

Microsoft 365 for enterprise documentation and resources

Best-in-class productivity apps with intelligent cloud services that transform the way you work.



GET STARTED
[Learn about Microsoft 365 for enterprise](#)



QUICKSTART
[Accelerate your deployment with FastTrack](#)



TRAINING
[Train your IT pros and admins](#)

Get help with Microsoft 365 for enterprise and other resources

Explore Microsoft 365 for enterprise deployment guidance, features, and services.

Deploy key elements

- [Identity infrastructure](#)
- [Windows 10 Enterprise](#)
- [Microsoft 365 Apps for enterprise](#)
- [Microsoft Intune](#)

Manage Microsoft 365 for enterprise

- [Windows 10 Enterprise](#)
- [Microsoft 365 Apps for enterprise](#)
- [Apps with Intune](#)
- [Microsoft 365 services](#)

Additional resources

Learn more about other Microsoft 365 features and resources.

[Microsoft Purview](#)

Help your organization govern information, protect against risks, and comply with legal or regulatory standards.

[Microsoft 365 security](#)

Protect your organization across attack surfaces with robust security services and solutions.

[Microsoft 365 technical community](#)

Connect and collaborate with
peers and experts in the
Microsoft Tech Community and
share Microsoft 365 best...

Microsoft 365 for enterprise overview

Article • 05/13/2024

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

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

Components

Microsoft 365 for enterprise consists of:

[] Expand table

Services	Description
Local apps and cloud-based apps and productivity services	Includes both Microsoft 365 Apps for enterprise, 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 11 Enterprise	Meets the needs of both large and midsize organizations. It's the most productive and secure version of Windows for users. For IT professionals, it also provides comprehensive deployment, device, and app management.
Device management and advanced security services	Includes Microsoft Intune, which is a cloud-based enterprise mobility management service that helps enable your workforce to be productive while protecting your organization data.

Plans

Microsoft 365 for enterprise is available in three plans.

[] Expand table

Plan name	Capabilities
E3	Access the Microsoft 365 core products and features to securely enhance workplace productivity and drive innovation.

Plan name	Capabilities
E5	Access the Microsoft 365 latest products and features. These include Defender for Office 365, security tools, and collaboration tools. This plan includes all E3 capabilities, plus advanced security, voice, and data analysis tools.
F3	Connect with your first-line workers through purpose-built tools and resources that they can use to help them do their best work.

If you have Microsoft 365 E3, you can also get these add-ons:

- Identity & Threat Protection
- Information Protection & Compliance
- [Microsoft 365 E5 Compliance](#)
- Microsoft 365 E5 Insider Risk

Microsoft 365 E3 users can use these add-ons to take advantage of some of the additional features Microsoft 365 E5 includes.

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

Get the big picture

The [Microsoft 365 for enterprise poster](#) is a central location for you to view:

- The benefits of Microsoft 365 for enterprise, and how apps and services map to its value pillars.
- Microsoft 365 for enterprise plans and which components they contain.
- The key components of the Microsoft modern workplace, which Microsoft 365 for enterprise enables.
- The [Microsoft 365 Productivity Library](#) and representative scenarios for some common organization departments.

You can also [download a copy of the poster](#).

Transition your entire organization

To get a better picture about how to move your entire organization to the products and services in Microsoft 365 for enterprise, see the [transition poster](#).



Transition Your Organization to Microsoft 365 for enterprise

Check the boxes for what you have and follow the rows to digitally transform your business.

From	To	Benefits	Guidance
Windows <input checked="" type="checkbox"/> Windows 7* <input type="checkbox"/> Windows 8.1	Windows 10	Most modern, secure Windows ever	 aka.ms/m365te01
Office client <input checked="" type="checkbox"/> Office 2010** <input type="checkbox"/> Office 2013 <input type="checkbox"/> Office 2016	Microsoft 365 Apps for enterprise	Ongoing updates include the latest features	 aka.ms/m365te02
Office servers <input checked="" type="checkbox"/> Exchange Server 2010** <input type="checkbox"/> Exchange Server 2013 <input type="checkbox"/> Exchange Server 2016	Exchange Online	Scalable, available, secure, and always up to date, with built-in compliance and information protection	 aka.ms/m365te03
<input checked="" type="checkbox"/> SharePoint Server 2010*** <input type="checkbox"/> SharePoint Server 2013 <input type="checkbox"/> SharePoint Server 2016	SharePoint Online	Teamwork and collaboration across your organization	 aka.ms/m365te04
<input checked="" type="checkbox"/> Lync Server 2010*** <input type="checkbox"/> Lync Server 2013 <input type="checkbox"/> Skype for Business Server 2015	Microsoft Teams	Real-time meetings and collaboration across your organization	 aka.ms/m365te05

* Reached end of support on January 14, 2020.
** Reaches end of support on October 13, 2023.
*** Reaches end of support on April 13, 2021.

With Microsoft 365 E5 or E3 with the Identity & Threat Protection offering.
With Microsoft 365 E5 or E3 with the Information Protection & Compliance offering.

For more information, visit aka.ms/m365edeploy.

© 2019 Microsoft Corporation. All rights reserved.



This two-page poster is a quick way to inventory your existing infrastructure. It helps you to find guidance and move to the corresponding product or service in Microsoft 365 for enterprise. It includes Windows and Office products and other infrastructure and security elements, such as device management, identity, and information and threat protection.

Plan for and deploy

There are three ways to plan for and deploy the products, features, and components of Microsoft 365 for enterprise:

- In partnership with FastTrack

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

- With the help of Microsoft Consulting Services or a [Microsoft partner](#).

Consultants can analyze your current infrastructure and help you develop a plan to incorporate all the software and services of Microsoft 365 for enterprise.

- Do it yourself

Start with the [Networking roadmap](#) to build out or verify your existing infrastructure and productivity workloads.

For an example of how a fictional but representative multinational organization has deployed Microsoft 365 for enterprise, see the [Contoso Corporation case study](#).

Additional Microsoft 365 products

- [Microsoft 365 Business Premium](#)

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

- [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.

- [Microsoft 365 Government](#)

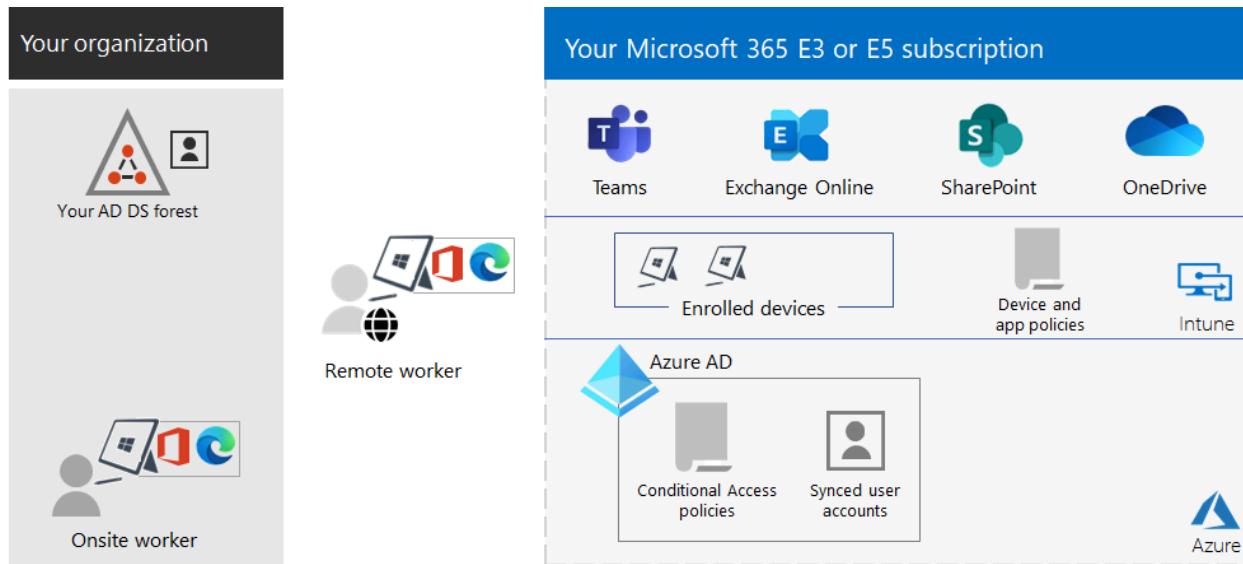
Empower United States public sector employees to work together, securely.

Best together with Surface and the Edge browser

Optimize your user's integrated and secure productivity with the best-together combination of Microsoft 365 for enterprise, Microsoft Surface devices, and the Microsoft Edge browser. This cross-product integration provides:

- A common identity and sign-in security infrastructure.
- Integrated local and cloud apps for search, collaboration, productivity, and compliance.
- Comprehensive and integrated security for hardware, browser, local app, and cloud apps.
- A common infrastructure for IT management of installs and updates.

Here is an example for an enterprise organization.



For more information and configuration examples for a small and medium business and an educational institution, download the [Best together poster](#).

Microsoft

Best together with Microsoft 365, Surface, and Edge

To optimize your user's productivity with integration and comprehensive security, the best-together combination is Microsoft 365 with Microsoft Surface laptops and the Microsoft Edge browser.

Microsoft 365	Surface laptop	Edge browser	Microsoft Endpoint Manager (for enterprises)
Achieve more with innovative Office apps, intelligent cloud services, search, and enterprise-ready support for security and compliance.	Cloud productivity apps, Microsoft 365 Apps, and enterprise-ready security and compliance features.	World-class performance and compatibility; privacy protection and compliance; your data; and customization for learning experiences, enterprise search, and personal productivity.	Endpoint security, device management and intelligent cloud actions in a unified management platform.
Microsoft product-wide integration	Benefits		
Common identity and sign-in security	Active Directory (Azure AD) is the identity provider for devices and cloud apps and can enforce strong sign-in requirements with Conditional Access and multi-factor authentication (MFA).		
Integrated local and cloud apps for search, collaboration, productivity, and compliance	Microsoft 365 Apps is the always up-to-date suite of desktop apps you already know (including Word, PowerPoint, Excel, Outlook, and Teams) that are designed to work with Microsoft 365 cloud apps such as SharePoint, OneDrive, Exchange, and Teams.		
Comprehensive and integrated security for hardware, browser, local apps, and cloud apps	World-class security is built-in to Surface laptops, Windows 10, Microsoft 365, and Edge in a way that works best together leverages the intelligence of the Microsoft cloud, and is transparent to users.		
IT management of installs and updates	EndpointManager uses on-premises Configuration Manager servers and cloud-based Microsoft Intune to ensure that Windows 10, Microsoft 365 Apps, and Edge are easily installed and kept current with ongoing updates.		

The following sections show the components and configurations for an enterprise, a small or medium-sized business, and an educational institution.

An enterprise organization

Your organization

- Your AD DS forest (Icon: triangle with nodes)
- Onsite worker (Icon: person at computer)
- Remote worker (Icon: person with globe, computer, and mobile device)

Your Microsoft 365 E3 or E5 subscription

- Teams (Icon: people)
- Exchange Online (Icon: envelope)
- SharePoint (Icon: cloud with document)
- OneDrive (Icon: cloud)
- Enrolled devices (Icon: two devices)
- Device and app policies (Icon: document)
- Intune (Icon: cloud with gear)
- Azure AD (Icon: shield)
- Conditional Access policies (Icon: lock)
- Synced user accounts (Icon: person)
- Azure (Icon: triangle)

Component	That includes
Microsoft 365 E3 or E5	Cloud productivity apps, Microsoft 365 Apps, and enterprise-ready security and compliance features
Onsite and remote worker devices	Surface laptop with Microsoft 365 Apps and the Edge browser installed
Identity	Hybrid identity with synchronized on-premises accounts, Conditional Access policies, and MFA for secure sign-ins
Install and updates	On-premises network has Endpoint Configuration Manager for installs, updates, and settings
Device management	Surface laptops are enrolled in Intune and receive device and app policies

January 2021 © 2021 Microsoft Corporation. All rights reserved.

Microsoft

Best together with Microsoft 365, Surface, and Edge

A small or medium-sized business

Your business

- Onsite worker (Icon: person at computer)
- Remote worker (Icon: person with globe, computer, and mobile device)

Your Microsoft 365 Business Premium subscription

- Teams (Icon: people)
- Exchange Online (Icon: envelope)
- SharePoint (Icon: cloud with document)
- OneDrive (Icon: cloud)
- Enrolled devices (Icon: two devices)
- Device and app policies (Icon: document)
- Intune (Icon: cloud with gear)
- Azure AD (Icon: shield)
- Conditional Access policies (Icon: lock)
- User accounts (Icon: person)
- Azure (Icon: triangle)

Component	That includes
Microsoft 365 Business Premium	Cloud productivity apps, Microsoft 365 Apps, search, and security and compliance features
Onsite and remote worker devices	Surface laptop with Microsoft 365 Apps and the Edge browser installed
Identity	Cloud-only identity, Conditional Access policies, and MFA for secure sign-ins
Install and updates	Microsoft cloud and Intune for installs, updates, and settings
Device management	Surface laptops are enrolled in Intune and receive device and app policies

An educational institution

Your school's Microsoft 365 Education A3 or A5 subscription

- Student (Icon: graduation cap)

Component	That includes
Microsoft 365 A3 or A5	Cloud productivity apps, Microsoft 365 Apps, Education A3 or A5, and security and compliance features
Student devices	Surface laptop with Microsoft 365 Apps and the Edge browser installed
Identity	Cloud-only identity, Conditional Access policies, and MFA for secure sign-ins
Install and updates	Microsoft cloud and Intune for Education for installs, updates, and settings
Device management	Surface laptops are enrolled in Intune for education and receive device and app policies

Where to start

Microsoft 365	Surface laptops	Edge browser	Endpoint Manager
microsoft.com/microsoft365	microsoft.com/surface	microsoft.com/edge	microsoft.com/endpointmanager

January 2021 © 2021 Microsoft Corporation. All rights reserved.

Microsoft 365 training



To learn more about Microsoft 365 and work toward a Microsoft 365 certification, you can start with [Microsoft 365 Fundamentals](#).

See also

[Microsoft 365 for enterprise product page ↗](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Networking roadmap for Microsoft 365

Article • 06/26/2024

Microsoft 365 for enterprise includes collaboration and productivity cloud services, Microsoft Intune, and many identity and security services of Microsoft Azure. All 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.

A crucial part of your Microsoft 365 onboarding is to ensure that your network and Internet connections are set up for optimized access. Configuring your on-premises network to access a globally distributed Software-as-a-Service (SaaS) cloud is different from a traditional network that is optimized for traffic to on-premises datacenters and a central Internet connection.

Use these articles to understand the key differences and to modify your edge devices, client computers, and on-premises network to get the best performance for your on-premises users.

Plan

In the planning phase of your networking implementation:

- [Understand how Microsoft 365 networking works](#)
- [Learn about network connectivity principles](#)
- [Assess your current network connectivity](#)
- [Plan for your network devices](#)
- [Get your network set up for migration](#)

Deploy

In the deployment phase of your networking implementation:

- [Ensure your enterprise network is optimized for Microsoft 365 connectivity](#)
- [Add the DNS domains for your organization](#)
- [Optimize connectivity for remote workers using VPN split tunneling](#)
- [Configure CDN to improve network performance](#)
- [Optimize your connectivity to Microsoft 365 endpoints](#)
- If needed, [configure ExpressRoute](#)

Manage

In the management phase of your networking implementation:

- Test and optimize using the Microsoft 365 network connectivity test tool
- Ensure that your network devices are using the latest Office 365 endpoints
- Monitor and tune your networking performance
- Monitor your Microsoft 365 connectivity

Network equipment vendors

If you are a network equipment vendor, join the [Microsoft 365 Networking Partner Program](#). Enroll in the program to build Microsoft 365 network connectivity principles into your products and solutions.

How Contoso did networking for Microsoft 365

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



Next step

Start your networking planning with the [Microsoft 365 networking connectivity overview](#).

Feedback

Was this page helpful?

Yes	No
-----	----

[Provide product feedback ↗](#)

Microsoft 365 network connectivity overview

Article • 12/29/2023

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Microsoft 365 is a distributed Software-as-a-Service (SaaS) cloud that provides productivity and collaboration scenarios through a diverse set of micro-services and applications. Client components of Microsoft 365 such as Outlook, Word, and PowerPoint run on user computers and connect to other components of Microsoft 365 that run in Microsoft datacenters. The most significant factor that determines the quality of the Microsoft 365 end user experience is network reliability and low latency between Microsoft 365 clients and Microsoft 365 service front doors.

In this article, you'll learn about the goals of Microsoft 365 networking, and why Microsoft 365 networking requires a different approach to optimization than generic Internet traffic.

Microsoft 365 networking goals

The ultimate goal of Microsoft 365 networking is to optimize the end user experience by enabling the least restrictive access between clients and the closest Microsoft 365 endpoints. The quality of end user experience is directly related to the performance and responsiveness of the application that the user is using. For example, Microsoft Teams relies on low latency so that user phone calls, conferences and shared screen collaborations are glitch-free, and Outlook relies on great networking connectivity for instant search features that apply server-side indexing and AI capabilities.

The primary goal in the network design should be to minimize latency by reducing the round-trip time (RTT) from client machines to the Microsoft Global Network, Microsoft's public network backbone that interconnects all of Microsoft's datacenters with low latency, high availability cloud application entry points spread around the world. You can learn more about the Microsoft Global Network at [How Microsoft builds its fast and reliable global network](#).

Optimizing Microsoft 365 network performance doesn't need to be complicated. You can get the best possible performance by following a few key principles:

- Identify Microsoft 365 network traffic

- Allow local branch egress of Microsoft 365 network traffic to the internet from each location where users connect to Microsoft 365
- Allow Microsoft 365 traffic to bypass proxies and packet inspection devices

For more information on Microsoft 365 network connectivity principles, see [Microsoft 365 Network Connectivity Principles](#).

Traditional network architectures and SaaS

Traditional network architecture principles for client/server workloads are designed around the assumption that traffic between clients and endpoints doesn't extend outside the corporate network perimeter. Also, in many enterprise networks, all outbound Internet connections traverse the corporate network, and egress from a central location.

In traditional network architectures, higher latency for generic Internet traffic is a necessary tradeoff in order to maintain network perimeter security, and performance optimization for Internet traffic typically involves upgrading or scaling out the equipment at network egress points. However, this approach doesn't address the requirements for optimum network performance of SaaS services such as Microsoft 365.

Identifying Microsoft 365 network traffic

We're making it easier to identify Microsoft 365 network traffic and making it simpler to manage the network identification.

- New categories of network endpoints to differentiate highly critical network traffic from network traffic that's not impacted by Internet latencies. There are just a handful of URLs and supporting IP Addresses in the most critical "Optimize" category.
- Web services for script usage or direct device configuration and change management of Microsoft 365 network identification. Changes are available from the web service, or in RSS format, or on email using a Microsoft Flow template.
- [Office 365 Network partner program](#) with Microsoft partners who provide devices or services that follow Microsoft 365 network connectivity principles and have simple configuration.

Securing Microsoft 365 connections

The goal of traditional network security is to harden the corporate network perimeter against intrusion and malicious exploits. Most enterprise networks enforce network

security for Internet traffic using technologies like proxy servers, firewalls, SSL break and inspect, deep packet inspection, and data loss prevention systems. These technologies provide important risk mitigation for generic Internet requests but can dramatically reduce performance, scalability, and the quality of end user experience when applied to Microsoft 365 endpoints.

Microsoft 365 helps meet your organization's needs for content security and data usage compliance with built-in security and governance features designed specifically for Microsoft 365 features and workloads. For more information about Microsoft 365 security and compliance, see [Microsoft Defender for Office 365](#) and [Microsoft Purview risk and compliance solutions](#). For more information about Microsoft's recommendations and support position on advanced network solutions that perform advanced-level processing on Microsoft 365 traffic, see [Using third-party network devices or solutions on Office 365 traffic](#).

Why is Microsoft 365 networking different?

Microsoft 365 is designed for optimal performance using endpoint security and encrypted network connections, reducing the need for perimeter security enforcement. Microsoft 365 datacenters are located across the world and the service is designed to use various methods for connecting clients to best available service endpoints. Since user data and processing are distributed between many Microsoft datacenters, there's no single network endpoint to which client machines can connect. In fact, data and services in your Microsoft 365 tenant are dynamically optimized by the Microsoft Global Network to adapt to the geographic locations from which they're accessed by end users.

Certain common performance issues are created when Microsoft 365 traffic is subject to packet inspection and centralized egress:

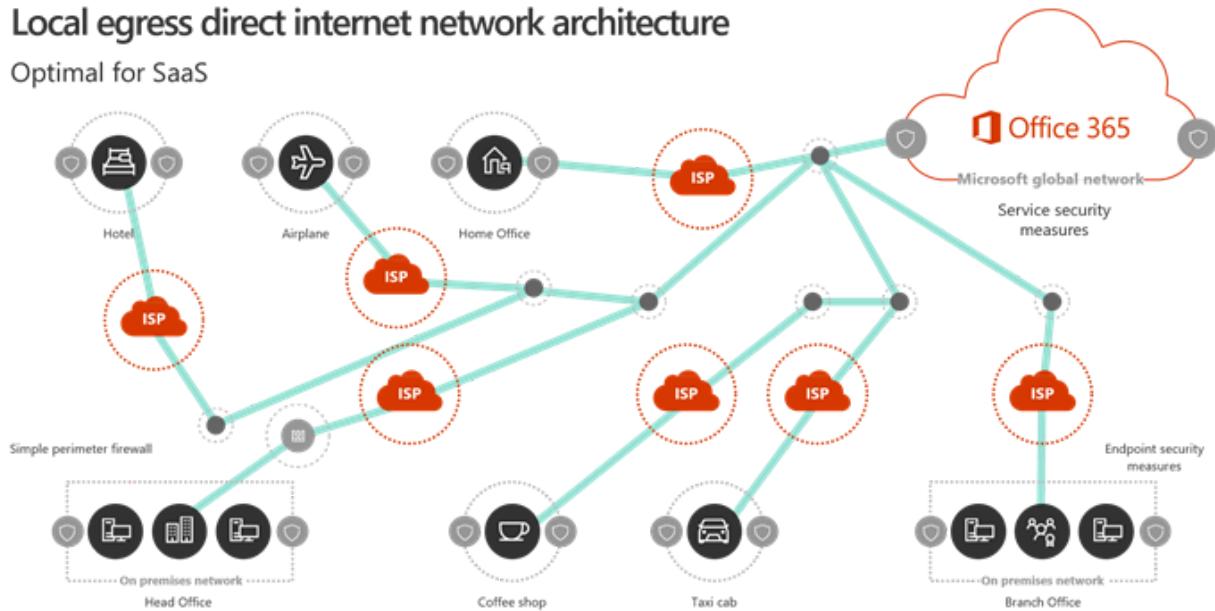
- High latency can cause poor performance of video and audio streams, and slow response of data retrieval, searches, real-time collaboration, calendar free/busy information, in-product content and other services
- Egressing connections from a central location defeats the dynamic routing capabilities of the Microsoft 365 global network, adding latency and round-trip time
- Decrypting SSL secured Microsoft 365 network traffic and re-encrypting it can cause protocol errors and has security risk

Shortening the network path to Microsoft 365 entry points by allowing client traffic to egress as close as possible to their geographic location can improve connectivity performance and the end user experience in Microsoft 365. It can also help to reduce the impact of future changes to the network architecture on Microsoft 365 performance

and reliability. The optimum connectivity model is to always provide network egress at the user's location, regardless of whether this is on the corporate network or remote locations such as home, hotels, coffee shops, and airports. Generic Internet traffic and WAN based corporate network traffic would be separately routed and not use the local direct egress model. This local direct egress model is represented in the diagram below.

Local egress direct internet network architecture

Optimal for SaaS



The local egress architecture has the following benefits for Microsoft 365 network traffic over the traditional model:

- Provides optimal Microsoft 365 performance by optimizing route length. End user connections are dynamically routed to the nearest Microsoft 365 entry point by the Microsoft Global Network's *Distributed Service Front Door* infrastructure, and traffic is then routed internally to data and service endpoints over Microsoft's ultra-low latency high availability fiber.
- Reduces the load on corporate network infrastructure by allowing local egress for Microsoft 365 traffic, bypassing proxies and traffic inspection devices.
- Secures connections on both ends by applying client endpoint security and cloud security features, avoiding application of redundant network security technologies.

ⓘ Note

The *Distributed Service Front Door* infrastructure is the Microsoft Global Network's highly available and scalable network edge with geographically distributed locations. It terminates end user connections and efficiently routes them within the Microsoft Global Network. You can learn more about the Microsoft Global Network at [How Microsoft builds its fast and reliable global network](#).

For more information on understanding and applying Microsoft 365 network connectivity principles, see [Microsoft 365 Network Connectivity Principles](#).

Conclusion

Optimizing Microsoft 365 network performance really comes down to removing unnecessary impediments. By treating Microsoft 365 connections as trusted traffic, you can prevent latency from being introduced by packet inspection and competition for proxy bandwidth. Allowing local connections between client machines and Office 365 endpoints enables traffic to be dynamically routed through the Microsoft Global Network.

Related Topics

[Microsoft 365 Network Connectivity Principles](#)

[Managing Office 365 endpoints](#)

[Office 365 URLs and IP address ranges](#)

[Office 365 IP Address and URL Web service](#)

[Assessing Microsoft 365 network connectivity](#)

[Network planning and performance tuning for Microsoft 365](#)

[Office 365 performance tuning using baselines and performance history](#)

[Performance troubleshooting plan for Office 365](#)

[Content Delivery Networks](#)

[Microsoft 365 connectivity test](#) ↗

[How Microsoft builds its fast and reliable global network](#) ↗

[Office 365 Networking blog](#) ↗

Feedback

Was this page helpful?

Yes

No

[Provide product feedback](#) ↗

Microsoft 365 network connectivity principles

Article • 05/23/2024

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Before you begin planning your network for Microsoft 365 network connectivity, it's important to understand the connectivity principles for securely managing Microsoft 365 traffic and getting the best possible performance. This article helps you understand the most recent guidance for securely optimizing Microsoft 365 network connectivity.

