementations.

Dynamics 365 for Business Central is an enterprise resource planning offering, provided as a Software as a Service (SaaS) by Microsoft to small and medium-sized enterprises. The service processes personal data to assist with finance, manufacturing, customer relationship management, supply chains, analytics and electronic commerce.

Dynamics 365 for Talent is offered as a software as a service (SaaS), that provides customers with the management of Human resources and consists of the following services:

- *Core HR* - A service to streamline recordkeeping tasks and automate processes related to staffing an organization. These processes include employee retention, benefits administration,

	<p>compensation, training, performance reviews, and change management.</p> <ul style="list-style-type: none"> - <i>Attract</i>- a service to find, interview, and hire personnel. - <i>Onboarding</i>- a service to help onboard new hires into their job.
Microsoft Social Engagement	<p>(MSE) is an ancillary service to Dynamics 365 offered to enterprise customers to (i) enable processing of public social media posts and personal data posted by data subjects in a limited number of social media outlets to help them analyze and identify topics of interest (e.g. trends), and manage corporate or institutional presence in these virtual places (e.g. fan pages), including publishing content to specific social media outlets (listen); and (ii) engage directly with data subjects via private communications in social media (engage).</p>
	<p>In its processor capacity operating the services enumerated above, Dynamics 365 processes personal data only to provide customers its online services as described, including purposes compatible with providing those services such as personalization, security, fraud and malware prevention, troubleshooting and improvement.</p>
	<p>Microsoft processes data on behalf of the customer (tenant) as necessary to provide the requested service as set forth in our Online Services Terms.</p>

Data retention	<p>Microsoft will retain Customer Data for the duration of the customer's right to use the service and until all Customer Data is deleted or returned in accordance with the customer's instructions or the terms of the Online Services Terms. At all times during the term of the customer's subscription, the customer will have the ability to access and extract Customer Data stored in the service. Microsoft will retain Customer Data stored in the Online Service in a limited function account for 90 days after expiration or termination of the customer's subscription so that the customer may extract the data. After the 90-day retention period ends, Microsoft will disable the customer's account and delete the Customer Data. The customer can delete Customer Data and Pseudonymous data at any time using the capabilities described in the Dynamics' <i>Data Subject Rights Guide</i>.</p>	
Location and transfers of personal data	<p>If Customer provisions its instance of Dynamics 365 Core Services in Australia, Canada, the European Union, India, Japan, the United Kingdom or the United States, Microsoft will store Customer Data at rest within the specified geographic area, subject to certain exceptions as set out in the Online Services Terms. Detailed information about Customer Data storage can be found in the Trust Center. For personal data from the European Economic Area and Switzerland, Microsoft will ensure that transfers of Personal Data to a third country or an international organization are subject to appropriate safeguards as described in Article 46 of the GDPR. In addition to Microsoft's commitments under the Standard Contractual Clauses for processors and other model contracts, Microsoft is certified to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks and the commitments they entail.</p>	

Data subject rights	<p>When operating as a processor, Microsoft makes available to customer (data controllers) the personal data of their data subjects and the ability to fulfill data subject requests when they exercise their rights under the GDPR. We do so in a manner consistent with the functionality of the product and our role as a processor. If we receive a request from a customer's data subjects to exercise one or more of its rights under the GDPR, we redirect the data subject to make its request directly to the data controller.</p> <p>The <i>Dynamics 365 Data Subject Request GDPR Documentation</i> provides a description of how to support data subject rights using the capabilities in Dynamics</p>	
An assessment of the necessity and proportionality of the processing operations in relation to the purposes	<p>Such an assessment will depend on the controller's needs and purposes of processing.</p> <p>In its processor capacity, Microsoft offers D365 to process personal data only to provide customers its online services, including purposes compatible with providing those services such as personalization to the customer, security, fraud and malware prevention, troubleshooting and improvement. Microsoft processes data on behalf of the customer (tenant) as necessary to provide the requested service as set forth in our Online Services Terms found at http://microsoft.com/licensing/contracts.</p>	
An assessment of the risks to the rights and freedoms of data subjects	<p>The key risks to the rights and freedoms of data subjects from the use of Dynamics 365 will be a function of how and in what context the data controller implements, configures, and uses it.</p> <p>However, as with any service, personal data held in the service may be at risk of unauthorized access or inadvertent disclosure. Measures Microsoft takes to address such risks are discussed below.</p>	