Traditional enterprise networks are designed primarily to provide users access to applications and data hosted in company operated datacenters with strong perimeter security. The traditional model assumes that users will access applications and data from inside the corporate network perimeter, over WAN links from branch offices, or remotely over VPN connections.

Adoption of SaaS applications like Microsoft 365 moves some combination of services and data outside the network perimeter. Without optimization, traffic between users and SaaS applications is subject to latency introduced by packet inspection, network hairpins, inadvertent connections to geographically distant endpoints and other factors. You can ensure the best Microsoft 365 performance and reliability by understanding and implementing key optimization guidelines.

In this article, you'll learn about:

- [Microsoft 365 architecture](#) as it applies to customer connectivity to the cloud
- Updated [Microsoft 365 connectivity principles](#) and strategies for optimizing network traffic and the end-user experience
- The [Office 365 Endpoints web service](#), which allows network administrators to consume a structured list of endpoints for use in network optimization
- Guidance for [optimizing connectivity to Microsoft 365 services](#)
- [Comparing network perimeter security with endpoint security](#)
- [Incremental optimization](#) options for Microsoft 365 traffic
- The [Microsoft 365 connectivity test](#), a new tool for testing basic connectivity to Microsoft 365

Microsoft 365 architecture

Microsoft 365 is a distributed Software-as-a-Service (SaaS) cloud that provides productivity and collaboration scenarios through a diverse set of micro-services and applications. Examples include Exchange Online, SharePoint Online, Microsoft Teams, Exchange Online Protection, Office in a browser, and many others. While specific Microsoft 365 applications might have their unique features as it applies to customer network and connectivity to the cloud, they all share some key principals, goals, and architecture patterns. These principles and architecture patterns for connectivity are typical for many other SaaS clouds. At the same time, they're different from the typical deployment models of Platform-as-a-Service and Infrastructure-as-a-Service clouds, such as Microsoft Azure.

One of the most significant architectural features of Microsoft 365 (that is often missed or misinterpreted by network architects) is that it's a truly global distributed service, in the context of how users connect to it. The location of the target Microsoft 365 tenant is important to understand the locality of where customer data is stored within the cloud. However, the user experience with Microsoft 365 doesn't involve connecting directly to disks containing the data. The user experience with Microsoft 365 (including performance, reliability, and other important quality characteristics) involves connectivity through highly distributed service front doors that are scaled out across hundreds of Microsoft locations worldwide. In most cases, the best user experience is achieved by allowing the customer network to route user requests to the closest Microsoft 365 service entry point. This is preferable rather than connecting to Microsoft 365 through an egress point in a central location or region.

For most customers, Microsoft 365 users are distributed across many locations. To achieve the best results, the principles outlined in this document should be looked at from the scale-out (not scale-up) point of view. While also focusing on optimizing connectivity to the nearest point of presence in the Microsoft Global Network, not to the geographic location of the Microsoft 365 tenant. In essence, this means that even though Microsoft 365 tenant data might be stored in a specific geographic location, Microsoft 365 experience for that tenant remains distributed. It can be present in very close (network) proximity to every end-user location that the tenant has.

Microsoft 365 connectivity principles

Microsoft recommends the following principles to achieve optimal Microsoft 365 connectivity and performance. Use these Microsoft 365 connectivity principles to manage your traffic and get the best performance when connecting to Microsoft 365.

The primary goal in the network design should be to minimize latency by reducing the round-trip time (RTT) from your network into the Microsoft Global Network, Microsoft's

public network backbone that interconnects all of Microsoft's datacenters with low latency and cloud application entry points spread around the world. You can learn more about the Microsoft Global Network at [How Microsoft builds its fast and reliable global network](#).

Identify and differentiate Microsoft 365 traffic

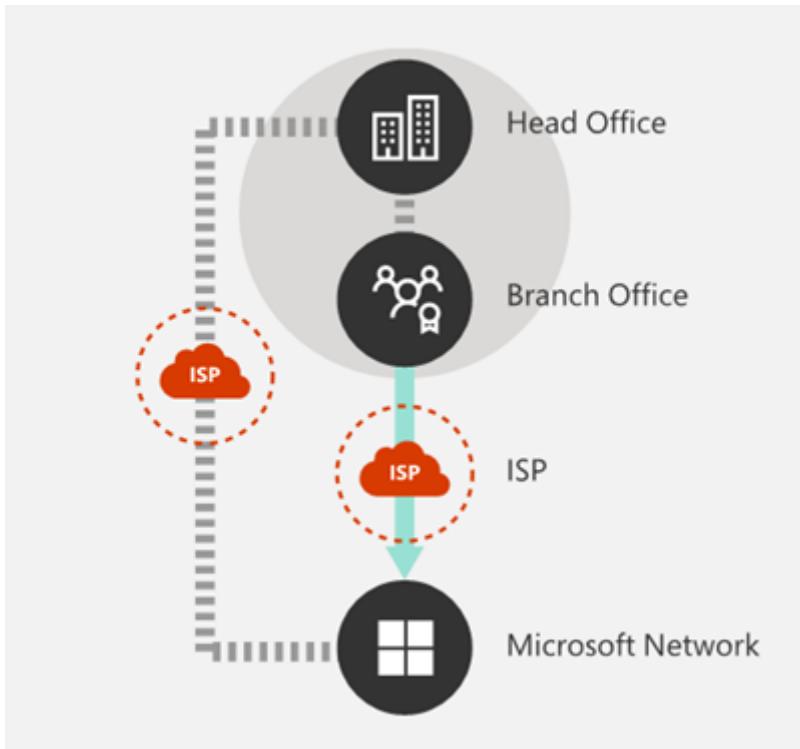


Identifying Microsoft 365 network traffic is the first step in being able to differentiate that traffic from generic Internet-bound network traffic. Microsoft 365 connectivity can be optimized by implementing a combination of approaches like network route optimization, firewall rules, browser proxy settings. Additionally, bypassing of network inspection devices for certain endpoints is also beneficial.

For more information on Microsoft 365 optimization methods, see the [optimizing connectivity to Microsoft 365 services](#) section.

Microsoft now publishes all Microsoft 365 endpoints as a web service and provides guidance on how best to use this data. For more information on how to fetch and work with Microsoft 365 endpoints, see the article [Office 365 URLs and IP address ranges](#).

Egress network connections locally



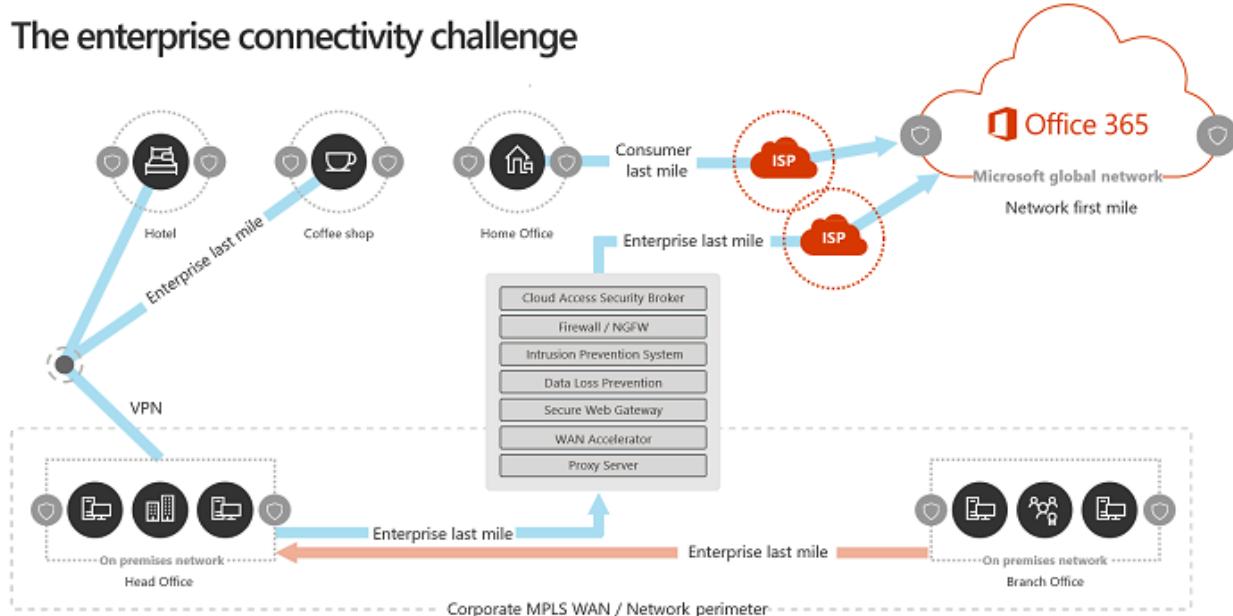
Local DNS and Internet egress is of critical importance for reducing connection latency and ensuring that user connections are made to the nearest point of entry to Microsoft 365 services. In a complex network topology, it's important to implement both local DNS and local Internet egress together. For more information about how Microsoft 365 routes client connections to the nearest point of entry, see the article [Client Connectivity](#).

Prior to the advent of cloud services such as Microsoft 365, end-user Internet connectivity as a design factor in network architecture was relatively simple. When Internet services and web sites are distributed around the globe, latency between corporate egress points and any given destination endpoint is largely a function of geographical distance.

In a traditional network architecture, all outbound Internet connections traverse the corporate network, and egress from a central location. As Microsoft's cloud offerings have matured, a distributed Internet-facing network architecture has become critical for supporting latency-sensitive cloud services. The Microsoft Global Network was designed to accommodate latency requirements with the Distributed Service Front Door infrastructure, a dynamic fabric of global entry points that routes incoming cloud service connections to the closest entry point. This is intended to reduce the length of the "last mile" for Microsoft cloud customers by effectively shortening the route between the customer and the cloud.

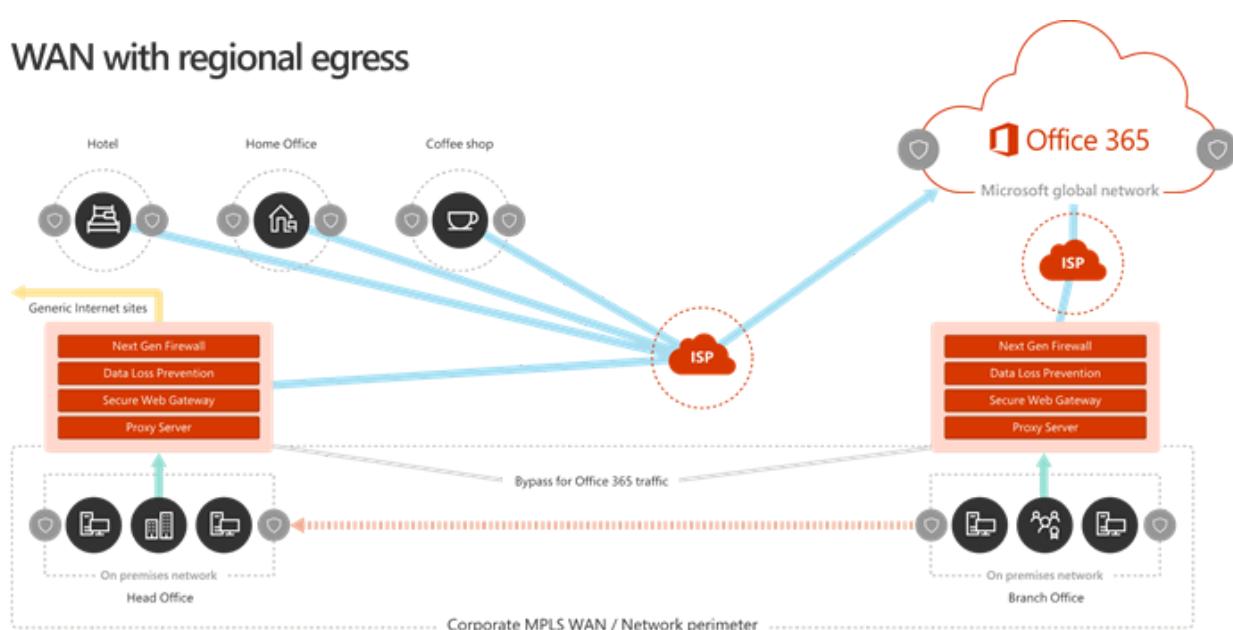
Enterprise WANs are often designed to backhaul network traffic to a central company head office for inspection before egress to the Internet, usually through one or more proxy servers. The following diagram illustrates such a network topology.

The enterprise connectivity challenge



Because Microsoft 365 runs on the Microsoft Global Network, which includes front-end servers around the world, there's often a front-end server close to the user's location. By providing local Internet egress and by configuring internal DNS servers to provide local name resolution for Microsoft 365 endpoints, network traffic destined for Microsoft 365 can connect to Microsoft 365 front end servers as close as possible to the user. The following diagram shows an example of a network topology that allows users connecting from main office, branch office, and remote locations to follow the shortest route to the closest Microsoft 365 entry point.

WAN with regional egress



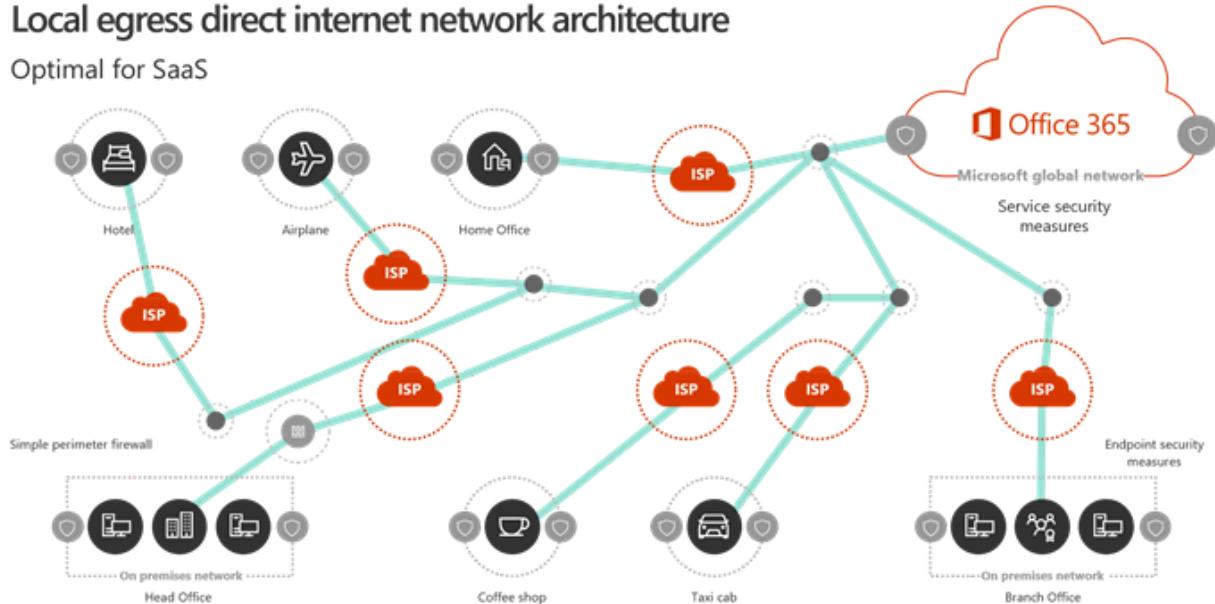
Shortening the network path to Microsoft 365 entry points in this way can improve connectivity performance and the end-user experience in Microsoft 365. It can also help to reduce the effect of future changes to the network architecture on Microsoft 365 performance and reliability.

Also, DNS requests can introduce latency if the responding DNS server is distant or busy. You can minimize name resolution latency by provisioning local DNS servers in branch locations and making sure they're configured to cache DNS records appropriately.

While regional egress can work well for Microsoft 365, the optimum connectivity model would be to always provide network egress at the user's location, regardless of whether it is on the corporate network or remote locations such as homes, hotels, coffee shops, and airports. This local direct egress model is represented in the following diagram.

Local egress direct internet network architecture

Optimal for SaaS

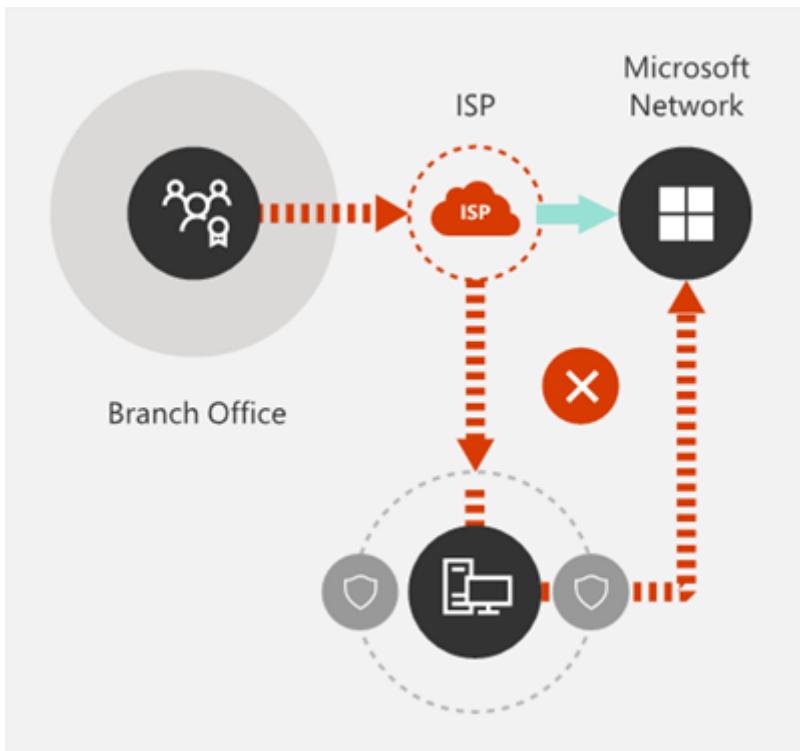


Enterprises who have adopted Microsoft 365 can take advantage of the Microsoft Global Network's Distributed Service Front Door architecture by ensuring that user connections to Microsoft 365 take the shortest possible route to the nearest Microsoft Global Network entry point. The local egress network architecture does this by allowing Microsoft 365 traffic to be routed over the nearest egress, regardless of user location.

The local egress architecture has the following benefits over the traditional model:

- Provides optimal Microsoft 365 performance by optimizing route length. end-user connections are dynamically routed to the nearest Microsoft 365 entry point by the Distributed Service Front Door infrastructure.
- Reduces the load on corporate network infrastructure by allowing local egress.
- Secures connections on both ends by using client endpoint security and cloud security features.

Avoid network hairpins



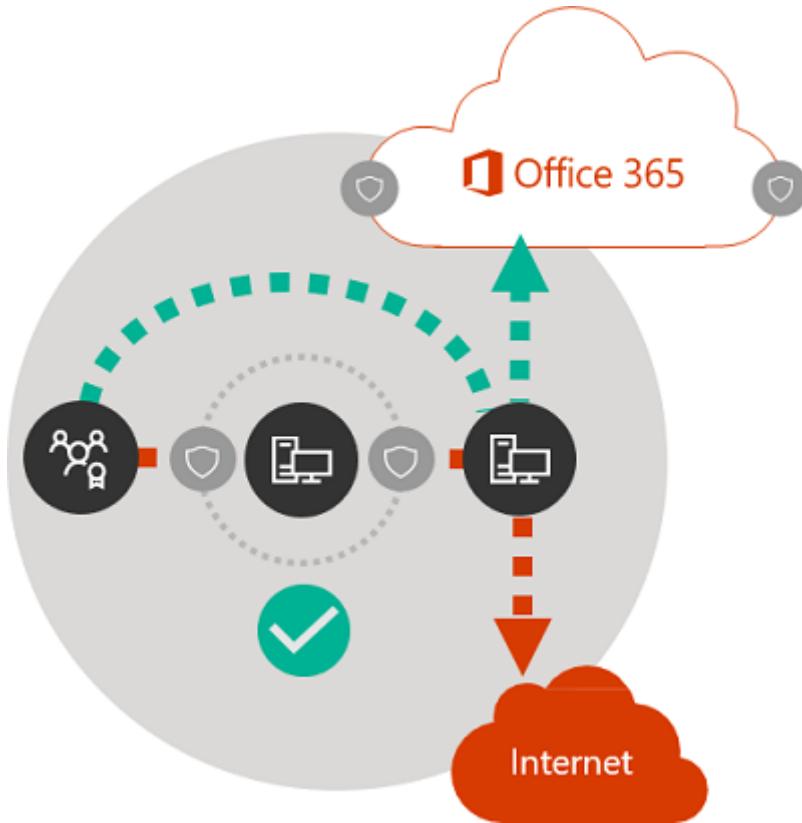
As a general rule of thumb, the shortest, most direct route between user and closest Microsoft 365 endpoint offers the best performance. A network hairpin happens when WAN or VPN traffic bound for a particular destination is first directed to another intermediate location (such as security stack, cloud access broker, or cloud-based web gateway), introducing latency and potential redirection to a geographically distant endpoint. Network hairpins are also caused by routing/peering inefficiencies or suboptimal (remote) DNS lookups.

To ensure that Microsoft 365 connectivity isn't subject to network hairpins even in the local egress case, check whether the ISP that is used to provide Internet egress for the user location has a direct peering relationship with the Microsoft Global Network in close proximity to that location. You might also want to configure egress routing to send trusted Microsoft 365 traffic directly. This is as opposed to proxying or tunneling through a third-party cloud or cloud-based network security vendor that processes your Internet-bound traffic. Local DNS name resolution of Microsoft 365 endpoints helps to ensure that in addition to direct routing, the closest Microsoft 365 entry points are being used for user connections.

If you use cloud-based network or security services for your Microsoft 365 traffic, ensure that the result of the hairpin is evaluated and its effect on Microsoft 365 performance is understood. This can be done by examining the number and locations of service provider locations through which the traffic is forwarded in relationship to number of your branch offices and Microsoft Global Network peering points, quality of the network peering relationship of the service provider with your ISP and Microsoft, and the performance effect of backhauling in the service provider infrastructure.

Due to the large number of distributed locations with Microsoft 365 entry points and their proximity to end-users, routing Microsoft 365 traffic to any third-party network or security provider can have an adverse effect on Microsoft 365 connections if the provider network isn't configured for optimal Microsoft 365 peering.

Assess bypassing proxies, traffic inspection devices, and duplicate security technologies



Enterprise customers should review their network security and risk reduction methods specifically for Microsoft 365 bound traffic and use Microsoft 365 security features to reduce their reliance on intrusive, performance impacting, and expensive network security technologies for Microsoft 365 network traffic.

Most enterprise networks enforce network security for Internet traffic using technologies like proxies, TLS inspection, packet inspection, and data loss prevention systems. These technologies provide important risk mitigation for generic Internet requests but can dramatically reduce performance, scalability, and the quality of end user experience when applied to Microsoft 365 endpoints.

Office 365 Endpoints web service

Microsoft 365 administrators can use a script or REST call to consume a structured list of endpoints from the Office 365 Endpoints web service and update the configurations of perimeter firewalls and other network devices. This ensures that traffic bound for

Microsoft 365 is identified, treated appropriately and managed differently from network traffic bound for generic and often unknown Internet web sites. For more information on how to use the Office 365 Endpoints web service, see the article [Office 365 URLs and IP address ranges](#).

PAC (Proxy Automatic Configuration) scripts

Microsoft 365 administrators can create PAC (Proxy Automatic Configuration) scripts that can be delivered to user computers via WPAD or GPO. PAC scripts can be used to bypass proxies for Microsoft 365 requests from WAN or VPN users, allowing Microsoft 365 traffic to use direct Internet connections rather than traversing the corporate network.

Microsoft 365 security features

Microsoft is transparent about datacenter security, operational security, and risk reduction around Microsoft 365 servers and the network endpoints that they represent. Microsoft 365 built-in security features are available for reducing network security risk, such as Microsoft Purview Data Loss Prevention, antivirus, Multifactor Authentication, Customer Lockbox, Defender for Office 365, Microsoft 365 Threat Intelligence, Microsoft 365 Secure Score, Exchange Online Protection, and Network DDOS Security.

For more information on Microsoft datacenter and Global Network security, see the [Microsoft Trust Center](#).

Optimizing connectivity to Microsoft 365 services

Microsoft 365 services are a collection of dynamic, interdependent, and deeply integrated products, applications, and services. When configuring and optimizing connectivity to Microsoft 365 services, it is not feasible to link specific endpoints (domains) with a few Microsoft 365 scenarios to implement allow-listing at the network level. Microsoft does not support selective allow-listing as it causes connectivity and service incidents for users. Network administrators should therefore always apply Microsoft 365 guidelines for network allow-listing and common network optimizations to the full set of required network endpoints (domains) that are [published](#) and updated regularly. While we are simplifying Microsoft 365 network endpoints in response to customer feedback, network administrators should be aware of the following core patterns in the existing set of endpoints today:

- Where possible, the published domain endpoints will include wildcards to significantly lower the network configuration effort for customers.
 - Microsoft 365 announced a domain consolidation initiative (cloud.microsoft), providing customers a way to simplify their network configurations and automatically accrue network optimizations for this domain to many current and future Microsoft 365 services.
 - Exclusive use of cloud.microsoft root domain for security isolation and specific functions. This enables customer network and security teams to trust Microsoft 365 domains, while improving connectivity to those endpoints and avoiding unnecessary network security processing.
 - Certain endpoint definitions specify unique IP prefixes corresponding to their domains. This feature supports customers with intricate network structures, enabling them to apply precise network optimizations by utilizing IP prefix details.

The following network configurations are recommended for all “Required” Microsoft 365 network endpoints (domains) and categories:

- Explicitly permitting Microsoft 365 network endpoints in the network devices and services that user connections go through (e.g., network perimeter security devices like proxies, firewalls, DNS, cloud-based network security solutions, etc.)
- Bypass Microsoft 365 domains from TLS decryption, traffic interception, deep packet inspection, and network packet and content filtering. Note that many outcomes that customers are using these network technologies for in the context of untrusted/unmanaged applications can be achieved by Microsoft 365 security features natively.
- Direct internet access should be prioritized for the Microsoft 365 domains by reducing reliance on wide area network (WAN) backhauling, avoiding network hairpins, and enabling a more efficient internet egress local to the users and directly to the Microsoft network.
- Ensure that DNS name resolution occurs close to the network egress to ensure that connections are served through the most optimal Microsoft 365 front door.
- Prioritize Microsoft 365 connections along the network path, ensuring capacity and quality of service for Microsoft 365 experiences.
- Bypass traffic intermediation devices such as proxies and VPN services.

Customers with complex network topologies, implementing network optimizations like custom routing, IP based proxy bypass, and split tunnel VPN may require IP prefix information in addition to domains. To facilitate these customer scenarios Microsoft 365 network endpoints are grouped into categories to prioritize and ease the configuration of these additional network optimizations. Network endpoints classified under the “Optimize” and “Allow” categories carry high traffic volumes and are sensitive to

network latency and performance, and customers may want to optimize connectivity to those first. Network endpoints under the “Optimize” and “Allow” categories have IP addresses listed along with domains. Network endpoints classified under the “Default” category do not have IP addresses associated with them as they are more dynamic in nature and IP addresses change over time.

Additional network considerations

When optimizing connectivity to Microsoft 365, certain network configurations may have a negative impact on Microsoft 365 availability, interoperability, performance, and user experience. Microsoft has not tested the following network scenarios with our services, and they are known to cause connectivity issues.

- TLS termination or deep packet inspection of any M365 domains with customer proxies or other types of network devices or services.
 - Blocking specific protocols or protocol versions such as QUIC, WebSocket’s, etc. by intermediate network infrastructure or service.
 - Forcing downgrade or failover of protocols (such as UDP --> TCP, TLS1.3 --> TLS1.2 --> TLS1.1) used between client applications and Microsoft 365 services.
 - Routing connections through network infrastructure applying its own authentication such as proxy authentication.

We recommend that customers avoid using these network techniques to traffic destined to Microsoft 365 domains and bypass these for Microsoft 365 connections.

Microsoft recommends setting up an automated system to download and apply the M365 network endpoint list regularly. Please refer to [Change management for Microsoft 365 IP addresses and URLs for more information](#).

Comparing network perimeter security with endpoint security

The goal of traditional network security is to harden the corporate network perimeter against intrusion and malicious exploits. As organizations adopt Microsoft 365, some network services and data are partly or completely migrated to the cloud. As for any fundamental change to network architecture, this process requires a reevaluation of network security that takes emerging factors into account:

- As cloud services are adopted, network services and data are distributed between on-premises datacenters and the cloud, and perimeter security is no longer adequate on its own.

- Remote users connect to corporate resources both in on-premises datacenters and in the cloud from uncontrolled locations such as homes, hotels, and coffee shops.
- Purpose-built security features are increasingly built into cloud services and can potentially supplement or replace existing security systems.

Microsoft offers a wide range of Microsoft 365 security features and provides prescriptive guidance for employing security best practices that can help you to ensure data and network security for Microsoft 365. Recommended best practices include:

- **Use multi-factor authentication (MFA)** MFA adds an extra layer of protection to a strong password strategy by requiring users to acknowledge a phone call, text message, or an app notification on their smart phone after correctly entering their password.
- **Use Microsoft Defender for Cloud Apps** Configure policies to track anomalous activity and act on it. Set up alerts with Microsoft Defender for Cloud Apps so that admins can review unusual or risky user activity, such as downloading large amounts of data, multiple failed sign-in attempts, or connections from an unknown or dangerous IP addresses.
- **Configure Data Loss Prevention (DLP)** DLP allows you to identify sensitive data and create policies that help prevent your users from accidentally or intentionally sharing the data. DLP works across Microsoft 365 including Exchange Online, SharePoint Online, and OneDrive so that your users can stay compliant without interrupting their workflow.
- **Use Customer Lockbox** As a Microsoft 365 admin, you can use Customer Lockbox to control how a Microsoft support engineer accesses your data during a help session. In cases where the engineer requires access to your data to troubleshoot and fix an issue, Customer Lockbox allows you to approve or reject the access request.
- **Use Secure Score** A security analytics tool that recommends what you can do to further reduce risk. Secure Score looks at your Microsoft 365 settings and activities and compares them to a baseline established by Microsoft. You get a score based on how aligned you are with best security practices.

A holistic approach to enhanced security should include consideration of the following:

- Shift emphasis from perimeter security towards endpoint security by applying cloud-based and Office client security features.
 - Shrink the security perimeter to the datacenter
 - Enable equivalent trust for user devices inside the office or at remote locations
 - Focus on securing the data location and the user location

- Managed user machines have higher trust with endpoint security
- Manage all information security holistically, not focusing solely on the perimeter
 - Redefine WAN and building perimeter network security by allowing trusted traffic to bypass security devices and separating unmanaged devices to guest Wi-Fi networks
 - Reduce network security requirements of the corporate WAN edge
 - Some network perimeter security devices such as firewalls are still required, but load is decreased
 - Ensures local egress for Microsoft 365 traffic
- Improvements can be addressed incrementally as described in the [Incremental optimization](#) section. Some optimization techniques might offer better cost/benefit ratios depending on your network architecture, and you should choose optimizations that make the most sense for your organization.

For more information on Microsoft 365 security and compliance, see the articles [Microsoft 365 security](#) and [Microsoft Purview](#).

Incremental optimization

We have represented the ideal network connectivity model for SaaS earlier in this article, but for many large organizations with historically complex network architectures, it isn't practical to directly make all of these changes. In this section, we discuss many incremental changes that can help to improve Microsoft 365 performance and reliability.

The methods you'll use to optimize Microsoft 365 traffic varies depending on your network topology and the network devices you have implemented. Large enterprises with many locations and complex network security practices need to develop a strategy that includes most or all of the principles listed in the [Microsoft 365 connectivity principles](#) section, while smaller organizations might only need to consider one or two.

You can approach optimization as an incremental process, applying each method successively. The following table lists key optimization methods in order of their effect on latency and reliability for the largest number of users.

[\[+\] Expand table](#)

Optimization method	Description	Impact
Local DNS resolution and Internet egress	Provision local DNS servers in each location and ensure that Microsoft 365 connections egress to the Internet as close as possible to the user's location.	Minimize latency Improve reliable connectivity to the Internet

Optimization method	Description	Impact
		closest Microsoft 365 entry point
Add regional egress points	If your corporate network has multiple locations but only one egress point, add regional egress points to enable users to connect to the closest Microsoft 365 entry point.	Minimize latency Improve reliable connectivity to the closest Microsoft 365 entry point
Bypass proxies and inspection devices	Configure browsers with PAC files that send Microsoft 365 requests directly to egress points. Configure edge routers and firewalls to permit Microsoft 365 traffic without inspection.	Minimize latency Reduce load on network devices
Enable direct connection for VPN users	For VPN users, enable Microsoft 365 connections to connect directly from the user's network rather than over the VPN tunnel by implementing split tunneling.	Minimize latency Improve reliable connectivity to the closest Microsoft 365 entry point
Migrate from traditional WAN to SD-WAN	SD-WANs (Software Defined Wide Area Networks) simplify WAN management and improve performance by replacing traditional WAN routers with virtual appliances, similar to the virtualization of compute resources using virtual machines (VMs).	Improve performance and manageability of WAN traffic Reduce load on network devices

Related articles

[Microsoft 365 Network Connectivity Overview](#)

[Managing Office 365 endpoints](#)

[Office 365 URLs and IP address ranges](#)

[Office 365 IP Address and URL Web service](#)

[Assessing Microsoft 365 network connectivity](#)

[Network planning and performance tuning for Microsoft 365](#)

[Office 365 performance tuning using baselines and performance history](#)

[Performance troubleshooting plan for Office 365](#)

[Content Delivery Networks](#)

[Microsoft 365 connectivity test ↗](#)

[How Microsoft builds its fast and reliable global network ↗](#)

[Office 365 Networking blog ↗](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Assessing Microsoft 365 network connectivity

Article • 03/15/2024

This article applies to Microsoft 365 Enterprise.

Microsoft 365 is designed to enable customers all over the world to connect to the service using an internet connection. As the service evolves, the security, performance, and reliability of Microsoft 365 are improved based on customers using the internet to establish a connection to the service.

Customers planning to use Microsoft 365 should assess their existing and forecasted internet connectivity needs as a part of the deployment project. For enterprise class deployments reliable and appropriately sized internet connectivity is a critical part of consuming Microsoft 365 features and scenarios.

Network evaluations can be performed by many different people and organizations depending on your size and preferences. The network scope of the assessment can also vary depending on where you're at in your deployment process. To help you get a better understanding of what it takes to perform a network assessment, we've produced a network assessment guide to help you understand the options available to you. This assessment determines what steps and resources need to be added to the deployment project to enable you to successfully adopt Microsoft 365.

A comprehensive network assessment provides possible solutions to networking design challenges along with implementation details. Some network assessments show that optimal network connectivity to Microsoft 365 can be accommodated with minor configuration or design changes to the existing network and internet egress infrastructure.

Some assessments indicate network connectivity to Microsoft 365 will require additional investments in networking components. For example, enterprise networks that span branch offices and multiple geographic regions might require investments in SD-WAN solutions or optimized routing infrastructure to support internet connectivity to Microsoft 365. Occasionally an assessment indicates network connectivity to Microsoft 365 is influenced by regulation or performance requirements for scenarios such as [Skype for Business Online media quality](#). These additional requirements might lead to investments in internet connectivity infrastructure, routing optimization, and specialized direct connectivity.

Some resources to help you assess your network:

- See [Microsoft 365 network connectivity overview](#) for conceptual information about Microsoft 365 networking.
- See [Microsoft 365 Network Connectivity Principles](#) to understand the connectivity principles for securely managing Microsoft 365 traffic and getting the best possible performance.
- Sign up for [Microsoft FastTrack](#) for guided assistance with Microsoft 365 planning, design, and deployment.
- See the [Microsoft 365 connectivity test](#) section to run basic connectivity tests that provide specific guidance about networking connectivity improvements that can be made between a given user location and Microsoft 365.

 **Note**

Microsoft authorization is required to use ExpressRoute for Microsoft 365.

Microsoft reviews every customer request and only authorizes ExpressRoute for Microsoft 365 usage when a customer's regulatory requirement mandates direct connectivity. If you have such requirements, please provide the text excerpt and web link to the regulation which you interpret to mean that direct connectivity is required in the [ExpressRoute for Microsoft 365 Request Form](#) to begin a Microsoft review. Unauthorized subscriptions trying to create route filters for Microsoft 365 will receive an [error message](#).

Key points to consider when planning your network assessment for Microsoft 365:

- Microsoft 365 is a secure, reliable, high performance service that runs over the public internet. We continue to invest to enhance these aspects of the service. All Microsoft 365 services are available via internet connectivity.
- We're continually optimizing core aspects of Microsoft 365 such as availability, global reach, and performance for internet based connectivity. For example, many Microsoft 365 services leverage an expanding set of internet facing edge nodes. This edge network offers the best proximity and performance to connections coming over the internet.
- When considering using Microsoft 365 for any of the included services such as Teams or Skype for Business Online voice, video, or meeting capabilities, customers should complete an end to end network assessment and meet connectivity requirements using [Microsoft FastTrack](#).

If you're evaluating Microsoft 365 and aren't sure where to begin with your network assessment or have found network design challenges that you need assistance to overcome, work with your Microsoft account team.

The Microsoft 365 connectivity test

The [Microsoft 365 connectivity test](#) is a proof of concept (POC) network assessment tool that runs basic connectivity tests against your Microsoft 365 tenant and makes specific network design recommendations for optimal Microsoft 365 performance. The tool highlights common large enterprise network perimeter design choices that are useful for Internet web browsing but impact the performance of large SaaS applications such as Microsoft 365.

The Network Onboarding tool does the following:

- Detects your location, or you can specify a location to test
- Checks the location of your network egress
- Tests the network path to the nearest Microsoft 365 service front door
- Provides advanced tests using a downloadable Windows 10 application that makes perimeter network design recommendations related to proxy servers, firewalls, and DNS. The tool also runs performance tests for Skype for Business Online, Microsoft Teams, SharePoint and Exchange Online.

The tool has two components: a browser-based UI that collects basic connectivity information, and a downloadable Windows 10 application that runs advanced tests and returns additional assessment data.

The browser-based tool displays the following information:

- Results and impact tab
 - The location on a map of the in-use service front door
 - The location on a map of other service front doors that would provide optimal connectivity
 - Relative performance compared to other Microsoft 365 customers near you
- Details and solutions tab
 - User location by city and country/region
 - Network egress location by city, state and country/region
 - User to network egress distance
 - Microsoft 365 Exchange Online service front door location
 - Optimal Microsoft 365 Exchange Online service front door(s) for user location
 - Customers in your metro area with better performance

The Advanced Tests downloadable application provides the following additional information:

- Details and solutions tab (appended)
 - User's default gateway

- Client DNS Server
- Client DNS Recursive Resolver
- Exchange Online DNS server
- SharePoint DNS server
- Proxy server identification
- Media connectivity check
- Media quality packet loss
- Media quality latency
- Media quality jitter
- Media quality packet reorder
- Connectivity tests to multiple feature-specific endpoints
- Network path diagnostics that include tracert and latency data for the Exchange Online, SharePoint Online and Teams services

You can read about the Microsoft 365 connectivity test and provide feedback at the [Updated Microsoft 365 connectivity test POC with new network design recommendations](#) blog post. Information about future updates to this tool and other Microsoft 365 networking updates will be posted to the [Microsoft 365 Networking](#) blog.

Here's a short link you can use to come back: <https://aka.ms/o365networkconnectivity>.

Related articles

[Microsoft 365 Network Connectivity Overview](#)

[Microsoft 365 Network Connectivity Principles](#)

[Managing Microsoft 365 endpoints](#)

[Microsoft 365 URLs and IP address ranges](#)

[Microsoft 365 IP Address and URL Web service](#)

[Microsoft 365 network and performance tuning](#)

[Microsoft 365 Enterprise overview](#)

Feedback

Was this page helpful?



Provide product feedback ↗

Plan for network devices that connect to Microsoft 365 services

Article • 06/27/2024

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Some network hardware may have limitations on the number of concurrent sessions that are supported. For organizations having more than 2,000 users, we recommend that they monitor their network devices to ensure they're capable of handling the additional Microsoft 365 service traffic. Simple Network Management Protocol (SNMP) monitoring software can help you do this.

This article is part of [Network planning and performance tuning for Microsoft 365](#).

On-premises outgoing Internet proxy settings also affect connectivity to Microsoft 365 services for your client applications. You must also configure your network proxy devices to allow connections for Microsoft cloud services URLs and applications. Every organization is different. To get an idea for how Microsoft manages this process and the amount of bandwidth we provision, [read the case study](#) ↗ .

The following Skype for Business Help articles have more information about Skype for Business settings:

- [Troubleshooting Skype for Business Online sign-in errors for administrators](#)
- [You cannot connect to Skype for Business, or certain features don't work, because an on-premises firewall blocks the connection](#) ↗

ⓘ Note

While many of these settings are Skype for Business-specific, the general guidance on network configuration is useful for all Microsoft 365 services.

Determining Network Capacity

Every network device that exists on a connection has its capacity limit. These devices include the client and server network adapters, routers, switches, and hubs that interconnect them. Adequate network capacity means that none of them are saturated. Monitoring network activity is essential to help ensure that the actual loads on all

network devices are less than their maximum capacity. Network capacity affects proxy device performance.

In most situations, the Internet connection bandwidth sets the limit for the amount of traffic. Weak performance during peak traffic hours is probably caused by excessive use of the Internet link. This situation also applies to a branch office scenario, where branch office proxy server computers are connected to the proxy device at the branch's headquarters over a slow Wide Area Network (WAN) link.

To test network capacity, monitor the network activity on the proxy network interface. If it's more than 75 percent of the maximum bandwidth of any network interface, consider increasing the bandwidth of the network infrastructure that's inadequate. Or, consider using advanced features, such as HTTP compression.

WAN Accelerators

If your organization uses wide area network (WAN) acceleration proxy appliances, you may encounter issues when you access the Microsoft 365 services. You may need to optimize your network device or devices to ensure that your users have a consistent experience when accessing Microsoft 365. For example, Microsoft 365 services encrypt some Microsoft 365 content and the TCP header. Your device may not be able to handle this kind of traffic.

Read our support statement about [Using WAN Optimization Controller or Traffic/Inspection devices with Microsoft 365](#).

Hardware and Software Load-balancing Devices

Your organization needs to use a hardware load balancer (HLB) or a Network Load Balancing (NLB) solution to distribute requests to your Active Directory Federation Services (AD FS) servers and/or your Exchange hybrid servers. Load-balancing devices control the network traffic to the on-premises servers. These servers are crucial in helping to ensure the availability of single sign-on and Exchange hybrid deployment.

We provide a software-based NLB solution built into Windows Server. Microsoft 365 supports this solution to achieve load balancing.

Firewalls and proxies

For more details on configuring firewalls and proxies to connect to Microsoft 365, read [Managing Microsoft 365 endpoints](#), [Assessing Microsoft 365 network connectivity](#), and [Microsoft 365 endpoints FAQ](#) to learn more about devices and circuit selection.

See also

[Setup guides for Microsoft 365 services](#)

[Microsoft 365 Enterprise overview](#)

Feedback

Was this page helpful?



Yes



No

[Provide product feedback](#)

Network and migration planning for Office 365

Article • 04/15/2024

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

This article contains links to information about network planning and testing, and migration to Office 365.

Before you deploy for the first time or migrate to Office 365, you can use the information in these articles to estimate the bandwidth you need and then to test and verify that you have enough bandwidth to deploy or migrate to Office 365.

This article is part of [Network planning and performance tuning for Office 365](#).

For the steps to optimize your network for Microsoft 365 and other Microsoft cloud platforms and services, see the [Microsoft Cloud Networking for Enterprise Architects](#) poster.

Estimate network bandwidth requirements

Using Office 365 might increase the utilization of your organization's internet circuit. It's important to determine if the amount of bandwidth currently available is enough to handle the estimated increase once Office 365 is fully deployed while leaving at least 20% capacity to handle the busiest of days.

To estimate the bandwidth, use the following steps:

1. Assess the number of clients that will use each Internet egress. Let our multi-terabit network handle as much of the connection as possible.
2. Determine which Office 365 services and features will be available for clients to use. You'll likely have groups of people with different services or usage profiles.
3. Measure the network use for a pilot group of clients. Ensure the pilot clients are representative of the different profiles of people in the organization and the different geographic locations. You can cross-check your results against our old calculators for [Exchange](#) and [Microsoft Teams](#) or the [case study](#) we performed on our own network.
4. Use the measurements from the pilot group to extrapolate the entire organization's needs and retest to validate the estimations before making any

changes to your network.

Test your existing network

Network tools. Test and validate your Internet bandwidth to determine download, upload, and latency constraints. These tools will help you determine the capabilities of your network for migration as well as after you're fully deployed.

- [Microsoft Remote Connectivity Analyzer](#) : Tests connectivity in your Exchange Online environment.
- Use the [Microsoft Support and Recovery Assistant for Office 365](#) to fix Outlook and Office 365 problems.
- [Microsoft 365 network connectivity test tool](#): Tests Microsoft 365 network connectivity.

Best practices for network planning and improving migration performance for Office 365

Dig a little deeper into these best practices for more information about improving your Office 365 experience.

1. Want to get started helping your users right away? See [Best practices for using Office 365 on a slow network](#) for tips on using Office 365, including SharePoint, Exchange Online, and Lync Online, when your network just isn't cooperating. This article links out to loads of content on TechNet and Support.office.com for optimizing your Office 365 experience and includes information on easy ways to customize your web pages and how to set your Internet Explorer settings for the best Office 365 experience.
2. Read [Office 365 Network Connectivity Principles](#) to understand the connectivity principles for securely managing Office 365 traffic and getting the best possible performance. This article will help you understand the most recent guidance for securely optimizing Office 365 network connectivity.
3. Improve mail migration performance by carefully managing the schedule for Windows Updates. You can update your client computers in batches and ensure that all client computers are updated before migrating to Office 365 to regulate

the use of network bandwidth. For more information, see [Manually update and configure desktops for Office 365 for the latest updates](#).

4. Office 365 network traffic performs best when it's treated as a trusted Internet service and allowed to bypass much of the traditional filtering and scanning that some organizations place on network traffic to untrusted Internet services. This typically includes removing outbound processing such as proxy user authentication and packet inspection, as well as ensuring local egress to the Internet with the proper Network Address Translation (NAT) and enough bandwidth capacity to handle the increased network requests. Refer to [Managing Office 365 endpoints](#) for additional guidance on configuring your network to handle Office 365 as a trusted Internet service on your network.
5. Ensure [Managing Office 365 endpoints](#). The additional traffic going to Office 365 results in an increase of outbound proxy connections and an increase in secure traffic over TLS/SSL.
6. If your outbound proxies require user authentication you might experience slow connectivity or a loss of functionality. Bypassing the authentication requirement for the Office 365 domains can reduce this overhead.
7. If you have a large number of shared calendars and mailboxes, you might see an increase in the number of connections from Outlook to Exchange. For instance, the Outlook client may open up to two additional connections for each shared calendar in use. In this situation, ensure that the egress proxy can handle the connections, or bypass the proxy for connections to Office 365 for Outlook.
8. Determine the maximum number of supported devices for a public IP address and how to load balance across multiple IP addresses. For more information, see [NAT support with Office 365](#).
9. If you're inspecting outbound connections from computers on your network, bypassing this filtering to the Office 365 domains will improve connectivity and performance. Additionally, bypassing outbound inspection often removes the need for a single Internet egress and enables local Internet egress for Office 365 destined network requests.
10. Some customers find internal network settings can affect performance. Settings such as maximum transmission unit (MTU) size, network autonegotiation or autodetection, and suboptimal routes to the Internet are common places to look.

Network planning reference for Office 365

These articles contain detailed Office 365 network reference information.

- [Managing Office 365 endpoints ↗](#)
- [Content delivery networks](#)
- [External Domain Name System records for Office 365](#)
- [IPv6 support in Office 365 services](#)
- [Office 365 Network Connectivity Principles](#)
- [Plan for network devices that connect to Office 365 services](#)
- [Setup guides for Office 365 services](#)

See also

[Microsoft 365 Enterprise overview](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Add a domain to Microsoft 365

Article • 08/11/2024

[Check the Domains FAQ](#) if you don't find what you're looking for.

Check out all of our small business content on [Small business help & learning](#).

Check out [Microsoft 365 small business help](#) on YouTube.

Before you begin

To add, modify, or remove domains, you **must** be a **Domain Name Administrator** of a [business or enterprise plan](#). These changes affect the whole tenant; *Customized administrators* or *regular users* can't make these changes.

Tip

If you need help with the steps in this topic, consider [working with a Microsoft small business specialist](#). With Business Assist, you and your employees get around-the-clock access to small business specialists as you grow your business, from onboarding to everyday use.

Watch: Add a domain

Check out this video and others on our [YouTube channel](#).

<https://www.microsoft.com/en-us/videoplayer/embed/RE4dN8c?autoplay=false&postJsIMsg=true>

Your company might need multiple domain names for different purposes. For example, you might want to add a different spelling of your company name because customers are already using it and their communications failed to reach you.

Where possible, we recommend that your organization use a custom domain name, as it can enhance your email's appearance and improve its reputation.

Tip

Where possible, we recommend that your organization use a custom domain name, as it can enhance your email's appearance and improve its reputation.

1. In the Microsoft 365 admin center, choose [Setup](#).
2. Select **Get your custom domain set up**, then **Get Started > Add domain**.
3. Enter the new domain name that you want to add, and then select **Next**.
4. Sign in to your domain registrar, and then select **Next**.
5. Choose the services for your new domain.
6. Select **Next > Authorize > Next**, and then **Finish**. Your new domain is added.

Add a domain

Follow these steps to add, set up, or continue setting up a domain.

1. Go to the admin center at <https://portal.partner.microsoftonline.cn>.
2. Go to the **Settings > Domains** page.
3. Select **Add domain**.
4. Enter the name of the domain you want to add, then select **Next**.
5. Choose how you want to verify that you own the domain.
 - a. If your domain registrar uses **Domain Connect**, Microsoft [will set up your records automatically](#) by having you sign in to your registrar and confirm the connection to Microsoft 365. You are returned to the admin center and Microsoft automatically verifies your domain.
 - b. You can use a TXT record to verify your domain. Select this and select **Next** to see instructions for how to add this DNS record to your registrar's website. It can take up to 10 minutes to verify after you add the record although some DNS hosting providers require up to 48 hours.
 - c. You can add a text file to your domain's website. **Select** and download the .txt file from the setup wizard, then **upload** the file to your website's top level folder. The path to the file should look similar to: `http://mydomain.com/ms39978200.txt`. We confirm you own the domain by finding the file on your website.
6. Choose how you want to make the DNS changes required for Microsoft to use your domain.
 - a. Choose **Add the DNS records for me** if your registrar supports **Domain Connect**, and Microsoft [will set up your records automatically](#) by having you sign in to your registrar and confirm the connection to Microsoft 365.

- b. Choose **I'll add the DNS records myself** if you want to attach only specific Microsoft 365 services to your domain or if you want to skip it for now and do this later. **Choose this option if you know exactly what you're doing.**
7. If you chose to *add DNS records yourself*, select **Next** and you see a page with all the records that you need to add to your registrars website to set up your domain.
If the portal doesn't recognize your registrar, you can [follow these general instructions](#).
If you don't know the DNS hosting provider or domain registrar for your domain, see [Find your domain registrar or DNS hosting provider](#).
If you want to wait for later, either unselect all the services and select **Continue**, or in the previous domain connection step, choose **More Options** and select **Skip this for now**.
8. Select **Finish** - you're done!

Add or edit custom DNS records

Follow these steps to add a custom record for a website or third party service.