<p>The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned</p>	<p>Microsoft is committed to helping protect the security of Customer's information. In compliance with the provisions of Article 32 of the GDPR, Microsoft has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Customer Data and Support Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction.</p> <p>For detailed list of MS managed controls (technical and business process controls) for security implemented by Dynamics 365 please visit the Service Trust Portal. Further, Microsoft complies with all other GDPR obligations that apply to data processors, including but not limited to, providing data protection impact assessments and accurate record keeping.</p>	
---	---	--

[^1]: With respect to the criteria that the processing be on a "large scale," Recital 91 of the GDPR clarifies that: "The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory."

[Learn more](#)

[Microsoft Trust Center](#)

Data Protection Impact Assessments: Guidance for Data Controllers Using Microsoft Professional Services

2/22/2019 • 11 minutes to read • [Edit Online](#)

Introduction to Microsoft Professional Services

Microsoft Professional Services includes a diverse group of technical architects, engineers, consultants, and support professionals dedicated to delivering on Microsoft's mission of empowering customers to do more and achieve more. Find out more about Microsoft Professional Services here (https://www.microsoft.com/microsoftservices/professional_services.aspx) and by going to the Microsoft Professional Services section on the Microsoft Trust Center (<https://www.microsoft.com/trustcenter/cloudservices/commercialsupport>).

Microsoft Professional Services takes its obligations under the General Data Protection Regulation (GDPR) seriously. The information in this document is designed to provide information about how Microsoft's support and consulting offerings that customers can use when preparing Data Protection Impact Assessments (DPIAs) under GDPR.

Introduction to DPIAs

Under the General Data Protection Regulation (GDPR), data controllers are required to prepare a DPA for processing operations that are "likely to result in a high risk to the rights and freedoms of natural persons." There is nothing inherent in Microsoft Professional Services that would necessarily require the creation of a DPA by a data controller using it. Rather, whether a DPA is required will be dependent on the details and context of the type of services and how the data controller uses the professional services.

The purpose of this document is to provide data controllers with information about Professional Services that will help them to determine whether a DPA is needed and, if so, what details to include.

Part 1 – Determining Whether A DPA is Needed

Article 35 of the GDPR requires a data controller to create a Data Protection Impact Assessment "[w]here a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons." It further sets out particular factors that would indicate such a high risk, which are discussed in the following table. In determining whether a DPA is needed, a data controller should consider these factors, along with any other relevant factors, in light of the data controller's specific implementation(s) and use(s) of Professional Services.

Table 1 - Risk factors and relevant information

Risk Factor	Relevant Information about Professional Services

<p>A systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;</p>	<p>Professional Services does perform certain routine or automated processing of data, such as break/fix support (e.g., assisting customers when their computer breaks), account migration, and analysis of system vulnerabilities. Professional Services solutions, excluding customer development covered under the note below, are not intended to perform processing on which decisions are based that produce legal or similarly significant effects on individuals.</p>
<p>Processing on a large scale^[^1] of special categories of data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation), or of personal data relating to criminal convictions and offences;</p>	<p>Professional Services are not intended to be utilized in work that requires the processing of special categories of personal data, excluding customer development covered under the note below.</p> <p>However, a data controller could use Professional Services consulting solutions to process the enumerated special categories of data. For instance, Professional Services offers healthcare industry database development which could be used by a data controller to process personal data associated with a health condition. It is the responsibility of the controller to assess and either restrict or document this usage as appropriate.</p>
<p>A systematic monitoring of a publicly accessible area on a large scale</p>	<p>Professional Services are not intended to be utilized in work that requires or facilitates such monitoring, excluding customer development covered under the note below.</p> <p>If a data controller used Professional Services to develop this type of system or used IT systems to process data collected through such monitoring than it would be the responsibility of the data controller as described below.</p>

[Custom Development Note] Professional Services offers a wide variety of consulting solutions. A data controller could potentially request a solution that, in accordance with the above criteria, would be a high-risk solution. For instance, a data controller may request that Professional Services create a solution to develop a business intelligence engine for employment decisions or credit applications or a solution that involves user tracking, specialized use of Artificial Intelligence (AI)/Analytics, or processing of special categories of personal data.