1. Sign in to the [Microsoft 365 admin center](#).
2. Go to the **Settings > Domains** page.
3. On the **Domains** page, select a domain.
4. Under **DNS records**, select **Custom Records**; then select **Add record**.
5. Select the type of DNS record you want to add and type the information for the new record.
6. Select **Save**.

Registrars with Domain Connect

[Domain Connect](#) enabled registrars let you add your domain to Microsoft 365 in a three-step process that takes minutes.

In the wizard, we confirm that you own the domain, and then automatically set up your domain's records, so that email comes to Microsoft 365 and other Microsoft 365 services, like Teams, work with your domain.

Note

Make sure you disable any popup blockers in your browser before you start the setup wizard.

Domain Connect registrars integrating with Microsoft 365

- [Aruba.it ↗](#)
- [IONOS ↗](#)
- [EuroDNS ↗](#)
- [Cloudflare ↗](#)
- [GoDaddy \(*Media Temple*\) ↗](#)
- [WordPress.com ↗](#)
- [Plesk ↗](#)
- SecureServer or WildWestDomains (GoDaddy resellers using SecureServer DNS hosting)
 - Examples:
 - [DomainsPricedRight ↗](#)
 - [DomainRightNow ↗](#)

What happens to my email and website?

After you finish setup, the MX record for your domain is updated to point to Microsoft 365 and all email for your domain will start coming to Microsoft 365. Make sure you add users and set up mailboxes in Microsoft 365 for everyone who gets email on your domain!

If you have a website that you use with your business, it keeps working where it is. The Domain Connect setup steps don't affect your website.

Add an `onmicrosoft.com` domain

Each Microsoft 365 organization can have up to five `onmicrosoft.com` domains.

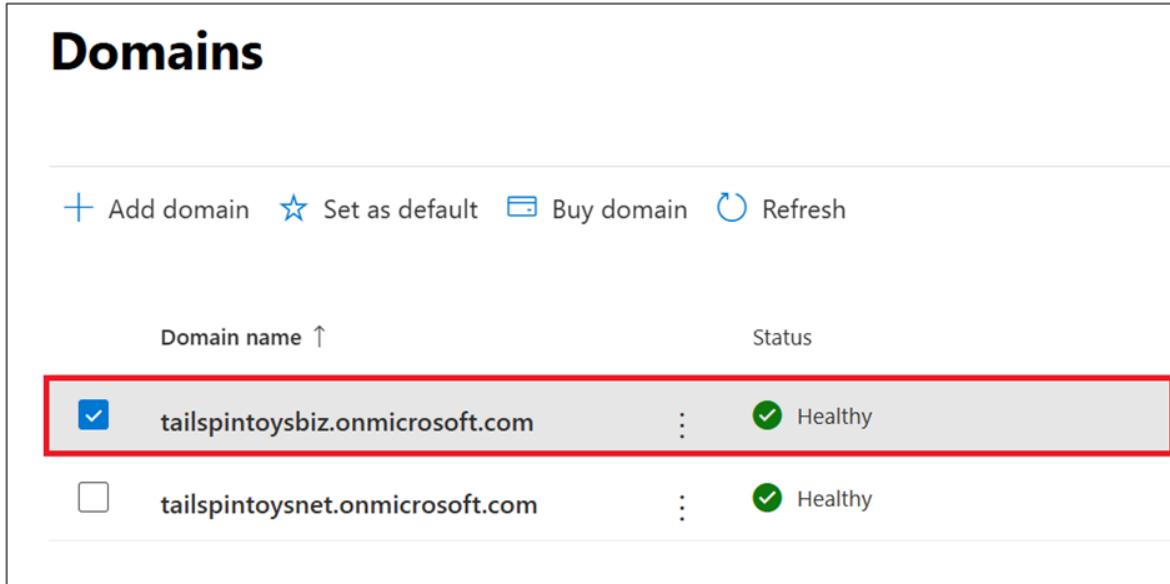
Note

You must be a Domain Name admin to add a domain. Creating an additional `.onmicrosoft` domain and using it as your default will not do a rename for SharePoint Online. To make changes to your `.onmicrosoft` SharePoint domain you would need to use the [SharePoint domain rename preview](#) (currently available to

any tenant with less than 10,000 sites). If you're using Microsoft 365 mail services, removal of your initial .onmicrosoft domain is not supported.

To add an onmicrosoft.com domain:

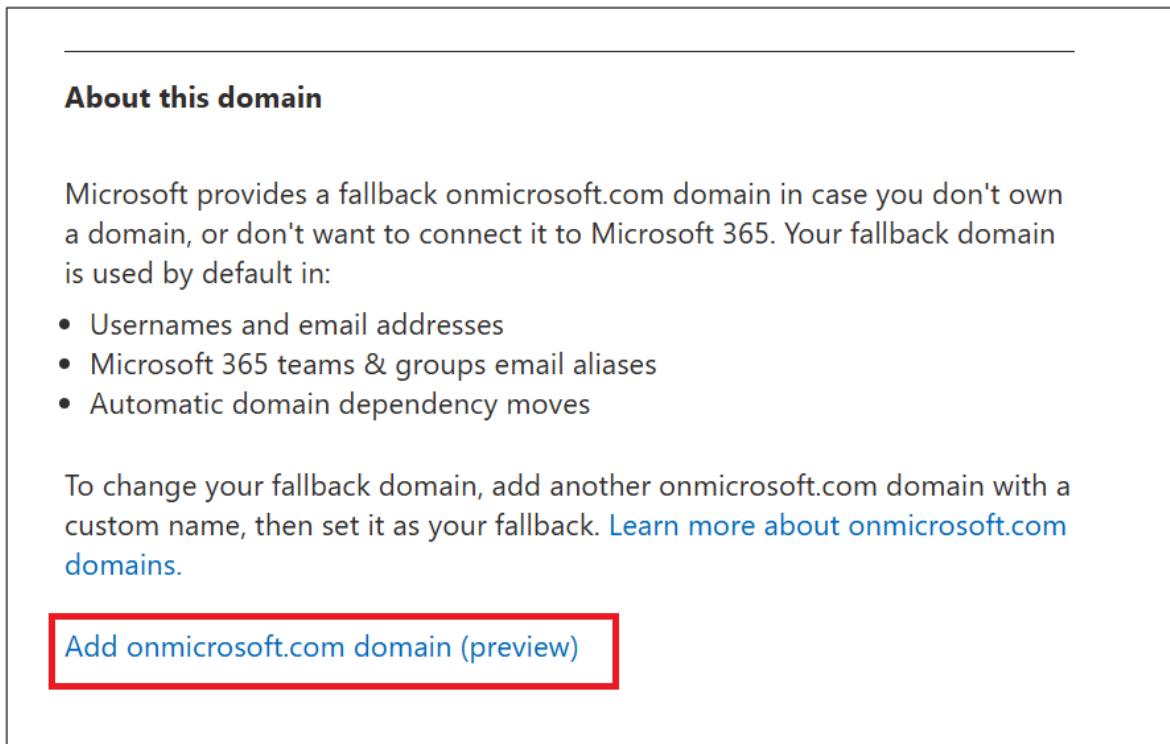
1. In the Microsoft 365 admin center, select **Settings**, and then select **Domains** ↗.
2. Select an existing *.onmicrosoft.com* domain.



The screenshot shows the Microsoft 365 Domains page. At the top, there are buttons for '+ Add domain', 'Set as default', 'Buy domain', and 'Refresh'. Below this is a table with two rows. The first row, containing 'tailspintoybiz.onmicrosoft.com', has a checked checkbox in the first column and a green checkmark in the 'Status' column. The second row, containing 'tailspintoysnet.onmicrosoft.com', has an unchecked checkbox in the first column and a green checkmark in the 'Status' column. A red box highlights the first row.

Domain name ↑		Status
<input checked="" type="checkbox"/>	tailspintoybiz.onmicrosoft.com	: ✓ Healthy
<input type="checkbox"/>	tailspintoysnet.onmicrosoft.com	: ✓ Healthy

3. On the **Overview** tab, select **Add onmicrosoft.com domain**.



The screenshot shows the Microsoft 365 Overview page. Under the 'About this domain' section, it says: 'Microsoft provides a fallback onmicrosoft.com domain in case you don't own a domain, or don't want to connect it to Microsoft 365. Your fallback domain is used by default in:' followed by a bulleted list: '• Usernames and email addresses', '• Microsoft 365 teams & groups email aliases', and '• Automatic domain dependency moves'. Below this, it says: 'To change your fallback domain, add another onmicrosoft.com domain with a custom name, then set it as your fallback. [Learn more about onmicrosoft.com domains](#)'. At the bottom, there is a red-bordered button labeled 'Add onmicrosoft.com domain (preview)'.

4. On the **Add onmicrosoft domain** page, in the **Domain name** box, enter the name for your new onmicrosoft.com domain.

Add an onmicrosoft.com domain (preview)

Use your organization's name or brand to customize a new onmicrosoft.com domain. After it's added, you can make it your fallback domain instead of M365B309532.onmicrosoft.com.

i This domain can't be removed after it's added. Make sure the spelling is correct before you add the domain, as you can only have 5 total onmicrosoft.com domains.

Domain name *

tailspintosbiz

onmicrosoft.com

! Note

Make sure to verify the spelling and accuracy of the domain name you entered. You are limited to five onmicrosoft.com domains, and currently they cannot be deleted once they are created.

5. Select **Add domain**. When successfully added, you'll see a message stating this.

Add an onmicrosoft.com domain (preview)

✓ Domain added. [Go to the new domain](#) to make tailspintosbiz.onmicrosoft.com your fallback.

You can set any domain you own as your default domain.

For more information on how to add an onmicrosoft.com domain, see [Add or replace your onmicrosoft.com domain](#).

Related content

[Domains FAQ](#) (article)

[What is a domain?](#) (article)

[Buy a domain name in Microsoft 365](#) (article)

[Add DNS records to connect your domain \(article\)](#)

[Change nameservers to set up Microsoft 365 with any domain registrar \(article\)](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Microsoft 365 IP Address and URL web service

Article • 02/05/2024

The Microsoft 365 IP Address and URL web service helps you better identify and differentiate Microsoft 365 network traffic, making it easier for you to evaluate, configure, and stay up to date with changes. This REST-based web service replaces the previous XML downloadable files, which were phased out on October 2, 2018.

As a customer or a network perimeter device vendor, you can build against the web service for Microsoft 365 IP address and FQDN entries. You can access the data directly in a web browser using these URLs:

- For the latest version of the Microsoft 365 URLs and IP address ranges, use <https://endpoints.office.com/version>.
- For the data on the Microsoft 365 URLs and IP address ranges page for firewalls and proxy servers, use <https://endpoints.office.com/endpoints/worldwide>.
- To get all the latest changes since July 2018 when the web service was first available, use <https://endpoints.office.com/changes/worldwide/0000000000>.

As a customer, you can use this web service to:

- Update your PowerShell scripts to obtain Microsoft 365 endpoint data and modify any formatting for your networking devices.
- Use this information to update PAC files deployed to client computers.

As a network perimeter device vendor, you can use this web service to:

- Create and test device software to download the list for automated configuration.
- Check for the current version.
- Get the current changes.

Note

If you are using Azure ExpressRoute to connect to Microsoft 365, please review [Azure ExpressRoute for Microsoft 365](#) to familiarize yourself with the Microsoft 365 services supported over Azure ExpressRoute. Also review the article [Microsoft 365 URLs and IP address ranges](#) to understand which network requests for Microsoft 365 applications require Internet connectivity. This will help to better configure your perimeter security devices.

For more information, see:

- [Announcement blog post in the Office 365 Tech Community Forum](#)
- [Office 365 Tech Community Forum for questions about use of the web services](#)

Common parameters

These parameters are common across all the web service methods:

- **format=<JSON | CSV>** —By default, the returned data format is JSON. Use this optional parameter to return the data in comma-separated values (CSV) format.
- **ClientRequestId=<guid>** —A required GUID that you generate for client association. Generate a unique GUID for each machine that calls the web service (the scripts included on this page generate a GUID for you). Don't use the GUIDs shown in the following examples because they might be blocked by the web service in the future. GUID format is xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx, where x represents a hexadecimal number.

To generate a GUID, you can use the [New-Guid](#) PowerShell command, or use an online service such as [Online GUID Generator](#).

Version web method

Microsoft updates the Microsoft 365 IP address and FQDN entries at the beginning of each month. Out-of-band updates are sometimes published due to support incidents, security updates or other operational requirements.

The data for each published instance is assigned a version number, and the version web method enables you to check for the latest version of each Microsoft 365 service instance. We recommend that you check the version not more than once an hour.

Parameters for the version web method are:

- **AllVersions=<true | false>** —By default, the version returned is the latest. Include this optional parameter to request all published versions since the web service was first released.
- **Format=<JSON | CSV | RSS>** —In addition to the JSON and CSV formats, the version web method also supports RSS. You can use this optional parameter along with the *AllVersions=true* parameter to request an RSS feed that can be used with Outlook or other RSS readers.

- **Instance=<Worldwide | China | USGovDoD | USGovGCCHigh>** —This optional parameter specifies the instance to return the version for. If omitted, all instances are returned. Valid instances are: Worldwide, China, USGovDoD, USGovGCCHigh.

The version web method isn't rate limited and doesn't ever return 429 HTTP Response Codes. The response to the version web method does include a cache-control header recommending caching of the data for 1 hour. The result from the version web method can be a single record or an array of records. The elements of each record are:

- **instance**—The short name of the Microsoft 365 service instance.
- **latest**—The latest version for endpoints of the specified instance.
- **versions**—A list of all previous versions for the specified instance. This element is only included if the *AllVersions* parameter is true.

Version web method examples

Example 1 request URI: <https://endpoints.office.com/version?ClientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7> ↗

This URI returns the latest version of each Microsoft 365 service instance. Example result:

```
JSON
[{"instance": "Worldwide", "latest": "2018063000"}, {"instance": "USGovDoD", "latest": "2018063000"}, {"instance": "USGovGCCHigh", "latest": "2018063000"}, {"instance": "China", "latest": "2018063000"}]
```

ⓘ Important

The GUID for the ClientRequestID parameter in these URLs are only an example. To try the web service URLs out, generate your own GUID. The GUIDs shown in these

examples may be blocked by the web service in the future.

Example 2 request URI: <https://endpoints.office.com/version/Worldwide?>

[ClientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7 ↗](#)

This URI returns the latest version of the specified Microsoft 365 service instance.

Example result:

JSON

```
{  
  "instance": "Worldwide",  
  "latest": "2018063000"  
}
```

Example 3 request URI: [https://endpoints.office.com/version/Worldwide?Format=CSV&ClientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7 ↗](https://endpoints.office.com/version/Worldwide?Format=CSV&ClientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7)

This URI shows output in CSV format. Example result:

CSV

```
instance,latest  
Worldwide,2018063000
```

Example 4 request URI: [https://endpoints.office.com/version/Worldwide?AllVersions=true&ClientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7 ↗](https://endpoints.office.com/version/Worldwide?AllVersions=true&ClientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7)

This URI shows all prior versions that have been published for the Microsoft 365 worldwide service instance. Example result:

JSON

```
{  
  "instance": "Worldwide",  
  "latest": "2018063000",  
  "versions": [  
    "2018063000",  
    "2018062000"  
  ]  
}
```

Example 5 RSS Feed URI: [https://endpoints.office.com/version/worldwide?clientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7&allVersions=true&format=RSS ↗](https://endpoints.office.com/version/worldwide?clientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7&allVersions=true&format=RSS)

This URI shows an RSS feed of the published versions that include links to the list of changes for each version. Example result:

```
XML

<?xml version="1.0" encoding="ISO-8859-1"?>
<rss version="2.0" xmlns:a10="https://www.w3.org/2005/Atom">
<channel>
<link>https://aka.ms/o365ip</link>
<description/>
<language>en-us</language>
<lastBuildDate>Thu, 02 Aug 2018 00:00:00 Z</lastBuildDate>
<item>
<guid isPermaLink="false">2018080200</guid>
<link>https://endpoints.office.com/changes/Worldwide/2018080200?
singleVersion&clientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7</link>
<description>Version 2018080200 includes 2 changes. IPs: 2 added and 0
removed.</description>
<pubDate>Thu, 02 Aug 2018 00:00:00 Z</pubDate>
</item>
```

Endpoints web method

The endpoints web method returns all records for IP address ranges and URLs that make up the Microsoft 365 service. The latest data from the endpoints web method should always be used for network device configuration. Microsoft provides advance notice 30 days prior to publishing new additions to give you time to update access control lists and proxy server bypass lists. We recommend that you only call the endpoints web method again when the version web method indicates that a new version of the data is available.

Parameters for the endpoints web method are:

- **ServiceAreas=<Common | Exchange | SharePoint | Skype>** —A comma-separated list of service areas. Valid items are *Common*, *Exchange*, *SharePoint*, and *Skype*. Because *Common* service area items are a prerequisite for all other service areas, the web service always includes them. If you don't include this parameter, all service areas are returned.
- **TenantName=<tenant_name>** —Your Microsoft 365 tenant name. The web service takes your provided name and inserts it in parts of URLs that include the tenant name. If you don't provide a tenant name, those parts of URLs have the wildcard character (*).
- **NoIPv6=<true | false>** —Set the value to *true* to exclude IPv6 addresses from the output if you don't use IPv6 in your network.

- **Instance=<Worldwide | China | USGovDoD | USGovGCCHigh>** —This required parameter specifies the instance from which to return the endpoints. Valid instances are: *Worldwide*, *China*, *USGovDoD*, and *USGovGCCHigh*.

If you call the endpoints web method too many times from the same client IP address, you might receive HTTP response code 429 (*Too Many Requests*). If you get this response code, wait 1 hour before repeating your request, or generate a new GUID for the request. As a general best practice, only call the endpoints web method when the version web method indicates that a new version is available.

The result from the endpoints web method is an array of records in which each record represents a specific endpoint set. The elements for each record are:

- **id**—The immutable ID number of the endpoint set.
- **serviceArea**—The service area that this is part of: *Common*, *Exchange*, *SharePoint*, or *Skype*.
- **urls**—URLs for the endpoint set. A JSON array of DNS records. Omitted if blank.
- **tcpPorts**—TCP ports for the endpoint set. All ports elements are formatted as a comma-separated list of ports or port ranges separated by a dash character (-). Ports apply to all IP addresses and all URLs in the endpoint set for a given category. Omitted if blank.
- **udpPorts**—UDP ports for the IP address ranges in this endpoint set. Omitted if blank.
- **ips**—The IP address ranges associated with this endpoint set as associated with the listed TCP or UDP ports. A JSON array of IP address ranges. Omitted if blank.
- **category**—The connectivity category for the endpoint set. Valid values are *Optimize*, *Allow*, and *Default*. If you search the endpoints web method output for the category of a specific IP address or URL, it's possible that your query will return multiple categories. In such a case, follow the recommendation for the highest priority category. For example, if the endpoint appears in both *Optimize* and *Allow*, you should follow the requirements for *Optimize*. Required.
- **expressRoute** — *True* if this endpoint set is routed over ExpressRoute, *False* if not.
- **required** — *True* if this endpoint set is required to have connectivity for Microsoft 365 to be supported. *False* if this endpoint set is optional.
- **notes**—For optional endpoints, this text describes Microsoft 365 functionality that would be unavailable if IP addresses or URLs in this endpoint set can't be accessed at the network layer. Omitted if blank.

Endpoints web method examples

Example 1 request URI: <https://endpoints.office.com/endpoints/Worldwide?>

[ClientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7 ↗](#)

This URI obtains all endpoints for the Microsoft 365 worldwide instance for all workloads. Example result that shows an excerpt of the output:

```
JSON

[

  {

    "id": 1,
    "serviceArea": "Exchange",
    "serviceAreaDisplayName": "Exchange Online",
    "urls": [
      [
        "*.protection.outlook.com"
      ],
      "ips": [
        [
          "2a01:111:f403::/48", "23.103.132.0/22", "23.103.136.0/21",
          "23.103.198.0/23", "23.103.212.0/22", "40.92.0.0/14", "40.107.0.0/17",
          "40.107.128.0/18", "52.100.0.0/14", "213.199.154.0/24",
          "213.199.180.128/26", "94.245.120.64/26", "207.46.163.0/24",
          "65.55.88.0/24", "216.32.180.0/23", "23.103.144.0/20", "65.55.169.0/24",
          "207.46.100.0/24", "2a01:111:f400:7c00::/54", "157.56.110.0/23",
          "23.103.200.0/22", "104.47.0.0/17", "2a01:111:f400:fc00::/54",
          "157.55.234.0/24", "157.56.112.0/24", "52.238.78.88/32"
        ],
        "tcpPorts": "443",
        "expressRoute": true,
        "category": "Allow"
      },
      {
        "id": 2,
        "serviceArea": "Exchange",
        "serviceAreaDisplayName": "Exchange Online",
        "urls": [
          [
            "*.mail.protection.outlook.com"
          ]
        ],
        "ips": [
          [
            "2a01:111:f403::/48", "23.103.132.0/22", "23.103.136.0/21",
            "23.103.198.0/23", "23.103.212.0/22", "40.92.0.0/14", "40.107.0.0/17",
            "40.107.128.0/18", "52.100.0.0/14", "213.199.154.0/24",
            "213.199.180.128/26", "94.245.120.64/26", "207.46.163.0/24",
            "65.55.88.0/24", "216.32.180.0/23", "23.103.144.0/20", "65.55.169.0/24",
            "207.46.100.0/24", "2a01:111:f400:7c00::/54", "157.56.110.0/23",
            "23.103.200.0/22", "104.47.0.0/17", "2a01:111:f400:fc00::/54",
            "157.55.234.0/24", "157.56.112.0/24", "52.238.78.88/32"
          ],
          "tcpPorts": "443",
          "expressRoute": true,
          "category": "Allow"
        }
      ]
    ]
  }
]
```

The full output of the request in this example would contain other endpoint sets.

Example 2 request URI: <https://endpoints.office.com/endpoints/Worldwide?ServiceAreas=Exchange&ClientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7>

This example obtains endpoints for the Microsoft 365 Worldwide instance for Exchange Online and dependencies only.

The output, for example, 2 is similar to example 1 except that the results wouldn't include endpoints for SharePoint or Skype for Business Online.

Changes web method

The changes web method returns the most recent updates that have been published, typically the previous month's changes to IP address ranges and URLs.

The most critical changes to endpoints data are new URLs and IP addresses. Failure to add an IP address to a firewall access control list or a URL to a proxy server bypass list can cause an outage for Microsoft 365 users behind that network device.

Notwithstanding operational requirements, new endpoints are published to the web service 30 days in advance of the date the endpoints are provisioned for use to give you time to update access control lists and proxy server bypass lists.

The required parameter for the changes web method is:

- **Version=<YYYYMMDDNN>** —Required URL route parameter. This value is the version that you have currently implemented. The web service will return the changes since that version. The format is *YYYYMMDDNN*, where *NN* is a natural number incremented if there are multiple versions required to be published on a single day, with *00* representing the first update for a given day. The web service requires the *version* parameter to contain exactly 10 digits.

The changes web method is rate limited in the same way as the endpoints web method. If you receive a 429 HTTP response code, wait 1 hour before repeating your request or generate a new GUID for the request.

The result from the changes web method is an array of records in which each record represents a change in a specific version of the endpoints. The elements for each record are:

- **id**—The immutable ID of the change record.
- **endpointSetId**—The ID of the endpoint set record that is changed.
- **disposition**—Describes what the change did to the endpoint set record. Values are *change*, *add*, or *remove*.
- **impact**—Not all changes will be equally important to every environment. This element describes the expected impact to an enterprise network perimeter environment as a result of this change. This element is included only in change records of version **2018112800** and later. Options for the impact are:
 - **AddedIp** – An IP address was added to Microsoft 365 and will be live on the service soon. This represents a change you need to take on a firewall or other layer 3 network perimeter device. If you don't add this before we start using it, you may experience an outage.
 - **AddedUrl** – A URL was added to Microsoft 365 and will be live on the service soon. This represents a change you need to take on a proxy server or URL

parsing network perimeter device. If you don't add this URL before we start using it, you may experience an outage.

- AddedIpAndUrl—Both an IP address and a URL were added. This represents a change you need to take on either a firewall layer 3 device or a proxy server or URL parsing device. If you don't add this IP/URL pair before we start using it, you may experience an outage.
- AddedSubstituteUrl – An FQDN previously unpublished due to a wildcard is now published because the wildcard URL was removed. This change is effective immediately.
- RemovedIpOrUrl – At least one IP address or URL was removed from Microsoft 365. Remove the network endpoints from your perimeter devices, but there's no deadline for you to do this.
- ChangedIsExpressRoute – The ExpressRoute support attribute was changed. If you use ExpressRoute, you might need to take action depending on your configuration.
- MovedIpOrUrl – We moved an IP address or Url between this endpoint set and another one. Generally no action is required.
- RemovedDuplicateIpOrUrl – We removed a duplicate IP address or Url but it's still published for Microsoft 365. Generally no action is required.
- OtherNonPriorityChanges – We changed something less critical than all of the other options, such as the contents of a note field.
- version—The version of the published endpoint set in which the change was introduced. Version numbers are of the format YYYYMMDDNN, where NN is a natural number incremented if there are multiple versions required to be published on a single day.
- previous—A substructure detailing previous values of changed elements on the endpoint set. This won't be included for newly added endpoint sets. Includes *ExpressRoute*, *serviceArea*, *category*, *required*, *tcpPorts*, *udpPorts*, and *notes*.
- current—A substructure detailing updated values of changes elements on the endpoint set. Includes *ExpressRoute*, *serviceArea*, *category*, *required*, *tcpPorts*, *udpPorts*, and *notes*.
- add —A substructure detailing items to be added to endpoint set collections. Omitted if there are no additions.
 - effectiveDate—Defines the date when the additions will be live in the service.
 - ips—Items to be added to the *ips* array.
 - urls- Items to be added to the *urls* array.
- remove—A substructure detailing items to be removed from the endpoint set. Omitted if there are no removals.
 - ips—Items to be removed from the *ips* array.
 - urls- Items to be removed from the *urls* array.

Changes web method examples

Example 1 request URI: <https://endpoints.office.com/changes/worldwide/0000000000?ClientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7>

This requests all previous changes to the Microsoft 365 worldwide service instance.
Example result:

```
JSON

[

  {

    "id": 424,
    "endpointSetId": 32,
    "disposition": "Change",
    "version": "2018062700",
    "remove":


      {

        "urls":


          [


            "*.api.skype.com", "skypegraph.skype.com"
          ]
      }
  },
  {


    "id": 426,
    "endpointSetId": 31,
    "disposition": "Change",
    "version": "2018062700",
    "add":


      {

        "effectiveDate": "20180609",
        "ips":


          [
            "51.140.203.190/32"
          ]
      },
    "remove":


      {

        "ips":


          [

```

Example 2 request URI: <https://endpoints.office.com/changes/worldwide/2018062700?ClientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7>

This requests changes since the specified version to the Microsoft 365 Worldwide instance. In this case, the version specified is the latest. Example result:

```
JSON

[

  {


    "id": 3,
```

```

"endpointSetId":33,
"changeDescription":"Removing old IP prefixes",
"disposition":"Change",
"version":"2018031301",
"remove":{
    "ips":["65.55.127.0/24","66.119.157.192/26","66.119.158.0/25",
    "111.221.76.128/25","111.221.77.0/26","207.46.5.0/24"]
}
},
{
"id":4,
"endpointSetId":45,
"changeDescription":"Removing old IP prefixes",
"disposition":"Change",
"version":"2018031301",
"remove":{
    "ips":["13.78.93.8/32","40.113.87.220/32","40.114.149.220/32",
    "40.117.100.83/32","40.118.214.164/32","104.208.31.113/32"]
}
}
]

```

Example PowerShell script

You can run this PowerShell script to see if there are actions you need to take for updated data. You can run this script as a scheduled task to check for a version update. To avoid excessive load on the web service, try not to run the script more than once an hour.

The script does the following:

- Checks the version number of the current Microsoft 365 Worldwide instance endpoints by calling the web service REST API.
- Checks for a current version file at `$Env:TEMP\O365_endpoints_latestversion.txt`. The path of the global variable `$Env:TEMP` is usually `C:\Users\<username>\AppData\Local\Temp`.
- If this is the first time the script has been run, the script returns the current version and all current IP addresses and URLs, writes the endpoints version to the file `$Env:TEMP\O365_endpoints_latestversion.txt` and the endpoints data output to the file `$Env:TEMP\O365_endpoints_data.txt`. You can modify the path and/or name of the output file by editing these lines:

PowerShell

```
$versionpath = $Env:TEMP + "\O365_endpoints_latestversion.txt"  
$datapath = $Env:TEMP + "\O365_endpoints_data.txt"
```

- On each subsequent execution of the script, if the latest web service version is identical to the version in the *O365_endpoints_latestversion.txt* file, the script exits without making any changes.
- When the latest web service version is newer than the version in the *O365_endpoints_latestversion.txt* file, the script returns the endpoints and filters for the **Allow** and **Optimize** category endpoints, updates the version in the *O365_endpoints_latestversion.txt* file, and writes the updated data to the *O365_endpoints_data.txt* file.

The script generates a unique *ClientRequestId* for the computer it's executed on, and reuses this ID across multiple calls. This ID is stored in the *O365_endpoints_latestversion.txt* file.

To run the PowerShell script

1. Copy the script and save it to your local hard drive or script location as *Get-O365WebServiceUpdates.ps1*.
2. Execute the script in your preferred script editor such as the PowerShell ISE or VS Code, or from a PowerShell console using the following command:

```
PowerShell  
  
powershell.exe -file <path>\Get-O365WebServiceUpdates.ps1
```

There are no parameters to pass to the script.

```
PowerShell  
  
<# Get-O365WebServiceUpdates.ps1  
From https://aka.ms/ipurlws  
v1.1 8/6/2019  
  
DESCRIPTION  
This script calls the REST API of the Microsoft 365 IP and URL Web Service  
(Worldwide instance)  
and checks to see if there has been a new update since the version stored in  
an existing  
$Env:TEMP\O365_endpoints_latestversion.txt file in your user directory's  
temp folder  
(usually C:\Users\<username>\AppData\Local\Temp).
```

```
If the file doesn't exist, or the latest version is newer than the current
version in the
file, the script returns IPs and/or URLs that have been changed, added or
removed in the latest
update and writes the new version and data to the output file
$Env:TEMP\0365_endpoints_data.txt.
```

USAGE

```
Run as a scheduled task every 60 minutes.
```

PARAMETERS

```
n/a
```

PREREQUISITES

```
PS script execution policy: Bypass
```

```
PowerShell 3.0 or later
```

```
Does not require elevation
```

```
#>
```

```
#Requires -Version 3.0
```

```
# web service root URL
```

```
$ws = "https://endpoints.office.com"
```

```
# path where output files will be stored
```

```
$versionpath = $Env:TEMP + "\0365_endpoints_latestversion.txt"
```

```
$datapath = $Env:TEMP + "\0365_endpoints_data.txt"
```

```
# fetch client ID and version if version file exists; otherwise create new
file and client ID
```

```
if (Test-Path $versionpath) {
```

```
    $content = Get-Content $versionpath
```

```
    $clientRequestId = $content[0]
```

```
    $lastVersion = $content[1]
```

```
    Write-Output ("Version file exists! Current version: " + $lastVersion)
```

```
}
```

```
else {
```

```
    Write-Output ("First run! Creating version file at " + $versionpath +
".")
```

```
    $clientRequestId = [GUID]::NewGuid().Guid
```

```
    $lastVersion = "0000000000"
```

```
    @($clientRequestId, $lastVersion) | Out-File $versionpath
```

```
}
```

```
# call version method to check the latest version, and pull new data if
version number is different
```

```
$version = Invoke-RestMethod -Uri ($ws + "/version/Worldwide?
```

```
clientRequestId=" + $clientRequestId)
```

```
if ($version.latest -gt $lastVersion) {
```

```
    Write-Host "New version of Microsoft 365 worldwide commercial service
instance endpoints detected"
```

```
    # write the new version number to the version file
```

```
    @($clientRequestId, $version.latest) | Out-File $versionpath
```

```
    # invoke endpoints method to get the new data
```

```
    $endpointSets = Invoke-RestMethod -Uri ($ws + "/endpoints/Worldwide?
```

```
clientRequestId=" + $clientRequestId)
```

```

# filter results for Allow and Optimize endpoints, and transform these
into custom objects with port and category
# URL results
$flatUrls = $endpointSets | ForEach-Object {
    $endpointSet = $_
    $urls = $($if ($endpointSet.urls.Count -gt 0) { $endpointSet.urls } 
else { @() })
    $urlCustomObjects = @()
    if ($endpointSet.category -in ("Allow", "Optimize")) {
        $urlCustomObjects = $urls | ForEach-Object {
            [PSCustomObject]@{
                category = $endpointSet.category;
                url      = $_;
                tcpPorts = $endpointSet.tcpPorts;
                udpPorts = $endpointSet.udpPorts;
            }
        }
    }
    $urlCustomObjects
}
# IPv4 results
$flatIp4s = $endpointSets | ForEach-Object {
    $endpointSet = $_
    $ips = $($if ($endpointSet.ips.Count -gt 0) { $endpointSet.ips } else
{ @() })
    # IPv4 strings contain dots
    $ip4s = $ips | Where-Object { $_ -like '*.*' }
    $ip4CustomObjects = @()
    if ($endpointSet.category -in ("Allow", "Optimize")) {
        $ip4CustomObjects = $ip4s | ForEach-Object {
            [PSCustomObject]@{
                category = $endpointSet.category;
                ip       = $_;
                tcpPorts = $endpointSet.tcpPorts;
                udpPorts = $endpointSet.udpPorts;
            }
        }
    }
    $ip4CustomObjects
}
# IPv6 results
$flatIp6s = $endpointSets | ForEach-Object {
    $endpointSet = $_
    $ips = $($if ($endpointSet.ips.Count -gt 0) { $endpointSet.ips } else
{ @() })
    # IPv6 strings contain colons
    $ip6s = $ips | Where-Object { $_ -like '*:*' }
    $ip6CustomObjects = @()
    if ($endpointSet.category -in ("Optimize")) {
        $ip6CustomObjects = $ip6s | ForEach-Object {
            [PSCustomObject]@{
                category = $endpointSet.category;
                ip       = $_;
                tcpPorts = $endpointSet.tcpPorts;
                udpPorts = $endpointSet.udpPorts;
            }
        }
    }
    $ip6CustomObjects
}

```

```

        }
    }
$ip6CustomObjects
}

# write output to screen
Write-Output ("Client Request ID: " + $clientRequestId)
Write-Output ("Last Version: " + $lastVersion)
Write-Output ("New Version: " + $version.latest)
Write-Output ""
Write-Output "IPv4 Firewall IP Address Ranges"
($flatIp4s.ip | Sort-Object -Unique) -join "," | Out-String
Write-Output "IPv6 Firewall IP Address Ranges"
($flatIp6s.ip | Sort-Object -Unique) -join "," | Out-String
Write-Output "URLs for Proxy Server"
($flatUrls.url | Sort-Object -Unique) -join "," | Out-String
Write-Output ("IP and URL data written to " + $datapath)

# write output to data file
Write-Output "Microsoft 365 IP and UL Web Service data" | Out-File
$datapath
    Write-Output "Worldwide instance" | Out-File $datapath -Append
    Write-Output "" | Out-File $datapath -Append
    Write-Output ("Version: " + $version.latest) | Out-File $datapath -
Append
    Write-Output "" | Out-File $datapath -Append
    Write-Output "IPv4 Firewall IP Address Ranges" | Out-File $datapath -
Append
    ($flatIp4s.ip | Sort-Object -Unique) -join "," | Out-File $datapath -
Append
    Write-Output "" | Out-File $datapath -Append
    Write-Output "IPv6 Firewall IP Address Ranges" | Out-File $datapath -
Append
    ($flatIp6s.ip | Sort-Object -Unique) -join "," | Out-File $datapath -
Append
    Write-Output "" | Out-File $datapath -Append
    Write-Output "URLs for Proxy Server" | Out-File $datapath -Append
    ($flatUrls.url | Sort-Object -Unique) -join "," | Out-File $datapath -
Append
}
else {
    Write-Host "Microsoft 365 worldwide commercial service instance
endpoints are up-to-date."
}

```

Example Python Script

Here's a Python script, tested with Python 3.6.3 on Windows 10, that you can run to see if there are actions you need to take for updated data. This script checks the version number for the Microsoft 365 Worldwide instance endpoints. When there's a change, it

downloads the endpoints and filters for the *Allow* and *Optimize* category endpoints. It also uses a unique ClientRequestId across multiple calls and saves the latest version found in a temporary file. Call this script once an hour to check for a version update.

Python

```
import json
import tempfile
from pathlib import Path
import urllib.request
import uuid
# helper to call the webservice and parse the response
def webApiGet(methodName, instanceName, clientRequestId):
    ws = "https://endpoints.office.com"
    requestPath = ws + '/' + methodName + '/' + instanceName + '?'
    clientRequestId=' ' + clientRequestId
    request = urllib.request.Request(requestPath)
    with urllib.request.urlopen(request) as response:
        return json.loads(response.read().decode())
# path where client ID and latest version number will be stored
datapath = Path(tempfile.gettempdir()) +
'/endpoints_clientid_latestversion.txt'
# fetch client ID and version if data exists; otherwise create new file
if datapath.exists():
    with open(datapath, 'r') as fin:
        clientRequestId = fin.readline().strip()
        latestVersion = fin.readline().strip()
else:
    clientRequestId = str(uuid.uuid4())
    latestVersion = '0000000000'
    with open(datapath, 'w') as fout:
        fout.write(clientRequestId + '\n' + latestVersion)
# call version method to check the latest version, and pull new data if
version number is different
version = webApiGet('version', 'Worldwide', clientRequestId)
if version['latest'] > latestVersion:
    print('New version of Microsoft 365 worldwide commercial service
instance endpoints detected')
    # write the new version number to the data file
    with open(datapath, 'w') as fout:
        fout.write(clientRequestId + '\n' + version['latest'])
    # invoke endpoints method to get the new data
    endpointSets = webApiGet('endpoints', 'Worldwide', clientRequestId)
    # filter results for Allow and Optimize endpoints, and transform these
    into tuples with port and category
    flatUrls = []
    for endpointSet in endpointSets:
        if endpointSet['category'] in ('Optimize', 'Allow'):
            category = endpointSet['category']
            urls = endpointSet['urls'] if 'urls' in endpointSet else []
            tcpPorts = endpointSet['tcpPorts'] if 'tcpPorts' in endpointSet
        else '':
            udpPorts = endpointSet['udpPorts'] if 'udpPorts' in endpointSet
```

```

        else '':
            flatUrls.extend([(category, url, tcpPorts, udpPorts) for url in
urls])
            flatIps = []
            for endpointSet in endpointSets:
                if endpointSet['category'] in ('Optimize', 'Allow'):
                    ips = endpointSet['ips'] if 'ips' in endpointSet else []
                    category = endpointSet['category']
                    # IPv4 strings have dots while IPv6 strings have colons
                    ip4s = [ip for ip in ips if '.' in ip]
                    tcpPorts = endpointSet['tcpPorts'] if 'tcpPorts' in endpointSet
                else '':
                    udpPorts = endpointSet['udpPorts'] if 'udpPorts' in endpointSet
                else '':
                    flatIps.extend([(category, ip, tcpPorts, udpPorts) for ip in
ip4s])
                print('IPv4 Firewall IP Address Ranges')
                print(', '.join(sorted(set([ip for (category, ip, tcpPorts, udpPorts) in
flatIps]))))
                print('URLs for Proxy Server')
                print(', '.join(sorted(set([url for (category, url, tcpPorts, udpPorts)
in flatUrls]))))

        # TODO send mail (e.g. with smtplib/email modules) with new endpoints
data
else:
    print('Microsoft 365 worldwide commercial service instance endpoints are
up-to-date')

```

Web Service interface versioning

Updates to the parameters or results for these web service methods may be required in the future. After the general availability version of these web services is published, Microsoft will make reasonable efforts to provide advance notice of material updates to the web service. When Microsoft believes that an update will require changes to clients using the web service, Microsoft will keep the previous version (one version back) of the web service available for at least 12 months after the release of the new version. Customers who don't upgrade during that time may be unable to access the web service and its methods. Customers must ensure that clients of the web service continue working without error if the following changes are made to the web service interface signature:

- Adding a new optional parameter to an existing web method that doesn't have to be provided by older clients and doesn't impact the result an older client receives.
- Adding a new named attribute in one of the response REST items or other columns to the response CSV.
- Adding a new web method with a new name that isn't called by the older clients.

Update notifications

You can use a few different methods to get email notifications when changes to the IP addresses and URLs are published to the web service.

- To use a Power Automate solution, see [Use Power Automate to receive an email for changes to Microsoft 365 IP Addresses and URLs](#).
- To deploy an Azure Logic App using an ARM template, see [Office 365 Update Notification \(v1.1\)](#).
- To write your own notification script using PowerShell, see [Send-MailMessage](#).

Exporting a Proxy PAC file

[Get-PacFile](#) is a PowerShell script that reads the latest network endpoints from the Microsoft 365 IP Address and URL web service and creates a sample PAC file. For information on using Get-PacFile, see [Use a PAC file for direct routing of vital Microsoft 365 traffic](#).

Related Topics

[Microsoft 365 URLs and IP address ranges](#)

[Managing Microsoft 365 endpoints](#)

[Microsoft 365 Network Connectivity Principles](#)

[Microsoft 365 network and performance tuning](#)

[Assessing Microsoft 365 network connectivity](#)

[Media Quality and Network Connectivity Performance in Skype for Business Online](#)

[Optimizing your network for Skype for Business Online](#)

[Microsoft 365 performance tuning using baselines and performance history](#)

[Performance troubleshooting plan for Microsoft 365](#)

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Other endpoints not included in the Microsoft 365 IP Address and URL Web service

Article • 01/31/2024

Some network endpoints were previously published and haven't been included in the [Microsoft 365 IP Address and URL Web Service](#). The web service publishes network endpoints that are required for Microsoft 365 connectivity across an enterprise perimeter network. This scope currently doesn't include:

1. Network connectivity that might be required from a Microsoft datacenter to a customer network (inbound hybrid server network traffic).
2. Network connectivity from servers on a customer network across the enterprise perimeter (outbound server network traffic).
3. Uncommon scenarios for network connectivity requirements from a user.
4. DNS resolution connectivity requirement (not listed below).
5. Internet Explorer or Microsoft Edge Trusted Sites.

Apart from DNS, these instances are all optional for most customers unless you need the specific scenario that is described.

[] Expand table

Row	Purpose	Destination	Type
1	Import Service for PST and file ingestion	Refer to the Import Service for more requirements.	Uncommon outbound scenario
2	Microsoft Support and Recovery Assistant for Office 365	https://autodiscover.outlook.com https://officecdn.microsoft.com https://api.diagnostics.office.com https://apibasic.diagnostics.office.com https://autodiscover-s.outlook.com https://cloudcheckenable.azurewebsites.net https://login.live.com https://login.microsoftonline.com https://login.windows.net https://o365diagtelemetry.trafficmanager.net https://odc.officeapps.live.com https://offcatedge.azureedge.net https://officeapps.live.com	Outbound server traffic

Row	Purpose	Destination	Type
		https://outlook.office365.com https://outlookdiagnostics.azureedge.net https://sara.api.support.microsoft.com	
3	Microsoft Entra Connect (w/SSO option) WinRM & remote PowerShell	Customer STS environment (AD FS Server and AD FS Proxy) TCP ports 80 & 443	Inbound server traffic
4	STS such as AD FS Proxy servers (for federated customers only)	Customer STS (such as AD FS Proxy) Ports TCP 443 or TCP 49443 w/ClientTLS	Inbound server traffic
5	Exchange Online Unified Messaging/SBC integration	Bidirectional between on-premises Session Border Controller and *.um.outlook.com	Outbound server-only traffic
6	Mailbox Migration When mailbox migration is initiated from on-premises Exchange Hybrid to Microsoft 365, Microsoft 365 connects to your published Exchange Web Services (EWS)/Mailbox Replication Services (MRS) server. If you need to allow inbound connections only from specific source IP ranges, create a permit rule for the IP addresses listed in the Exchange Online table in Microsoft 365 URL & IP ranges . To ensure that connectivity to published EWS endpoints (like OWA) isn't blocked, make sure the MRS proxy resolves to a separate FQDN and public IP address before you restrict connections.	Customer on-premises EWS/MRS Proxy TCP port 443	Inbound server traffic
7	Exchange Hybrid coexistence functions such as Free/Busy sharing.	Customer on-premises Exchange server	Inbound server traffic
8	Exchange Hybrid proxy authentication	Customer on-premises STS	Inbound server traffic
9	Used to configure Exchange Hybrid , using the Exchange	domains.live.com on TCP ports 80 & 443, only required for Exchange 2010 SP3 Hybrid	Outbound server-only

Row	Purpose	Destination	Type
	<p>Hybrid Configuration Wizard</p> <p>Note: These endpoints are only required to configure Exchange hybrid</p>	<p>Configuration Wizard GCC High, DoD IP addresses: 40.118.209.192/32; 168.62.190.41/32</p> <p>Worldwide Commercial & GCC: *.store.core.windows.net; asl.configure.office.com; tds.configure.office.com; mshybridservice.trafficmanager.net ; aka.ms/hybridwizard; shcwreleaseprod.blob.core.windows.net/shcw/*;</p>	traffic
10	<p>The AutoDetect service is used in Exchange Hybrid scenarios with Hybrid Modern Authentication with Outlook for iOS and Android</p> <pre><email_domain>.outlookmobile.com <email_domain>.outlookmobile.us 52.125.128.0/20 52.127.96.0/23</pre>	<p>Customer on-premises Exchange server on TCP 443</p>	Inbound server traffic
11	<p>Exchange hybrid Microsoft Entra authentication</p>	<p>*.msappproxy.net</p>	TCP outbound server-only traffic
12	<p>Skype for Business in Office 2016 includes video based screen sharing, which uses UDP ports. Prior Skype for Business clients in Office 2013 and earlier used RDP over TCP port 443.</p>	<p>TCP port 443 opens to 52.112.0.0/14</p>	Skype for Business older client versions in Office 2013 and earlier
13	<p>Skype for Business hybrid on-premises server connectivity to Skype for Business Online</p>	<p>13.107.64.0/18, 52.112.0.0/14 UDP ports 50,000-59,999 TCP ports 50,000-59,999; 5061</p>	Skype for Business on-premises server outbound connectivity
14	<p>Cloud PSTN with on-premises hybrid connectivity requires network connectivity open to the on-premises hosts. For more details about Skype for Business Online hybrid configurations</p>	<p>See Plan hybrid connectivity between Skype for Business Server and Office 365</p>	Skype for Business on-premises hybrid inbound

Row	Purpose	Destination	Type
15	Authentication and identity FQDNs	<p>The FQDN <code>secure.aadcdn.microsoftonline-p.com</code> needs to be in your client's Internet Explorer (IE) or Edge Trusted Sites Zone to function.</p>	Trusted Sites
16	Microsoft Teams FQDNs	<p>If you are using Internet Explorer or Microsoft Edge, you need to enable first, and third-party cookies and add the FQDNs for Teams to your Trusted Sites. This is in addition to the suite-wide FQDNs, CDNs, and telemetry listed in row 14. See Known issues for Microsoft Teams for more information.</p>	Trusted Sites
17	SharePoint Online and OneDrive for Business FQDNs	<p>All '.sharepoint.com' FQDNs with '<tenant>' in the FQDN need to be in your client's IE or Edge Trusted Sites Zone to function. In addition to the suite-wide FQDNs, CDNs, and telemetry listed in row 14, you need to also add these endpoints.</p>	Trusted Sites
18	Yammer	<p>Yammer is only available in the browser and requires the authenticated user to be passed through a proxy. All Yammer FQDNs need to be in your client's IE or Edge Trusted Sites Zone to function.</p>	Trusted Sites
19	Use Microsoft Entra Connect to sync on-premises user accounts to Microsoft Entra ID.	<p>See Hybrid Identity Required Ports and Protocols, Troubleshoot Microsoft Entra connectivity, and Microsoft Entra Connect Health Agent Installation.</p>	Outbound server-only traffic

Row	Purpose	Destination	Type
20	Microsoft Entra Connect with 21 ViaNet in China to sync on-premises user accounts to Microsoft Entra ID.	*.digicert.com:80 *.entrust.net:80 *.chinacloudapi.cn:443 secure.aadcdn.partner.microsoftonline-p.cn:443 *.partner.microsoftonline.cn:443	Outbound server-only traffic
		Also see Troubleshoot ingress with Microsoft Entra connectivity issues .	
21	Microsoft Stream (needs the Microsoft Entra user token). Microsoft 365 Worldwide (including GCC)	*.cloudapp.net *.api.microsoftstream.com *.notification.api.microsoftstream.com amp.azure.net api.microsoftstream.com az416426.vo.msecnd.net s0.assets-yammer.com vortex.data.microsoft.com web.microsoftstream.com TCP port 443	Inbound server traffic
22	Use MFA server for multifactor authentication requests, both new installations of the server and setting it up with Active Directory Domain Services (AD DS).	See Getting started with the Azure Multi-Factor Authentication Server .	Outbound server-only traffic
23	Microsoft Graph Change Notifications Developers can use change notifications to subscribe to events in the Microsoft Graph.	Public Cloud: 52.159.23.209, 52.159.17.84, 13.78.204.0, 52.148.24.136, 52.148.27.39, 52.147.213.251, 52.147.213.181, 20.127.53.125, 40.76.162.99, 40.76.162.42, 70.37.95.92, 70.37.95.11, 70.37.92.195, 70.37.93.191, 70.37.90.219, 20.9.36.45, 20.9.35.166, 20.9.36.128, 20.9.37.73, 20.9.37.76, 20.96.21.67, 20.69.245.215, 104.46.117.15, 20.96.21.98, 20.96.21.115, 137.135.11.161, 137.135.11.116, 20.253.156.113, 137.135.11.222, 137.135.11.250, 52.159.107.50, 52.159.107.4, 52.159.124.33, 52.159.109.205, 52.159.102.72, 20.98.68.182, 20.98.68.57, 20.98.68.200, 20.98.68.203, 20.98.68.218, 20.171.81.121, 20.25.189.138, 20.171.82.192, 20.171.83.146, 20.171.83.157, 52.142.114.29, 52.142.115.31, 20.223.139.245, 51.104.159.213, 51.104.159.181, 51.124.75.43, 51.124.73.177, 104.40.209.182, 51.138.90.7, 51.138.90.52, 20.199.102.157, 20.199.102.73, 20.216.150.67, 20.111.9.46, 20.111.9.77, 13.87.81.123, 13.87.81.35, 20.90.99.1, 13.87.81.133,	Inbound server traffic

Row	Purpose	Destination	Type	
		13.87.81.141, 20.91.212.211, 20.91.212.136, 20.91.213.57, 20.91.208.88, 20.91.209.147, 20.44.210.83, 20.44.210.146, 20.212.153.162, 52.148.115.48, 52.148.114.238, 40.80.232.177, 40.80.232.118, 52.231.196.24, 40.80.233.14, 40.80.239.196, 20.48.12.75, 20.48.11.201, 20.89.108.161, 20.48.14.35, 20.48.15.147, 104.215.13.23, 104.215.6.169, 20.89.240.165, 104.215.18.55, 104.215.12.254 20.20.32.0/19, 20.190.128.0/18, 20.231.128.0/19, 40.126.0.0/18, 2603:1006:2000::/48, 2603:1007:200::/48, 2603:1016:1400::/48, 2603:1017::/48, 2603:1026:3000::/48, 2603:1027:1::/48, 2603:1036:3000::/48, 2603:1037:1::/48, 2603:1046:2000::/48, 2603:1047:1::/48, 2603:1056:2000::/48, 2603:1057:2::/48		
		Microsoft Cloud for US Government: 52.244.33.45, 52.244.35.174, 52.243.157.104, 52.243.157.105, 52.182.25.254, 52.182.25.110, 52.181.25.67, 52.181.25.66, 52.244.111.156, 52.244.111.170, 52.243.147.249, 52.243.148.19, 52.182.32.51, 52.182.32.143, 52.181.24.199, 52.181.24.220 20.140.232.0/23, 52.126.194.0/23, 2001:489a:3500::/50		
24	Network Connection Status Indicator Used by Windows 10 and 11 to determine if the computer is connected to the internet (does not apply to non-Windows clients). When this URL cannot be	TCP port 443 Note: Developers can specify different ports when creating the subscriptions.	www.msftconnecttest.com Also see Manage connection endpoints for Windows 11 Enterprise and Manage connection endpoints for Windows 10 Enterprise, version 21H2 .	Outbound server-only traffic

Row	Purpose	Destination	Type
	reached, Windows assumes it isn't connected to the Internet and M365 Apps for Enterprise will not try to verify activation status, causing connections to Exchange and other services to fail.		
25	Teams Notifications on Mobile Devices Used by Android and Apple mobile devices to receive push notifications to the Teams client for incoming calls and other Teams services. When these ports are blocked, all push notifications to mobile devices fail.	For specific ports, see FCM ports and your firewall in the Google Firebase documentation and If your Apple devices aren't getting Apple push notifications .	Outbound server-only traffic

Related Topics

[Managing Microsoft 365 endpoints](#)

[Monitor Microsoft 365 connectivity](#)

[Client connectivity](#)

[Content delivery networks](#)

[Azure IP Ranges and Service Tags – Public Cloud](#)

[Azure IP Ranges and Service Tags – US Government Cloud](#)

[Azure IP Ranges and Service Tags – Germany Cloud](#)

[Azure IP Ranges and Service Tags – China Cloud](#)

[Microsoft Public IP Space](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Additional network security requirements for Office 365 GCC High and DOD

Article • 04/11/2024

This article applies to Office 365 GCC High, Office 365 DOD, Microsoft 365 GCC High, and Microsoft 365 DOD.