At the start of an engagement, Professional Services has processes to evaluate and address high-risk solutions it may be asked to work on. As part of this, Professional Services may require assurances from the data controller on GDPR compliance (e.g. contractual terms), a plan for development of a DPIA, or other criteria (e.g. agreed operating guidelines) as required of a data processor under the GDPR. However, regardless of Microsoft's actions it is the responsibility of the data controller to develop the DPIA with input where applicable from the processor of the customer's data.

Part 2 – Contents of a DPIA

Article 35(7) mandates that a Data Protection Impact Assessment specify the purposes of processing and a systematic description of the envisioned processing. A systematic description of a comprehensive DPIA might include factors such as the types of data processed, how long data is retained, where the data is located and transferred, and what third parties may have access to the data. In addition, the DPIA must include:

- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of natural persons; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to

ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

The table below contains information about Professional Services that is relevant to each of those elements. As in Part 1, data controllers must consider the details provided below, along with any other relevant factors, in the context of the controller's specific implementation(s) and use(s) of Professional Services.

Table 2 - Elements of DPIA for Relevant Professional Services

Element of a DPIA	Relevant Information About Professional Services
Purpose(s) of processing	<p>The purpose(s) of processing data using Professional Services is determined by the controller that implements, configures, and uses it.</p> <p>As specified by the Microsoft Professional Services Data Protection Addendum (MPSDPA), Microsoft, as a data processor, processes Support and Consulting Data only to provide the requested services to our customer, the data controller. Microsoft will not use Support and Consulting Data or information derived from it for any advertising or similar commercial purposes.</p>
The purpose(s) of processing data using Professional Services is determined by the controller that implements, configures, and uses it.	<p>As specified by the Microsoft Professional Services Data Protection Addendum (MPSDPA), Microsoft, as a data processor, processes Support and Consulting Data only to provide the requested services to our customer, the data controller. Microsoft will not use Support and Consulting Data or information derived from it for any advertising or similar commercial purposes.</p>
Categories of personal data processed	<p>Support and Consulting data means all data, including all text, sound, video, image files, or software, that are provided to Microsoft by, or on behalf of, Customer (or that Customer authorizes Microsoft to obtain from an Online Service) through an engagement with Microsoft to obtain Professional Services or Support. This may include information collected over phone, chat, e-mail, or web form. It may include description of problems, files transferred to Microsoft to resolve support issues, automated troubleshooters, or by accessing customer systems remotely with customer permission.</p> <p>Customer Data and Support Data do not include customer contact or billing data, such as subscription information, and payment data, which Microsoft collects and processes in its capacity as a data controller and which is outside the scope of this document.</p>

Data retention	<p>Microsoft will retain Support and Consulting Data for the duration of the customer engagement plus a retention period after the engagement ends as necessary to ensure quality and continuity of service. As an example, after a support case is closed the data is normally retained for a period to ensure the ability to reference it if the issue re-emerges and the case is re-opened.</p> <p>When Professional Services provides support, the engagement length is defined when the support case is closed. When Professional Services provides consulting services, the engagement length is often defined by the work order. In other cases, the engagement length is defined by the maintenance of the business relationship. In all cases, Support and Consulting Data will be deleted or returned on request or in accordance with the customer's instructions without undue delay using the capabilities described in the Professional Services <i>Data Subject Rights Guide</i>.</p>
Location and transfers of personal data	<p>Due to the nature of Professional Services, including the need to provide round-the-clock support, data may be transferred worldwide. A list of locations Microsoft operates in is available on request. For consulting services, data may be held in-country if agreed to within the work order.</p> <p>For personal data from the European Economic Area and Switzerland, Microsoft will ensure that transfers of personal data to a third country or an international organization are subject to appropriate safeguards as described in Article 46 of the GDPR. In addition to Microsoft's commitments under the Standard Contractual Clauses for processors and other model contracts as described in the MPSDPA, Microsoft is certified to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks and the commitments they entail.</p>