Office 365 GCC High and DOD are secure cloud environments to meet the needs of the United States Government and its suppliers and contractors. These cloud environments have extra network restrictions on which external endpoints the services are permitted to access.

GCC High and DOD customers planning to use federated identities or hybrid coexistence might require Microsoft to permit inbound and/or outbound access to your existing on-premises deployments. Examples of these activities include:

- Use of federated identities (with Active Directory Federation Services or similar supported Security token service (STS))
- Hybrid coexistence with an on-premises Exchange Server or Skype for Business deployment
- Migration of existing user content from an on-premises system

To permit the service to communicate with your on-premises endpoints, you **must** send an email to Office 365 engineering for network changes.

Warning

All requests have a **three-week** SLA and cannot be expedited due to the required security and compliance controls and deployment pipelines. This includes initial onboarding network requests as well as any changes after you have migrated to the service. Make sure that your network teams are aware of this timeline and include it in their planning cycles.

Send an email to [Office 365 Government Allow-List Requests](#) with the following information:

- **To:** [Office 365 Government Allow-List Requests](#)
- **From:** A tenant administrator - the send email **must** match a Global Administrator contact in your tenant

- **Email subject:** Office 365 GCC High Network Request - contoso.onmicrosoft.us
(replace with your tenant name)

The body of your message should include the following data:

- Your Microsoft Online Services tenant name (for example, contoso.onmicrosoft.com, fabrikam.onmicrosoft.us)
- An email distribution list that Microsoft communicates with for on-going communications related to network changes and/or follow up for invalid subnets
- Indicate whether you plan to use Microsoft Teams hybrid coexistence with your on-premises deployments
- Federated identity system externally accessible URL (for example, sts.contoso.com) and IP address range in CIDR (Classless Inter-Domain Routing) notation (for example, 10.1.1.0/28)
- On-Premises public key infrastructure (PKI) Certificate Revocation List URL and IP address range in CIDR notation
- Externally accessible URL and IP address range for Exchange Server on-premises deployment in CIDR notation
- Externally accessible URL and IP address range for Skype for Business on-premises deployment in CIDR notation

For security and compliance reasons, keep in mind the following restrictions on your request:

- There's a four subnet limitation per tenant
- Subnets must be in CIDR Notation (for example, 10.1.1.0/28)
- Subnet ranges can't be larger than /24
- We **cannot** accommodate requests to allow access to commercial cloud services (commercial Office 365, Google G-Suite, Amazon Web Services, etc.)

Once Microsoft receives and approves your request, there's a three-week service-level agreement (SLA) for implementation and can't be expedited. You receive an initial acknowledgment when we receive your request and a final acknowledgment once it's complete.

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

DNS records for Office 365 DoD

Article • 04/11/2024

This article applies to Office 365 DoD and Microsoft 365 DoD

As part of onboarding to Office 365 DoD, you need to add your SMTP and SIP domains to your Online Services tenant. You do this using the New-MsolDomain cmdlet in Azure AD PowerShell or use the [Azure Government Portal](#) to start the process of adding the domain and proving ownership.

Once you have your domains added to your tenant and validated, use the following guidance to add the appropriate DNS records for the services. You might need to modify the below table to fit your organization's needs with respect to the inbound MX record(s) and any existing Exchange Autodiscover records you have in place. We strongly recommend coordinating these DNS records with your messaging team to avoid any outages or mis-delivery of email.

ⓘ Note

Azure AD and MSOnline PowerShell modules are deprecated as of March 30, 2024. To learn more, read the [deprecation update](#). After this date, support for these modules are limited to migration assistance to Microsoft Graph PowerShell SDK and security fixes. The deprecated modules will continue to function through March, 30 2025.

We recommend migrating to [Microsoft Graph PowerShell](#) to interact with Microsoft Entra ID (formerly Azure AD). For common migration questions, refer to the [Migration FAQ](#). Note: Versions 1.0.x of MSOnline may experience disruption after June 30, 2024.

Exchange Online

 Expand table

Type	Priority	Host name	Points to address or value	TTL
MX	0	@	tenant.mail.protection.office365.us (for more information, see below)	One Hour
TXT	-	@	v=spf1 include:spf.protection.office365.us -all	One Hour
CNAME	-	autodiscover	autodiscover-dod.office365.us	One Hour

Exchange Autodiscover record

If you have Exchange Server on-premises, we recommend leaving your existing record in place while you migrate to Exchange Online, and update that record once you complete your migration.

Exchange Online MX Record

The MX record value for your accepted domains follows a standard format as noted previously: *tenant.mail.protection.office365.us*, replacing *tenant* with the first part of your default tenant name.

For example, if your tenant name is *contoso.onmicrosoft.us*, you'd use *contoso.mail.protection.office365.us* as the value for your MX record.

External DNS records required for Teams

SRV records

[Expand table](#)

Type	Service	Protocol	Port	Weight	Priority	Name	Target	TTL
SRV	_sipfederationtls	_tcp	5061	1	100	@	sipfed.online.dod.skypeforbusiness.us	One Hour

Other DNS records

Important

If you have an existing *msoid* CNAME record in your DNS zone, you must **remove** the record from DNS at this time. The *msoid* record is incompatible with Microsoft 365 Enterprise Apps (*formerly Office 365 ProPlus*) and will prevent activation from succeeding.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) 

DNS records for Office 365 GCC High

Article • 04/11/2024

This article applies to Office 365 GCC High and Microsoft 365 GCC High

As part of onboarding to Office 365 GCC High, you need to add your Simple Mail Transfer Protocol (SMTP) and SIP domains to your Online Services tenant. You do this using the `New-MsolDomain` cmdlet in Azure AD PowerShell or use the [Azure Government Portal](#) to start the process of adding the domain and proving ownership.

Once you have your domains added to your tenant and validated, use the following guidance to add the appropriate DNS records for the following services. You might need to modify the below table to fit your organization's needs with respect to the inbound MX record(s) and any existing Exchange Autodiscover records you have in place. We strongly recommend coordinating these DNS records with your messaging team to avoid any outages or mis-delivery of email.

! Note

Azure AD and MSOnline PowerShell modules are deprecated as of March 30, 2024. To learn more, read the [deprecation update](#). After this date, support for these modules are limited to migration assistance to Microsoft Graph PowerShell SDK and security fixes. The deprecated modules will continue to function through March, 30 2025.

We recommend migrating to [Microsoft Graph PowerShell](#) to interact with Microsoft Entra ID (formerly Azure AD). For common migration questions, refer to the [Migration FAQ](#). Note: Versions 1.0.x of MSOnline may experience disruption after June 30, 2024.

Exchange Online

[Expand table](#)

Type	Priority	Host name	Points to address or value	TTL
MX	0	@	<i>tenant.mail.protection.office365.us</i> (for more information, see below)	One Hour
TXT	-	@	v=spf1 include:spf.protection.office365.us -all	One Hour
CNAME	-	autodiscover	autodiscover.office365.us	One Hour

Exchange Autodiscover record

If you have Exchange Server on-premises, we recommend leaving your existing record in place while you migrate to Exchange Online, and update that record once you complete your migration.

Exchange Online MX Record

The MX record value for your accepted domains follows a standard format as noted previously: *tenant.mail.protection.office365.us*, replacing *tenant* with the first part of your default tenant name.

For example, if your tenant name is *contoso.onmicrosoft.us*, you'd use *contoso.mail.protection.office365.us* as the value for your MX record.

External DNS records required for Teams

SRV records

[Expand table](#)

Type	Service	Protocol	Port	Weight	Priority	Name	Target	TTL
SRV	_sipfederationtls	_tcp	5061	1	100	@	sipfed.online.gov.skypeforbusiness.us	One Hour

Other DNS records

Important

If you have an existing *msoid* CNAME record in your DNS zone, you must **remove** the record from DNS at this time. The *msoid* record is incompatible with Microsoft 365 Enterprise Apps (*formerly Office 365 ProPlus*) and will prevent activation from succeeding.

Feedback

Was this page helpful?

Yes

No

[Provide product feedback](#) ↗

Office 365 Content Delivery Network (CDN) Quickstart

Article • 08/13/2024

You can use the built-in **Office 365 Content Delivery Network (CDN)** to host static assets (images, JavaScript, Stylesheets, WOFF files) to provide better performance for your SharePoint pages. The Office 365 CDN improves performance by caching static assets closer to the browsers requesting them, which helps to speed up downloads and reduce latency. Also, the Office 365 CDN uses the HTTP/2 protocol for improved compression and HTTP pipelining. The Office 365 CDN service is included as part of your SharePoint subscription.

For more detailed information, see [Use the Office 365 Content Delivery Network \(CDN\) with SharePoint](#).

⊗ Caution

As images are now automatically managed in a SharePoint service-managed Private CDN, the manually configured Private CDN is in the process of being deprecated. This means that customers no longer need to configure private CDN. The recommended practice remains unchanged as images will be hosted via the service-managed Private CDN automatically and Public CDN will continue to be available for all other file types, like CSS and JS. Any customers using Private CDN for file types other than images, will need to move those files into Public CDN. Public CDN is recommended for these file types, to enhance performance.

ⓘ Note

The Office 365 CDN is only available to tenants in the production (worldwide) cloud. Tenants in the US Government, China and Germany clouds do not currently support the Office 365 CDN.

Use the Page Diagnostics for SharePoint tool to identify items not in CDN

You can use the [Page Diagnostics for SharePoint tool](#) browser extension to easily list assets in your SharePoint in Microsoft 365 pages that can be added to a CDN origin.

The **Page Diagnostics for SharePoint tool** is a browser extension for the new Microsoft Edge (<https://www.microsoft.com/edge>) and Chrome browsers that analyzes both SharePoint in Microsoft 365 modern portal and classic publishing site pages. The tool provides a report for each analyzed page showing how the page performs against a defined set of performance criteria. To install and learn about the Page Diagnostics for SharePoint tool, visit [Use the Page Diagnostics tool for SharePoint](#).

When you run the Page Diagnostics for SharePoint tool on a SharePoint in Microsoft 365 page, you can select the **Diagnostic Tests** tab to see a list of assets not being hosted by the CDN. These assets are listed under the heading **Content Delivery Network (CDN) check** as shown in the screenshot following.

The screenshot shows the 'Diagnostic tests' tab of the Page diagnostics for SharePoint tool. It lists findings under three sections: 'Attention required', 'Improvement opportunities', and 'No action required'. Each section has a header with an up and down arrow icon. Under 'Attention required', there are three items: 'Large images detected' (marked with a red circle and an 'X'), 'Content Delivery Network (CDN) check' (marked with a red circle and an 'X'), and 'Requests to SharePoint' (marked with a red circle and an 'X'). Under 'Improvement opportunities', there is one item: 'Web parts using Iframes detected' (marked with a blue circle and a question mark). Under 'No action required', there are two items: 'Page weight under 500 KB' (marked with a green circle and a checkmark) and 'No web parts impacting page load time' (marked with a green circle and a checkmark). A purple callout box at the bottom left contains a note about the tool's compatibility.

Page diagnostics for SharePoint

Diagnostic tests Network trace

Attention required

- (X) Large images detected
- (X) Content Delivery Network (CDN) check
- (X) Requests to SharePoint

Improvement opportunities

- (?) Web parts using Iframes detected

No action required

- (✓) Page weight under 500 KB
- (✓) No web parts impacting page load time

! Note

The Page Diagnostics tool only works for SharePoint in Microsoft 365, and cannot be used on a SharePoint system page.

CDN Overview

The Office 365 CDN is designed to optimize performance for users by distributing frequently accessed objects like images and JavaScript files over a high-speed global network, reducing page load time and providing access to hosted objects as close as possible to the user. The CDN fetches your assets from a location called an *origin*. An origin can be a SharePoint site, document library, or folder that is accessible by a URL.

The Office 365 CDN is separated into two basic types:

- **Public CDN** is designed to be used for JS (JavaScript), CSS (StyleSheets), Web Font File (WOFF, WOFF2) and nonproprietary images like company logos.
- **Private CDN** is designed to be used for images (PNG, JPG, JPEG, etc.).

You can choose to have both public or private origins for your organization. Most organizations will choose to implement a combination of the two. Both public and private options provide similar performance gains, but each has unique attributes and advantages. For more information about public and private CDN origins, see [Choose whether each origin should be public or private](#).

How to enable Public and Private CDN with the default configuration

Before you make changes to the tenant CDN settings, you should verify that it meets compliance, security, and privacy policies of your organization.

For more detailed configuration settings, or if you have already enabled CDN and want to add additional locations (origins), see the section [Set up and configure the Office 365 CDN by using the SharePoint Management Shell](#)

Connect to your tenant using the SharePoint Management Shell:

```
PowerShell
```

```
Connect-SPOService -Url https://<YourTenantName>-admin.sharepoint.com
```

To enable your organization to use both public and private origins with the default configuration, type the following command:

```
PowerShell
```

```
Set-SPOTenantCdnEnabled -CdnType Both -Enable $true
```

Output of these cmdlets should look like the following:

```
Administrator: SharePoint Online Management Shell
PS C:\WINDOWS\system32> Connect-SPOSERVICE -Url https://[REDACTED]-admin.sharepoint.com
PS C:\WINDOWS\system32> Set-SPOTenantCdnEnabled -CdnType Both -Enable $true

WARNING: Enabling this feature will turn on a content delivery network (CDN) for this tenant to provide fast and reliable performance for shared assets. The CDN may have privacy and compliance standards that differ from the commitments and compliance boundaries outlined by the Microsoft Office365 Trust Center, and data cached through this service may not conform to the Microsoft Data Processing Terms (DPT). For more information on CDNs, see:https://go.microsoft.com/fwlink/?linkid=2077392

Confirm
Are you sure you want to perform this action?
Performing the operation "Enable Tenant CDN" on target "Private and Public CDN".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): Y

WARNING: Files of type GIF,ICO,JPEG,JPG,JS,PNG stored in the locations configured to serve as Private CDN origins will now also be served and cached in Content Delivery Network (CDN). Although only authenticated users are authorized to access such content, the CDN is not monitored nor governed by Microsoft content policies.

Private CDN enabled locations:
*/USERPHOTO.ASPX (configuration pending)
*/SITEASSETS (configuration pending)

WARNING: Files of type CSS,EOT,GIF,ICO,JPEG,JPG,JS,MAP,PNG,SVG,TTF,WOFF,WOFF2 stored in the locations configured to serve as Public CDN origins will now also be served and cached in Content Delivery Network (CDN). Such content will then be accessible by everyone anonymously not monitored nor governed by Microsoft content policies.

Public CDN enabled locations:
*/MASTERPAGE (configuration pending)
*/STYLE LIBRARY (configuration pending)
*/CLIENTSIDEASSETS (configuration pending)
```

See also

[Use the Page Diagnostics tool for SharePoint](#)

[Use the Office 365 Content Delivery Network \(CDN\) with SharePoint](#)

[Content Delivery Networks](#)

[Network planning and performance tuning for Office 365](#)

[SharePoint Performance Series - Office 365 CDN video series ↗](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Use the Office 365 Content Delivery Network (CDN) with SharePoint Online

Article • 01/26/2024

You can use the built-in Office 365 Content Delivery Network (CDN) to host static assets to provide better performance for your SharePoint Online pages. The Office 365 CDN improves performance by caching static assets closer to the browsers requesting them, which helps to speed up downloads and reduce latency. Also, the Office 365 CDN uses the [HTTP/2 protocol](#) for improved compression and HTTP pipelining. The Office 365 CDN service is included as part of your SharePoint Online subscription.

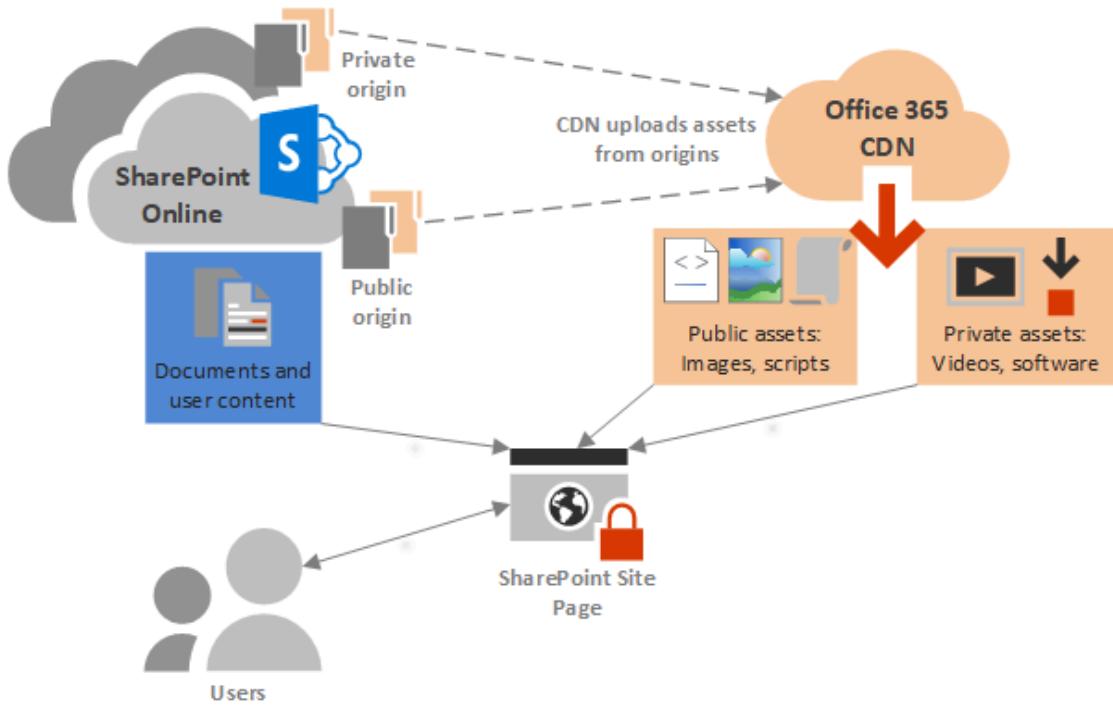
⊗ Caution

As images are now automatically managed in a SharePoint Online service-managed Private CDN, the manually configured Private CDN is in the process of being deprecated. This behavior means that customers no longer need to configure private CDN. The recommended practice remains unchanged as images are hosted via the service-managed Private CDN automatically. Public CDN continues to be available for all other file types (for example, CSS and JS). Customers using Private CDN for file types other than images, need to move those files into Public CDN. We recommend Public CDN for these file types to enhance performance.

ⓘ Note

The Office 365 CDN is only available to tenants in the **Production** (worldwide) cloud. Tenants in the US Government and China clouds do not currently support the Office 365 CDN.

The Office 365 CDN is composed of multiple CDNs that allow you to host static assets in multiple locations, or *origins*, and serve them from global high-speed networks. Depending on the kind of content you want to host in the Office 365 CDN, you can add **public** origins, **private** origins or both. See [Choose whether each origin should be public or private](#) for more information on the difference between public and private origins.



If you're already familiar with the way that CDNs work, you only need to complete a few steps to enable the Office 365 CDN for your tenant. This article describes how. Read on for information about how to get started hosting your static assets.

Tip

There are other Microsoft-hosted CDNs that can be used with Office 365 for specialized usage scenarios, but are not discussed in this topic because they fall outside the scope of the Office 365 CDN. For more information, see [Other Microsoft CDNs](#).

Head back to [Network planning and performance tuning for Office 365](#).

Overview of working with the Office 365 CDN in SharePoint Online

To set up the Office 365 CDN for your organization, you follow these basic steps:

- Plan for deployment of the Office 365 CDN
 - Determine which static assets you want to host on the CDN.
 - Determine where you want to store your assets. This location can be a SharePoint site, library or folder and is called an *origin*.

- Choose whether each origin should be public or private. You can add multiple origins of both public and private types.
- Set up and configure the CDN, using either PowerShell or the CLI for Microsoft 365
 - [Set up and configure the CDN by using the SharePoint Online Management Shell](#)
 - [Set up and configure the CDN by using PnP PowerShell](#)
 - [Set up and configure the CDN by using the CLI for Microsoft 365](#)

When you complete this step, you get the following results:

- The CDN is enabled for your organization.
- You added your origins, identifying each origin as public or private.

Once you're done with setup, you can [Manage the Office 365 CDN](#) over time by:

- Adding, updating, and removing assets
- Adding and removing origins
- Configuring CDN policies
- If necessary, disabling the CDN

Finally, see [Using your CDN assets](#) to learn about accessing your CDN assets from both public and private origins.

See [Troubleshooting the Office 365 CDN](#) for guidance on resolving common issues.

Plan for deployment of the Office 365 CDN

Before you deploy the Office 365 CDN for your Office 365 tenant, you should consider the following factors as part of your planning process.

- Determine which static assets you want to host on the CDN
- Determine where you want to store your assets
- Choose whether each origin should be public or private

Determine which static assets you want to host on the CDN

In general, CDNs are most effective for hosting *static assets*, or assets that don't change often. A good rule of thumb is to identify files that meet some or all of these conditions:

- Static files embedded in a page (like scripts and images) that might have a significant effect on page load times.
- Large files like executables and installation files.

- Resource libraries that support client-side code.

For example, adding repeatedly requested small files (site images and scripts) to a CDN origin can significantly improve site rendering performance and incrementally reduce the load on your SharePoint Online sites. Larger files (installation executables) can be downloaded from the CDN, delivering a positive performance effect and subsequent reduction of the load on your SharePoint Online site, even if they aren't accessed as often.

Performance improvement on a per-file basis is dependent on many factors, including the client's proximity to the nearest CDN endpoint, transient conditions on the local network, and so forth. Many static files are small, and can be downloaded from Office 365 in less than a second. However, a web page might contain many embedded files with a cumulative download time of several seconds. Serving these files from the CDN can significantly reduce the overall page load time. See [What performance gains does a CDN provide?](#) for an example.

Determine where you want to store your assets

The CDN fetches your assets from a location called an *origin*. An origin can be a SharePoint site, document library or folder that is accessible by a URL. You have great flexibility when you specify origins for your organization. For example, you can specify multiple origins or a single origin where you want to put all your CDN assets. You can choose to have both public or private origins for your organization. Most organizations choose to implement a combination of the two.

You can create new container for your origins such as folders or document libraries, and add files you want to make available from the CDN. This is a good approach for a specific set of assets that you want to be available from the CDN, and you want to restrict the set of CDN assets to only those files in the container.

You can also configure an existing site collection, site, library or folder as an origin, which makes all eligible assets in the container available from the CDN. Before you add an existing container as an origin, it's important to make sure you're aware of its contents and permissions so you don't inadvertently expose assets to anonymous access or unauthorized users.

You can define *CDN policies* to exclude content in your origins from the CDN. CDN policies exclude assets in public or private origins by attributes such as *file type* and *site classification*, and are applied to all origins of the CdnType (private or public) you specify in the policy. For example, if you add a private origin consisting of a site that contains multiple subsites, you can define a policy to exclude sites marked as **Confidential** so

content from sites with that classification applied aren't served from the CDN. The policy applies to content from *all* private origins that you added to the CDN.

Keep in mind that the greater the number of origins, the greater the effect on the time it takes the CDN service to process requests. We recommend that you limit the number of origins as much as possible.

Choose whether each origin should be public or private

When you identify an origin, you specify whether it should be made *public* or *private*. Access to CDN assets in public origins is anonymous, and CDN content in private origins is secured by dynamically generated tokens for greater security. Regardless of which option you choose, Microsoft does all the heavy lifting for you when it comes to administration of the CDN itself. Also, you can change your mind later, after you set up the CDN and identified your origins.

Both public and private options provide similar performance gains, but each has unique attributes and advantages.

Public origins within the Office 365 CDN are accessible anonymously, and hosted assets can be accessed by anyone who has the URL to the asset. Because access to content in public origins is anonymous, you should only use them to cache nonsensitive generic content such as JavaScript files, scripts, icons and images.

Private origins within the Office 365 CDN provide private access to user content such as SharePoint Online document libraries, sites and proprietary images. Access to content in private origins is secured by dynamically generated tokens so it can only be accessed by users with permissions to the original document library or storage location. Private origins in the Office 365 CDN can only be used for SharePoint Online content, and you can only access assets in private origins through redirection from your SharePoint Online tenant.

You can read more about how CDN access to assets in a private origin works in [Using assets in private origins](#).

Attributes and advantages of hosting assets in public origins

- Assets exposed in a public origin are accessible by everyone anonymously.

 **Important**

You should never place resources that contain user information or are considered sensitive to your organization in a public origin.

- If you remove an asset from a public origin, the asset might continue to be available for up to 30 days from the cache; however, we invalidate links to the asset in the CDN within 15 minutes.
- When you host style sheets (CSS files) in a public origin, you can use relative paths and URLs within the code. This result means that you can reference the location of background images and other objects relative to the location of the asset that's calling it.
- While you can construct a public origin's URL, you should proceed with caution, use the page context property, and follow the guidance for doing so. If access to the CDN becomes unavailable, the URL doesn't automatically resolve to your organization in SharePoint Online and might result in broken links and other errors. The URL is also subject to change, so you shouldn't hard code it to the current value.
- The default file types that are included for public origins are: .css, .eot, .gif, .ico, .jpeg, .jpg, .js, .map, .png, .svg, .ttf, .woff and .woff2. You can specify additional file types.
- You can configure a policy to exclude assets based on specified site classifications. For example, you can exclude all assets that are marked as "confidential" or "restricted", even if they're an allowed file type and are located in a public origin.

Attributes and advantages of hosting assets in private origins

- Private origins can only be used for SharePoint Online assets.
- Users can only access the assets from a private origin if they have permissions to access the container. Anonymous access to these assets is prevented.
- Assets in private origins must be referred from the SharePoint Online tenant. Direct access to private CDN assets doesn't work.
- If you remove an asset from the private origin, the asset might continue to be available for up to an hour from the cache. But, links to the asset in the CDN are invalid within 15 minutes of the removal of the asset.
- The default file types that are included for private origins are .gif, .ico, .jpeg, .jpg, .js, and .png. You can specify additional file types.

- Just like with public origins, you can configure a policy to exclude assets that are identified by site classifications that you specify even if you use wildcards to include all assets within a folder or document library.

For more information about why to use the Office 365 CDN, general CDN concepts, and other Microsoft CDNs you can use with your Office 365 tenant, see [Content Delivery Networks](#).

Default CDN origins

Unless you specify otherwise, Office 365 sets up some default origins for you when you enable the Office 365 CDN. If you initially opt not to provision them, you can add these origins after you complete setup. Unless you understand the consequences of skipping the setup of default origins and have a specific reason for doing so, you should allow them to be created when you enable the CDN.

Default private CDN origins:

- */siteassets

Default public CDN origins:

- */masterpage
- */style library
- */clientsideassets

Note

clientsideassets is a default public origin that was added to the Office 365 CDN service in December 2017. This origin must be present in order for SharePoint Framework solutions in the CDN to work. If you enabled the Office 365 CDN prior to December 2017, or if you skipped setup of default origins when you enabled the CDN, you can manually add this origin. For more information, see [My client-side web part or SharePoint Framework solution isn't working](#).

Set up and configure the Office 365 CDN by using the SharePoint Online Management Shell

The procedures in this section require you to use the SharePoint Online Management Shell to connect to SharePoint Online. For instructions, see [Connect to SharePoint Online PowerShell](#).

Complete these steps to set up and configure the CDN to host your assets in SharePoint Online using the SharePoint Online Management Shell.

▼ Select to expand

Enable your organization to use the Office 365 CDN

Before you make changes to the tenant CDN settings, you should retrieve the current status of the private CDN configuration in your Office 365 tenant. Connect to your tenant using the SharePoint Online Management Shell:

PowerShell

```
Connect-SPOSERVICE -Url https://contoso-admin.sharepoint.com
```

Now use the **Get-SPOTenantCdnEnabled** cmdlet to retrieve the CDN status settings from the tenant:

PowerShell

```
Get-SPOTenantCdnEnabled -CdnType <Public | Private>
```

The status of the CDN for the specified CdnType is shown on the screen.

Use the **Set-SPOTenantCdnEnabled** cmdlet to enable your organization to use the Office 365 CDN. You can enable your organization to use public origins, private origins, or both at once. You can also configure the CDN to skip the setup of default origins when you enable it. You can always add these origins later as described in this article.

In Windows PowerShell for SharePoint Online:

PowerShell

```
Set-SPOTenantCdnEnabled -CdnType <Public | Private | Both> -Enable $true
```

For example, to enable your organization to use both public and private origins, type the following command:

PowerShell

```
Set-SPOTenantCdnEnabled -CdnType Both -Enable $true
```

To enable your organization to use both public and private origins but skip setting up the default origins, type the following command:

PowerShell

```
Set-SPTenantCdnEnabled -CdnType Both -Enable $true -NoDefaultOrigins
```

See [Default CDN origins](#) for information about the origins that are provisioned by default when you enable the Office 365 CDN, and the potential effect of skipping the setup of default origins.

To enable your organization to use public origins, type the following command:

PowerShell

```
Set-SPTenantCdnEnabled -CdnType Public -Enable $true
```

To enable your organization to use private origins, type the following command:

PowerShell

```
Set-SPTenantCdnEnabled -CdnType Private -Enable $true
```

For more information about this cmdlet, see [Set-SPTenantCdnEnabled](#).

Change the list of file types to include in the Office 365 CDN (Optional)



When you define file types by using the **Set-SPTenantCdnPolicy** cmdlet, you overwrite the currently defined list. If you want to add additional file types to the list, use the cmdlet first to find out what file types are already allowed and include them in the list along with your new ones.

Use the **Set-SPTenantCdnPolicy** cmdlet to define static file types that can be hosted by public and private origins in the CDN. By default, common asset types are allowed, for example .css, .gif, .jpg, and .js.

In Windows PowerShell for SharePoint Online:

PowerShell

```
Set-SPTenantCdnPolicy -CdnType <Public | Private> -PolicyType  
IncludeFileExtensions -PolicyValue "<Comma-separated list of file types >"
```

For example, to enable the CDN to host .css and .png files, you would enter the command:

```
PowerShell
```

```
Set-SPOTenantCdnPolicy -CdnType Private -PolicyType IncludeFileExtensions -  
PolicyValue "CSS,PNG"
```

To see what file types are currently allowed by the CDN, use the **Get-SPOTenantCdnPolicies** cmdlet:

```
PowerShell
```

```
Get-SPOTenantCdnPolicies -CdnType <Public | Private>
```

For more information about these cmdlets, see [Set-SPOTenantCdnPolicy](#) and [Get-SPOTenantCdnPolicies](#).

Change the list of site classifications you want to exclude from the Office 365 CDN (Optional)

Tip

When you exclude site classifications by using the **Set-SPOTenantCdnPolicy** cmdlet, you overwrite the currently defined list. If you want to exclude additional site classifications, use the cmdlet first to find out what classifications are already excluded and then add them along with your new ones.

Use the **Set-SPOTenantCdnPolicy** cmdlet to exclude site classifications that you don't want to make available over the CDN. By default, no site classifications are excluded.

In Windows PowerShell for SharePoint Online:

```
PowerShell
```

```
Set-SPOTenantCdnPolicy -CdnType <Public | Private> -PolicyType  
ExcludeRestrictedSiteClassifications -PolicyValue "<Comma-separated list of  
site classifications >"
```

To see what site classifications are currently restricted, use the **Get-SPOTenantCdnPolicies** cmdlet:

PowerShell

```
Get-SPOTenantCdnPolicies -CdnType <Public | Private>
```

The returned properties are *IncludeFileExtensions*, *ExcludeRestrictedSiteClassifications* and *ExcludeIfNoScriptDisabled*.

The *IncludeFileExtensions* property contains the list of file extensions that are served from the CDN.

 **Note**

The default file extensions are different between public and private.

The *ExcludeRestrictedSiteClassifications* property contains the site classifications that you want to exclude from the CDN. For example, you can exclude sites marked as **Confidential** so content from sites with that classification applied isn't served from the CDN.

The *ExcludeIfNoScriptDisabled* property excludes content from the CDN based on the site-level *NoScript* attribute settings. By default, the *NoScript* attribute is set to **Enabled** for *Modern* sites and **Disabled** for *Classic* sites. This depends on your tenant settings.

For more information about these cmdlets, see [Set-SPOTenantCdnPolicy](#) and [Get-SPOTenantCdnPolicies](#).

Add an origin for your assets

Use the **Add-SPOTenantCdnOrigin** cmdlet to define an origin. You can define multiple origins. The origin is a URL that points to a SharePoint library or folder that contains the assets that you want to be hosted by the CDN.

 **Important**

You should never place resources that contain user information or are considered sensitive to your organization in a public origin.

PowerShell

```
Add-SPOTenantCdnOrigin -CdnType <Public | Private> -OriginUrl <path>
```

The value of *path* is the relative path to the library or folder that contains the assets. You can use wildcards in addition to relative paths. Origins support wildcards prepended to the URL. This allows you to create origins that span multiple sites. For example, to include all of the assets in the masterpages folder for all of your sites as a public origin within the CDN, type the following command:

```
PowerShell
```

```
Add-SPOTenantCdnOrigin -CdnType Public -OriginUrl */masterpage
```

- The wildcard modifier */ can only be used at the beginning of the path, and matches all URL segments under the specified URL.
- The path can point to a document library, folder or site. For example, the path */site1 matches all the document libraries under the site.

You can add an origin with a specific relative path. You can't add an origin using the full path.

This example adds a private origin of the siteassets library on a specific site:

```
PowerShell
```

```
Add-SPOTenantCdnOrigin -CdnType Private -OriginUrl sites/site1/siteassets
```

This example adds a private origin of the *folder1* folder in the site collection's site assets library:

```
PowerShell
```

```
Add-SPOTenantCdnOrigin -CdnType Private -OriginUrl  
sites/test/siteassets/folder1
```

If there's a space in the path, you can either surround the path in double quotes or replace the space with the URL encoding %20. The following examples add a private origin of the *folder 1* folder in the site collection's site assets library:

```
PowerShell
```

```
Add-SPOTenantCdnOrigin -CdnType Private -OriginUrl  
sites/test/siteassets/folder%201
```

```
PowerShell
```

```
Add-SPTenantCdnOrigin -CdnType Private -OriginUrl  
"sites/test/siteassets/folder 1"
```

For more information about this command and its syntax, see [Add-SPTenantCdnOrigin](#).

 **Note**

In private origins, assets being shared from an origin must have a major version published before they can be accessed from the CDN.

After you run the command, the system synchronizes the configuration across the datacenter. This result can take up to 15 minutes.

Example: Configure a public origin for your master pages and for your style library for SharePoint Online

Normally, these origins are set up for you by default when you enable the Office 365 CDN. However, if you want to enable them manually, follow these steps.

- Use the **Add-SPTenantCdnOrigin** cmdlet to define the style library as a public origin.

PowerShell

```
Add-SPTenantCdnOrigin -CdnType Public -OriginUrl */style%20library
```

- Use the **Add-SPTenantCdnOrigin** cmdlet to define the master pages as a public origin.

PowerShell

```
Add-SPTenantCdnOrigin -CdnType Public -OriginUrl */masterpage
```

For more information about this command and its syntax, see [Add-SPTenantCdnOrigin](#).

After you run the command, the system synchronizes the configuration across the datacenter. This result can take up to 15 minutes.

Example: Configure a private origin for your site assets, site pages, and publishing images for SharePoint Online

- Use the **Add-SPOTenantCdnOrigin** cmdlet to define the site assets folder as a private origin.

```
PowerShell
```

```
Add-SPOTenantCdnOrigin -CdnType Private -OriginUrl */siteassets
```

- Use the **Add-SPOTenantCdnOrigin** cmdlet to define the site pages folder as a private origin.

```
PowerShell
```

```
Add-SPOTenantCdnOrigin -CdnType Private -OriginUrl */sitepages
```

- Use the **Add-SPOTenantCdnOrigin** cmdlet to define the publishing images folder as a private origin.

```
PowerShell
```

```
Add-SPOTenantCdnOrigin -CdnType Private -OriginUrl */publishingimages
```

For more information about this command and its syntax, see [Add-SPOTenantCdnOrigin](#).

After you run the command, the system synchronizes the configuration across the datacenter. This result can take up to 15 minutes.

Example: Configure a private origin for a site collection for SharePoint Online

Use the **Add-SPOTenantCdnOrigin** cmdlet to define a site collection as a private origin.

For example:

```
PowerShell
```

```
Add-SPOTenantCdnOrigin -CdnType Private -OriginUrl sites/site1/siteassets
```

For more information about this command and its syntax, see [Add-SPOTenantCdnOrigin](#).

After you run the command, the system synchronizes the configuration across the datacenter. You might see a *Configuration pending* message. This message is expected as the SharePoint Online tenant connects to the CDN service. This result can take up to 15 minutes.

Manage the Office 365 CDN

After you set up the CDN, you can make changes to your configuration as you update content or as your needs change, as described in this section.

Add, update, or remove assets from the Office 365 CDN

After you complete the setup steps, you can add new assets, and update or remove existing assets whenever you want. Just make your changes to the assets in the folder or SharePoint library that you identified as an origin. If you add a new asset, it's available through the CDN immediately. However, if you update the asset, it takes up to 15 minutes for the new copy to propagate and become available in the CDN.

If you need to retrieve the location of the origin, you can use the **Get-SPTenantCdnOrigins** cmdlet. For information on how to use this cmdlet, see [Get-SPTenantCdnOrigins](#).

Remove an origin from the Office 365 CDN

You can remove access to a folder or SharePoint library that you identified as an origin using the **Remove-SPTenantCdnOrigin** cmdlet.

PowerShell

```
Remove-SPTenantCdnOrigin -OriginUrl <path> -CdnType <Public | Private | Both>
```

For information on how to use this cmdlet, see [Remove-SPTenantCdnOrigin](#).

Modify an origin in the Office 365 CDN

You can't modify an origin after you create it. Instead, remove the origin and then add a new one. For more information, see [To remove an origin from the Office 365 CDN](#) and [To add an origin for your assets](#).

Disable the Office 365 CDN

Use the **Set-SPOTenantCdnEnabled** cmdlet to disable the CDN for your organization. If you have both the public and private origins enabled for the CDN, you need to run the cmdlet twice as shown in the following examples.

To disable use of public origins in the CDN, enter the following command:

PowerShell

```
Set-SPOTenantCdnEnabled -CdnType Public -Enable $false
```

To disable use of the private origins in the CDN, enter the following command:

PowerShell

```
Set-SPOTenantCdnEnabled -CdnType Private -Enable $false
```

For more information about this cmdlet, see [Set-SPOTenantCdnEnabled](#).

Set up and configure the Office 365 CDN by using PnP PowerShell

The procedures in this section require you to use PnP PowerShell to connect to SharePoint Online. For instructions, see [Getting started with PnP PowerShell](#).

Complete these steps to set up and configure the CDN to host your assets in SharePoint Online using PnP PowerShell.

▼ Select to expand

Enable your organization to use the Office 365 CDN

Before you make changes to the tenant CDN settings, you should retrieve the current status of the private CDN configuration in your Office 365 tenant. Connect to your tenant using PnP PowerShell:

PowerShell

```
Connect-PnPOnline -Url https://contoso-admin.sharepoint.com -UseWebLogin
```

Now use the **Get-PnPTenantCdnEnabled** cmdlet to retrieve the CDN status settings from the tenant:

PowerShell

```
Get-PnPTenantCdnEnabled -CdnType <Public | Private>
```

The status of the CDN for the specified CdnType is shown on the screen.

Use the **Set-PnPTenantCdnEnabled** cmdlet to enable your organization to use the Office 365 CDN. You can enable your organization to use public origins, private origins, or both at the same time. You can also configure the CDN to skip the setup of default origins when you enable it. You can always add these origins later as described in this article.

In PnP PowerShell:

```
PowerShell
```

```
Set-PnPTenantCdnEnabled -CdnType <Public | Private | Both> -Enable $true
```

For example, to enable your organization to use both public and private origins, type the following command:

```
PowerShell
```

```
Set-PnPTenantCdnEnabled -CdnType Both -Enable $true
```

To enable your organization to use both public and private origins but skip setting up the default origins, type the following command:

```
PowerShell
```

```
Set-PnPTenantCdnEnabled -CdnType Both -Enable $true -NoDefaultOrigins
```

See [Default CDN origins](#) for information about the origins that are provisioned by default when you enable the Office 365 CDN, and the potential effect of skipping the setup of default origins.

To enable your organization to use public origins, type the following command:

```
PowerShell
```

```
Set-PnPTenantCdnEnabled -CdnType Public -Enable $true
```

To enable your organization to use private origins, type the following command:

```
PowerShell
```

```
Set-PnPTenantCdnEnabled -CdnType Private -Enable $true
```

For more information about this cmdlet, see [Set-PnPTenantCdnEnabled](#).

Change the list of file types to include in the Office 365 CDN (Optional)

Tip

When you define file types by using the **Set-PnPTenantCdnPolicy** cmdlet, you overwrite the currently defined list. If you want to add additional file types to the list, use the cmdlet first to find out what file types are already allowed and include them in the list along with your new ones.

Use the **Set-PnPTenantCdnPolicy** cmdlet to define static file types that can be hosted by public and private origins in the CDN. By default, common asset types are allowed, for example .css, .gif, jpg, and .js.

In PnP PowerShell:

PowerShell

```
Set-PnPTenantCdnPolicy -CdnType <Public | Private> -PolicyType  
IncludeFileExtensions -PolicyValue "<Comma-separated list of file types >"
```

For example, to enable the CDN to host .css and .png files, you would enter the command:

PowerShell

```
Set-PnPTenantCdnPolicy -CdnType Private -PolicyType IncludeFileExtensions -  
PolicyValue "CSS,PNG"
```

To see what file types are currently allowed by the CDN, use the **Get-PnPTenantCdnPolicies** cmdlet:

PowerShell

```
Get-PnPTenantCdnPolicies -CdnType <Public | Private>
```

For more information about these cmdlets, see [Set-PnPTenantCdnPolicy](#) and [Get-PnPTenantCdnPolicies](#).

Change the list of site classifications you want to exclude from the Office 365 CDN (Optional)

💡 Tip

When you exclude site classifications by using the `Set-PnPTenantCdnPolicy` cmdlet, you overwrite the currently defined list. If you want to exclude additional site classifications, use the cmdlet first to find out what classifications are already excluded and then add them along with your new ones.

Use the `Set-PnPTenantCdnPolicy` cmdlet to exclude site classifications that you don't want to make available over the CDN. By default, no site classifications are excluded.

In PnP PowerShell:

PowerShell

```
Set-PnPTenantCdnPolicy -CdnType <Public | Private> -PolicyType  
ExcludeRestrictedSiteClassifications -PolicyValue "<Comma-separated list of  
site classifications>"
```

To see what site classifications are currently restricted, use the `Get-PnPTenantCdnPolicies` cmdlet:

PowerShell

```
Get-PnPTenantCdnPolicies -CdnType <Public | Private>
```

The returned properties are `IncludeFileExtensions`, `ExcludeRestrictedSiteClassifications` and `ExcludeIfNoScriptDisabled`.

The `IncludeFileExtensions` property contains the list of file extensions that are served from the CDN.

ⓘ Note

The default file extensions are different between public and private.

The `ExcludeRestrictedSiteClassifications` property contains the site classifications that you want to exclude from the CDN. For example, you can exclude sites marked as **Confidential** so content from sites with that classification applied won't be served from the CDN.

The `ExcludeIfNoScriptDisabled` property excludes content from the CDN based on the site-level `NoScript` attribute settings. By default, the `NoScript` attribute is set to **Enabled** for *Modern* sites and **Disabled** for *Classic* sites. This depends on your tenant settings.

For more information about these cmdlets, see [Set-PnPTenantCdnPolicy](#) and [Get-PnPTenantCdnPolicies](#).

Add an origin for your assets

Use the **Add-PnPTenantCdnOrigin** cmdlet to define an origin. You can define multiple origins. The origin is a URL that points to a SharePoint library or folder that contains the assets that you want to be hosted by the CDN.

ⓘ Important

You should never place resources that contain user information or are considered sensitive to your organization in a public origin.

PowerShell

```
Add-PnPTenantCdnOrigin -CdnType <Public | Private> -OriginUrl <path>
```

The value of *path* is the relative path to the library or folder that contains the assets. You can use wildcards in addition to relative paths. Origins support wildcards prepended to the URL. This allows you to create origins that span multiple sites. For example, to include all of the assets in the masterpages folder for all of your sites as a public origin within the CDN, type the following command:

PowerShell

```
Add-PnPTenantCdnOrigin -CdnType Public -OriginUrl */masterpage
```

- The wildcard modifier `*/` can only be used at the beginning of the path, and matches all URL segments under the specified URL.
- The path can point to a document library, folder or site. For example, the path `*/site1` matches all the document libraries under the site.

You can add an origin with a specific relative path. You can't add an origin using the full path.

This example adds a private origin of the site assets library on a specific site:

PowerShell

```
Add-PnPNTenantCdnOrigin -CdnType Private -OriginUrl sites/site1/siteassets
```

This example adds a private origin of the *folder1* folder in the site collection's site assets library:

PowerShell

```
Add-PnPNTenantCdnOrigin -CdnType Private -OriginUrl  
sites/test/siteassets/folder1
```

If there's a space in the path, you can either surround the path in double quotes or replace the space with the URL encoding %20. The following examples add a private origin of the *folder 1* folder in the site collection's site assets library:

PowerShell

```
Add-PnPNTenantCdnOrigin -CdnType Private -OriginUrl  
sites/test/siteassets/folder%201
```

PowerShell

```
Add-PnPNTenantCdnOrigin -CdnType Private -OriginUrl  
"sites/test/siteassets/folder 1"
```

For more information about this command and its syntax, see [Add-PnPNTenantCdnOrigin](#).

Note

In private origins, assets shared from an origin must have a major version published before they're accessible from the CDN.

After you run the command, the system synchronizes the configuration across the datacenter. This result can take up to 15 minutes.

Example: Configure a public origin for your master pages and for your style library for SharePoint Online

Normally, these origins are set up for you by default when you enable the Office 365 CDN. However, if you want to enable them manually, follow these steps.

- Use the **Add-PnPTenantCdnOrigin** cmdlet to define the style library as a public origin.

PowerShell

```
Add-PnPTenantCdnOrigin -CdnType Public -OriginUrl */style%20library
```

- Use the **Add-PnPTenantCdnOrigin** cmdlet to define the master pages as a public origin.

PowerShell

```
Add-PnPTenantCdnOrigin -CdnType Public -OriginUrl */masterpage
```

For more information about this command and its syntax, see [Add-PnPTenantCdnOrigin](#).

After you run the command, the system synchronizes the configuration across the datacenter. This result can take up to 15 minutes.

Example: Configure a private origin for your site assets, site pages, and publishing images for SharePoint Online

- Use the **Add-PnPTenantCdnOrigin** cmdlet to define the site assets folder as a private origin.

PowerShell

```
Add-PnPTenantCdnOrigin -CdnType Private -OriginUrl */siteassets
```

- Use the **Add-PnPTenantCdnOrigin** cmdlet to define the site pages folder as a private origin.

PowerShell

```
Add-PnPTenantCdnOrigin -CdnType Private -OriginUrl */sitepages
```

- Use the **Add-PnPTenantCdnOrigin** cmdlet to define the publishing images folder as a private origin.

```
PowerShell
```

```
Add-PnPTenantCdnOrigin -CdnType Private -OriginUrl */publishingimages
```

For more information about this command and its syntax, see [Add-PnPTenantCdnOrigin](#).

After you run the command, the system synchronizes the configuration across the datacenter. This result can take up to 15 minutes.

Example: Configure a private origin for a site collection for SharePoint Online

Use the **Add-PnPTenantCdnOrigin** cmdlet to define a site collection as a private origin. For example:

```
PowerShell
```

```
Add-PnPTenantCdnOrigin -CdnType Private -OriginUrl sites/site1/siteassets
```

For more information about this command and its syntax, see [Add-PnPTenantCdnOrigin](#).

After you run the command, the system synchronizes the configuration across the datacenter. You might see a *Configuration pending* message. This result is expected as the SharePoint Online tenant connects to the CDN service. This result can take up to 15 minutes.

Manage the Office 365 CDN

After you set up the CDN, you can make changes to your configuration as you update content or as your needs change, as described in this section.

Add, update, or remove assets from the Office 365 CDN

After you complete the setup steps, you can add new assets, and update or remove existing assets whenever you want. Just make your changes to the assets in the folder or SharePoint library that you identified as an origin. If you add a new asset, it's available

through the CDN immediately. However, if you update the asset, it takes up to 15 minutes for the new copy to propagate and become available in the CDN.

If you need to retrieve the location of the origin, you can use the **Get-PnPTenantCdnOrigin** cmdlet. For information on how to use this cmdlet, see [Get-PnPTenantCdnOrigin](#).

Remove an origin from the Office 365 CDN

You can remove access to a folder or SharePoint library that you identified as an origin. To take this action, use the **Remove-PnPTenantCdnOrigin** cmdlet.

PowerShell

```
Remove-PnPTenantCdnOrigin -OriginUrl <path> -CdnType <Public | Private | Both>
```

For information on how to use this cmdlet, see [Remove-PnPTenantCdnOrigin](#).

Modify an origin in the Office 365 CDN

You can't modify an origin after you create it. Instead, remove the origin and then add a new one. For more information, see [To remove an origin from the Office 365 CDN](#) and [To add an origin for your assets](#).

Disable the Office 365 CDN

Use the **Set-PnPTenantCdnEnabled** cmdlet to disable the CDN for your organization. If you have both the public and private origins enabled for the CDN, you need to run the cmdlet twice as shown in the following examples.