Data sharing with third parties	<p>Microsoft shares data with third parties acting as our sub-processors to support functions such as customer and technical support, service maintenance, and other operations. Any subcontractors to which Microsoft transfers Support and Consulting Data will have entered into written agreements with Microsoft that are no less protective than the data protection terms of the MPSDPA. All third-party sub-processors with which Support and Consulting Data is shared under the MPSDPA are included in the Microsoft Commercial Support Contractors List.</p> <p>Microsoft will not disclose Support and Consulting Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Support and Consulting Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from the customer. If compelled to disclose Support and Consulting Data to law enforcement, Microsoft will promptly notify the customer and provide a copy of the demand unless legally prohibited from doing so.</p> <p>Upon receipt of any other third-party request for Support and Consulting Data, Microsoft will promptly notify the customer unless prohibited by law. Microsoft will reject the request unless required by law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from the customer.</p>
Data subject rights	<p>When operating as a processor, Microsoft makes available to customer (data controllers) the personal data of its data subjects and the ability to fulfill data subject requests when they exercise their rights under the GDPR. We do so in a manner consistent with the functionality of the product and our role as a processor. If we receive a request from the customer's data subject to exercise one or more of its rights under the GDPR, we redirect the data subject to make its request directly to the data controller.</p> <p>The <i>Professional Services Data Subject Request GDPR Documentation</i> provides a description of how the customer can address their data subject rights obligations in Professional Services.</p>
An assessment of the necessity and proportionality of the processing operations in relation to the purposes	<p>Such an assessment will depend on the controller's needs and purposes of processing.</p> <p>With regard to the processing carried out by Microsoft, such processing is necessary and proportional for the purpose of providing the services to the data controller. Microsoft commits to this in the MPSDPA.</p>
An assessment of the risks to the rights and freedoms of data subjects	<p>The key risks to the rights and freedoms of data subjects from the use of Professional Services will be a function of how and in what context the data controller implements, configures, and uses the professional services and any solutions provided by Professional Services.</p> <p>However, as with any service, personal data held in the service may be at risk of unauthorized access or inadvertent disclosure. Measures Microsoft takes to address such risks are discussed below.</p>

The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned

Microsoft is committed to helping protect the security of customer information. In compliance with the provisions of Article 32 of the GDPR, Microsoft has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Support and Consulting Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction.

Further, Microsoft complies with all other GDPR obligations that apply to data processors, including but not limited to, data protection impact assessments and record keeping.

[^1]: With respect to the criteria that the processing be on a "large scale," Recital 91 of the GDPR clarifies that: "The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory."

[Learn more](#)

[Microsoft Trust Center](#)

Microsoft's data protection officer

2/25/2019 • 2 minutes to read • [Edit Online](#)

Overview

Microsoft has designated a European Union Data Protection Officer (DPO) to be an independent advisor for Microsoft's engineering and business groups and to help ensure that all proposed processing of personal data meets EU legal requirements and Microsoft's corporate standards. The role was designed to meet the GDPR criteria set out in Articles 37-39.

Qualifications

The DPO role requires successful candidates to have at least seven years of professional data protection experience, or a mix of 10 years of data protection, security and enterprise risk management experience in order to be considered for the position. In addition, candidates must have demonstrated expertise in international data protection law and practices.

Nature of the role

The DPO is involved, properly and in a timely manner, in all key issues which relate to the protection of personal data. This is effectuated, in part, by the DPO's role in reviewing and advising on all Data Protection Impact Assessments (DPIAs) generated by Microsoft. As the DPIA program is designed to capture all personal data processing at Microsoft, the DPO will have cross-company visibility into, and the opportunity to inform and advise Microsoft of its obligations pursuant to the GDPR in regards to Microsoft's personal data processing. This same mechanism also allows the DPO to monitor Microsoft's compliance with applicable data protection regulations, including the GDPR, as well as Microsoft's internal policies and controls.

Position of the Data Protection Officer

The European Union DPO reports directly to Microsoft's Chief Privacy Officer, a senior executive within Microsoft's Corporate and Legal Affairs division. The DPO role has autonomy to perform the functions in an independent, unbiased manner. Through the Chief Privacy Officer's organization, the DPO has access to training and customer response resources as necessary to perform the DPO functions. The DPO is bound by confidentiality concerning their tasks through the use of a non-disclosure agreement.

Contact

Data subjects may contact the data protection officer by filling out the webform at <https://aka.ms/privacyresponse>. The DPO can also be reached by post at:

Microsoft EU Data Protection Officer

One Microsoft Place

South County Business Park

Leopardstown

Dublin 18

D18 P521

Ireland

Telephone: +353 (0) 1 295-3826

The contact details for the Data Protection Officer has been communicated to Microsoft's Supervisory Authority.

[Learn more](#)

[Microsoft Trust Center](#)