To disable use of public origins in the CDN, enter the following command:

PowerShell

```
Set-PnPTenantCdnEnabled -CdnType Public -Enable $false
```

To disable use of the private origins in the CDN, enter the following command:

PowerShell

```
Set-PnPTenantCdnEnabled -CdnType Private -Enable $false
```

For more information about this cmdlet, see [Set-PnPNTenantCdnEnabled](#).

Set up and configure the Office 365 CDN using the CLI for Microsoft 365

The procedures in this section require the [CLI for Microsoft 365](#). The, connect to your Office 365 tenant using the [login](#) command.

Complete these steps to set up and configure the CDN to host your assets in SharePoint Online using the CLI for Microsoft 365.

▼ Select to expand

Enable the Office 365 CDN

You can manage the state of the Office 365 CDN in your tenant using the [spo cdn set](#) command.

To enable the Office 365 Public CDN in your tenant, run the following command:

```
cli  
m365 spo cdn set --type Public --enabled true
```

To enable the Office 365 SharePoint CDN, run the following command:

```
cli  
m365 spo cdn set --type Private --enabled true
```

View the current status of the Office 365 CDN

To check if the particular type of Office 365 CDN is enabled or disabled, use the [spo cdn get](#) command.

To check if the Office 365 Public CDN is enabled, run the following command:

```
cli  
m365 spo cdn get --type Public
```

View the Office 365 CDN origins

To view the currently configured Office 365 Public CDN origins, run the following command:

```
cli
```

```
m365 spo cdn origin list --type Public
```

See [Default CDN origins](#) for information about the origins that are provisioned by default when you enable the Office 365 CDN.

Add an Office 365 CDN origin

 **Important**

You should never place resources that are considered sensitive to your organization in a SharePoint document library configured as a public origin.

Use the [spo cdn origin add](#) command to define a CDN origin. You can define multiple origins. The origin is a URL that points to a SharePoint library or folder that contains the assets that you want the CDN to host.

```
cli
```

```
m365 spo cdn origin add --type [Public | Private] --origin <path>
```

Where `path` is the relative path to the folder that contains the assets. You can use wildcards in addition to relative paths.

To include all assets in the **Master Page Gallery** of all sites as a public origin, run the following command:

```
cli
```

```
m365 spo cdn origin add --type Public --origin */masterpage
```

To configure a private origin for a specific site collection, run the following command:

```
cli
```

```
m365 spo cdn origin add --type Private --origin sites/site1/siteassets
```

Note

After adding a CDN origin, it might take up to 15 minutes for you to be able to retrieve files via the CDN service. You can verify if the particular origin has already been enabled using the [spo cdn origin list](#) command.

Remove an Office 365 CDN origin

Use the [spo cdn origin remove](#) command to remove a CDN origin for the specified CDN type.

To remove a public origin from the CDN configuration, run the following command:

```
cli
```

```
m365 spo cdn origin remove --type Public --origin */masterpage
```

Note

Removing a CDN origin doesn't effect the files stored in any document library that matches the origin. If these assets are referenced using their SharePoint URL, SharePoint automatically switches back to the original URL pointing to the document library. If the assets are referenced using a public CDN URL, removing the origin breaks the link, and you need to manually change them.

Modify an Office 365 CDN origin

It's not possible to modify an existing CDN origin. Instead, you should remove the previously defined CDN origin using the `spo cdn origin remove` command and add a new one using the `spo cdn origin add` command.

Change the types of files to include in the Office 365 CDN

By default, the following file types are included in the CDN: `.css`, `.eot`, `.gif`, `.ico`, `.jpeg`, `.jpg`, `.js`, `.map`, `.png`, `.svg`, `.ttf`, `.woff`, and `.woff2`. If you need to include additional file types in the CDN, you can change the CDN configuration using the [spo cdn policy set](#) command.

Note

When changing the list of file types, you overwrite the currently defined list. If you want to include additional file types, first use the [spo cdn policy list](#) command to find out which file types are currently configured.

To add the *JSON* file type to the default list of file types included in the public CDN, run the following command:

cli

```
m365 spo cdn policy set --type Public --policy IncludeFileExtensions --value "CSS,EOT,GIF,ICO,JPEG,JPG,JS,MAP,PNG,SVG,TTF,WOFF,JSON"
```

Change the list of site classifications you want to exclude from the Office 365 CDN

Use the [spo cdn policy set](#) command to exclude site classifications that you don't want to make available over the CDN. By default, no site classifications are excluded.

Note

When changing the list of excluded site classifications, you overwrite the currently defined list. If you want to exclude additional classifications, first use the [spo cdn policy list](#) command to find out which classifications are currently configured.

To exclude sites classified as *HBI* from the public CDN, run the following command:

cli

```
m365 spo cdn policy set --type Public --policy ExcludeRestrictedSiteClassifications --value "HBI"
```

Disable the Office 365 CDN

To disable the Office 365 CDN use the `spo cdn set` command, for example:

cli

```
m365 spo cdn set --type Public --enabled false
```

Using your CDN assets

Now that you enabled the CDN and configured origins and policies, you can begin using your CDN assets.

This section helps you understand how to use CDN URLs in your SharePoint pages and content so that SharePoint redirects requests for assets in both public and private origins to the CDN.

- [Updating links to CDN assets](#)
- [Using assets in public origins](#)
- [Using assets in private origins](#)

For information on how to use the CDN for hosting client-side web parts, see the article [Host your client-side web part from Office 365 CDN \(Hello World part 4\)](#).

ⓘ Note

If you add the *ClientSideAssets* folder to the **private** CDN origins list, CDN-hosted custom web parts will fail to render. Files used by SPFX web parts can only utilize the public CDN and the ClientSideAssets folder is a default origin for public CDN.

Updating links to CDN assets

To use assets that you added to an origin, you simply update links to the original file with the path to the file in the origin.

- Edit the page or content that contains links to assets you added to an origin. You can also use one of several methods to globally search and replace links across an entire site or site collection if you want to update the link to a given asset everywhere it appears.
- For each link to an asset in an origin, replace the path with the path to the file in the CDN origin. You can use relative paths.
- Save the page or content.

For example, consider the image `/site/SiteAssets/images/image.png`, which you copied to the document library folder `/site/CDN_origins/public/`. To use the CDN asset, replace the original path to the image file location with the path to the origin to make the new URL `/site/CDN_origins/public/image.png`.

If you want to use the full URL to the asset instead of a relative path, construct the link like so:

https://<TenantHostName>.sharepoint.com/sites/site/CDN_origins/public/image.png

Note

In general, you should not hardcode URLs directly to assets in the CDN. However, you can manually construct URLs for assets in public origins if needed. For more information, see [Hardcoding CDN URLs for public assets](#).

To learn about how to verify that assets are being served from the CDN, see [How do I confirm that assets are being served by the CDN?](#) in [Troubleshooting the Office 365 CDN](#).

Using assets in public origins

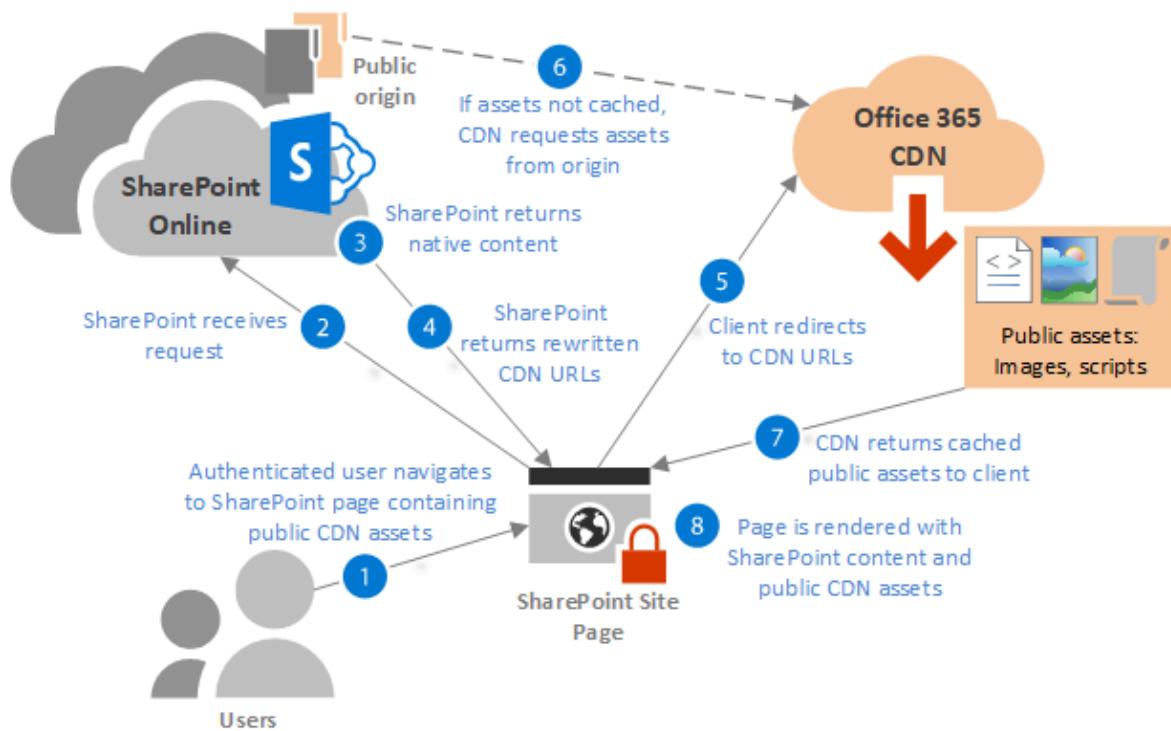
The **Publishing feature** in SharePoint Online automatically rewrites URLs of assets stored in public origins to their CDN equivalents so that assets are served from the CDN service instead of SharePoint.

If your origin is in a site with the Publishing feature enabled, and the assets you want to offload to the CDN are in one of the following categories, SharePoint automatically rewrites URLs for assets in the origin, if the asset hasn't been excluded by a CDN policy.

The following example is an overview where links are automatically rewritten by the SharePoint Publishing feature:

- IMG/LINK/CSS URLs in classic publishing page HTML responses.
 - This includes images added by authors within the HTML content of a page.
- Picture Library SlideShow webpart image URLs.
- Image fields in SPList REST API (RenderListDataAsStream) results.
 - Use the new property *ImageFieldsToTryRewriteToCdnUrls* to provide a comma separated list of fields.
 - Supports hyperlink fields and PublishingImage fields.
- SharePoint image renditions.

The following diagram illustrates the workflow when SharePoint receives a request for a page containing assets from a public origin.



Tip

If you want to disable auto-rewriting for specific URLs on a page, you can check out the page and add the query string parameter `?NoAutoReWrites=true` to the end of each link you want to disable.

Constructing CDN URLs for public assets

If the *Publishing* feature isn't enabled for a public origin, or the asset isn't one of the link types supported by the auto-rewrite feature of the CDN service, you can manually construct URLs to the CDN location of the assets and use these URLs in your content.

Note

You cannot hardcode or construct CDN URLs to assets in a private origin because the required access token that forms the last section of the URL is generated at the time the resource is requested. You can construct the URL for Public CDN and the URL should not be hard coded as it's subject to change.

For public CDN assets, the URL format looks like the following example:

HTTP

<https://publiccdn.sharepointonline.com/<TenantHostName>/sites/site/library/asset.png>

Replace **TenantHostName** with your tenant name. For example:

HTTP

<https://publiccdn.sharepointonline.com/contoso.sharepoint.com/sites/site/library/asset.png>

ⓘ Note

Use the page context property to construct the prefix instead of hard coding `https://publiccdn.sharepointonline.com`, because the URL is subject to change. If you use display templates with Classic SharePoint Online, you can use the property `window._spPageContextInfo.publicCdnBaseUrl` in your display template for the prefix of the URL. If you use SPFx web parts for modern and classic SharePoint, you can use the property `this.context.pageContext.legacyPageContext.publicCdnBaseUrl`, which also provides the prefix. If the prefix changes, your implementation is updated with it.

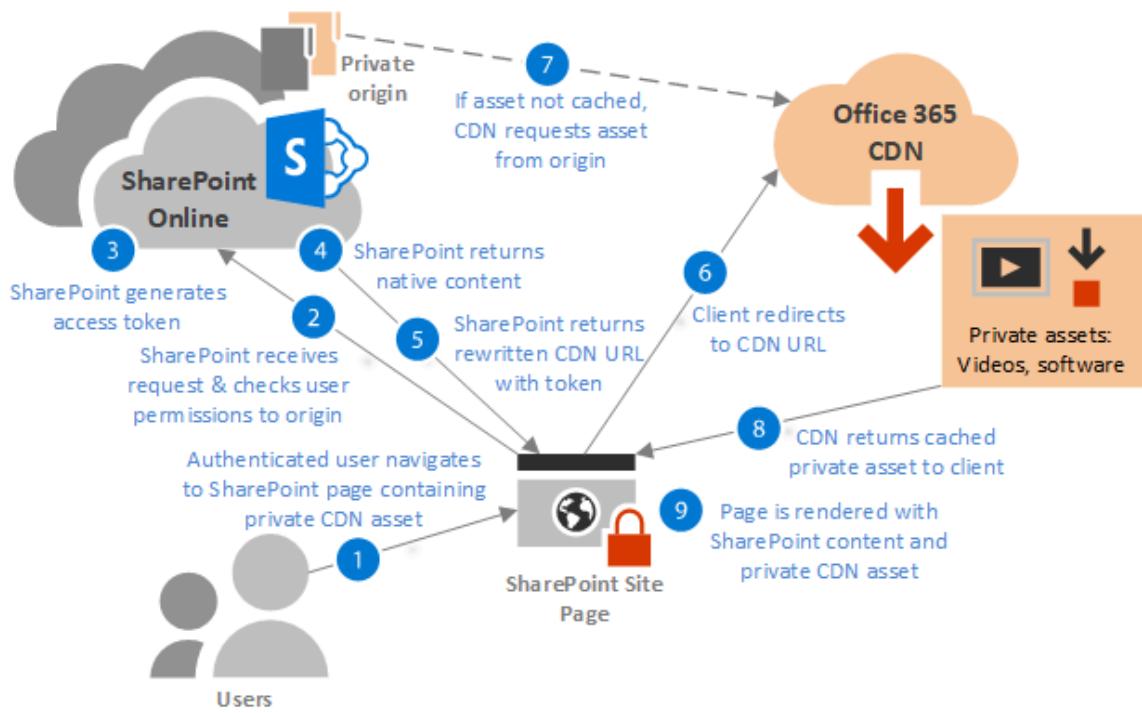
As an example for SPFx, you can construct the URL using the property `this.context.pageContext.legacyPageContext.publicCdnBaseUrl - / - host - / - relativeURL` for the item. For more information, see the video [Using CDN in Client-side code](#), which is part of the [season 1 performance series](#).

Using assets in private origins

No additional configuration is required to use assets in private origins. SharePoint Online automatically rewrites URLs for assets in private origins so requests for those assets are always served from the CDN. You can't manually build URLs to CDN assets in private origins because these URLs contain tokens that must be auto-generated by SharePoint Online at the time the asset is requested.

Access to assets in private origins is protected by dynamically generated tokens based on user permissions to the origin, with the caveats described in the following sections. Users must have at least **read** access to the origins for the CDN to render content.

The following diagram illustrates the workflow when SharePoint receives a request for a page containing assets from a private origin.



Token-based authorization in private origins

Access to assets in private origins in the Office 365 CDN is granted by tokens generated by SharePoint Online. Users who already have permission to access to the folder or library designated by the origin are automatically granted tokens that permit the user to access the file based on their permission level. These access tokens are valid for 30 to 90 minutes after they're generated to help prevent token replay attacks.

Once the access token is generated, SharePoint Online returns a custom URI to the client containing two authorization parameters *eat* (edge authorization token) and *oat* (origin authorization token). The structure of each token is <'expiration time in Epoch time format'>_<'secure signature'>. For example:

```
HTTP

https://privatecdn.sharepointonline.com/contoso.sharepoint.com/sites/site1/1
library1/folder1/image1.jpg?
eat=1486154359_cc59042c5c55c90b26a2775323c7c8112718431228fe84d568a3795a63912
840&oat=1486154359_7d73c2e3ba4b7b1f97242332900616db0d4ffb04312
```

ⓘ Note

Anyone in possession of the token can access the resource in the CDN. However, URLs containing these access tokens are only shared over HTTPS, so unless the URL

is explicitly shared by an end user before the token expires, the asset won't be accessible to unauthorized users.

Item-level permissions aren't supported for assets in private origins

It's important to note that SharePoint Online doesn't support item-level permissions for assets in private origins. For example, for a file located at

<https://contoso.sharepoint.com/sites/site1/library1/folder1/image1.jpg>, users have effective access to the file given the following conditions:

[] Expand table

User	Permissions	Effective access
User 1	Has access to folder1	Can access image1.jpg from the CDN
User 2	Doesn't have access to folder1	Can't access image1.jpg from the CDN
User 3	Doesn't have access to folder1, but is granted explicit permission to access image1.jpg in SharePoint Online	Can access the asset image1.jpg directly from SharePoint Online, but not from the CDN
User 4	Has access to folder1, but has been explicitly denied access to image1.jpg in SharePoint Online	Can't access the asset from SharePoint Online, but can access the asset from the CDN despite being denied access to the file in SharePoint Online

Troubleshooting the Office 365 CDN

How do I confirm that assets are being served by the CDN?

After you add links to CDN assets to a page, you can confirm that the asset is being served from the CDN by browsing to the page, right clicking on the image once it has rendered and reviewing the image URL.

You can also use your browser's developer tools to view the URL for each asset on a page, or use a third party network trace tool.

! Note

If you use a network tool such as Fiddler to test your assets outside of rendering the asset from a SharePoint page, you must manually add the referer header "Referer: <https://yourdomain.sharepoint.com>" to the GET request where the URL is the root URL of your SharePoint Online tenant.

You can't test CDN URLs directly in a web browser because you must have a referrer coming from SharePoint Online. However, if you add the CDN asset URL to a SharePoint page and then open the page in a browser, the CDN asset is rendered on the page.

For more information on using the developer tools in the Microsoft Edge browser, see [Microsoft Edge Developer Tools](#).

To watch a short video hosted in the [SharePoint Developer Patterns and Practices YouTube channel](#) that shows how to verify your CDN is working, see [Verifying your CDN usage and ensuring optimal network connectivity](#).

Why are assets from a new origin unavailable?

Assets in new origins won't immediately be available for use, as it takes time for the registration to propagate through the CDN and for the assets to be uploaded from the origin to CDN storage. The time required for assets to be available in the CDN depends on how many assets and the file sizes.

My client-side web part or SharePoint Framework solution isn't working

When you enable the Office 365 CDN for public origins, the CDN service automatically creates these default origins:

- */MASTERPAGE
- */STYLE LIBRARY
- */CLIENTSIDEASSETS

If the */clientsideassets origin is missing, SharePoint Framework solutions fail, and no warning or error messages are generated. This origin might be missing either because the CDN was enabled with the `-NoDefaultOrigins` parameter set to `$true`, or because the origin was manually deleted.

You can check to see which origins are present with the following PowerShell command:

```
PowerShell
```

```
Get-SPOTenantCdnOrigins -CdnType Public
```

Or you can check with the CLI for Microsoft 365:

```
cli
```

```
m365 spocdn origin list
```

To add the origin in PowerShell:

```
PowerShell
```

```
Add-SPOTenantCdnOrigin -CdnType Public -OriginUrl */CLIENTSIDEASSETS
```

To add the origin using the CLI for Microsoft 365:

```
cli
```

```
m365 spo cdn origin add --origin */CLIENTSIDEASSETS
```

What PowerShell modules and CLI shells do I need to work with the Office 365 CDN?

You can choose to work with the Office 365 CDN using either the **SharePoint Online Management Shell** PowerShell module or the **CLI for Microsoft 365**.

- [Getting started with SharePoint Online Management Shell](#)
- [Installing the CLI for Microsoft 365 ↗](#)

See also

[Content Delivery Networks](#)

[Network planning and performance tuning for Office 365](#)

[SharePoint Performance Series - Office 365 CDN video series ↗](#)

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Overview: VPN split tunneling for Microsoft 365

Article • 12/20/2023

ⓘ Note

This article is part of a set of articles that address Microsoft 365 optimization for remote users.

- For detailed guidance on implementing VPN split tunneling, see [Implementing VPN split tunneling for Microsoft 365](#).
- For a detailed list of VPN split tunneling scenarios, see [Common VPN split tunneling scenarios for Microsoft 365](#).
- For guidance on securing Teams media traffic in VPN split tunneling environments, see [Securing Teams media traffic for VPN split tunneling](#).
- For information about how to configure Stream and live events in VPN environments, see [Special considerations for Stream and live events in VPN environments](#).
- For information about optimizing Microsoft 365 worldwide tenant performance for users in China, see [Microsoft 365 performance optimization for China users](#).

Enterprises have traditionally used VPNs to support secure remote experiences for their users. While core workloads remained on-premises, a VPN from the remote client routed through a datacenter on the corporate network was the primary method for remote users to access corporate resources. To safeguard these connections, enterprises build layers of network security solutions along the VPN paths. This security was built to protect internal infrastructure and to safeguard mobile browsing of external web sites by rerouting traffic into the VPN and then out through the on-premises Internet perimeter. VPNs, network perimeters, and associated security infrastructure were often purpose-built and scaled for a defined volume of traffic, typically with most connectivity being initiated from within the corporate network, and most of it staying within the internal network boundaries.

For quite some time, VPN models where all connections from the remote user device are routed back into the on-premises network (known as *forced tunneling*) were largely sustainable as long as the concurrent scale of remote users was modest and the traffic

volumes traversing VPN were low. Some customers continued to use VPN force tunneling as the status quo even after their applications moved from inside the corporate perimeter to public SaaS clouds.

The use of forced tunneled VPNs for connecting to distributed and performance-sensitive cloud applications is suboptimal, but the negative effects have been accepted by some enterprises so as to maintain the security status quo. An example diagram of this scenario can be seen here:

Traditional enterprise connectivity and Internet access

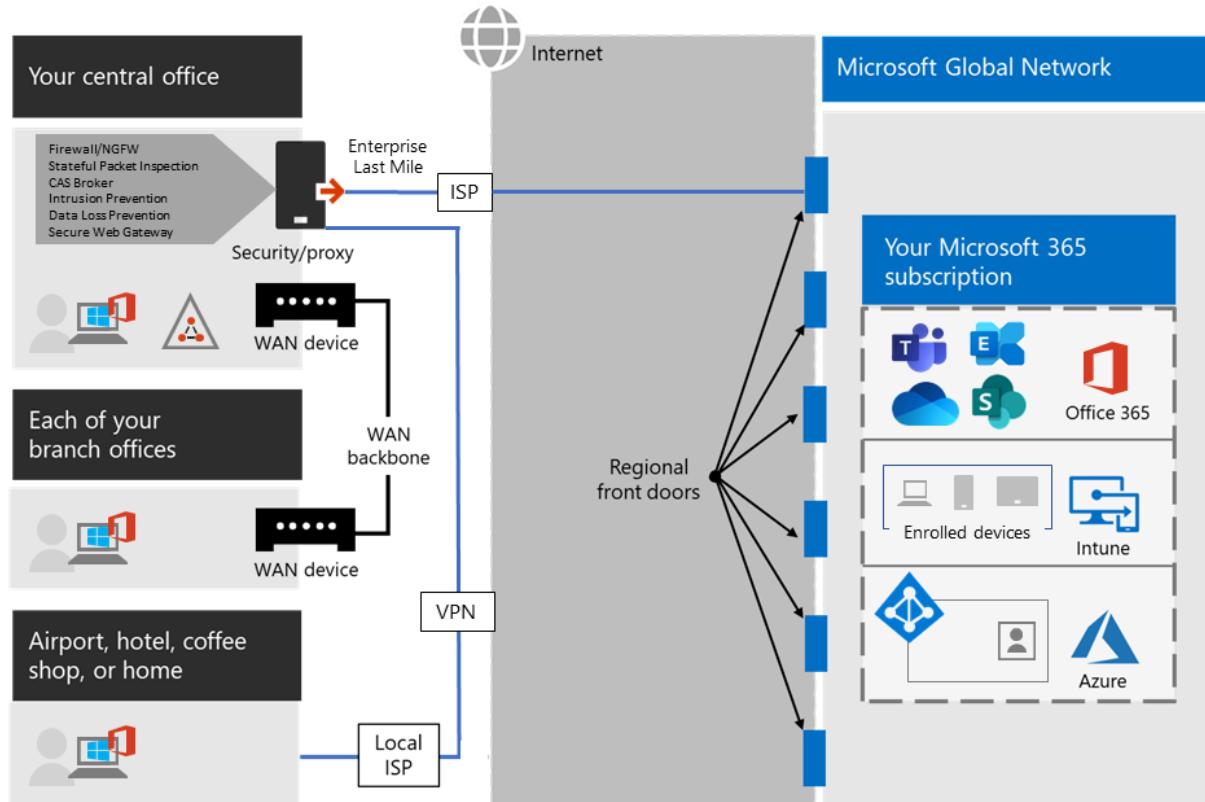


Figure 1: A traditional Forced Tunnel VPN solution.

This problem has been growing for many years, with many customers reporting a significant shift of network traffic patterns. Traffic that used to stay on premises now connects to external cloud endpoints. Many Microsoft customers report that previously, around 80% of their network traffic was to some internal source (represented by the dotted line in the preceding diagram). In 2020 that number decreased to around 20% or lower as they have shifted major workloads to the cloud. These trends aren't uncommon with other enterprises. Over time, as the cloud journey progresses, the above model becomes increasingly cumbersome and unsustainable, preventing an organization from being agile as they move into a cloud-first world.

The worldwide COVID-19 crisis escalated this problem to require immediate remediation. The need to ensure employee safety generated unprecedented demands on enterprise IT to support work-from-home productivity at a massive scale, which is

still true in the post-crisis era. Microsoft 365 is well positioned to help customers fulfill that demand, but high concurrency of users working from home generates a large volume of Microsoft 365 traffic which, if routed through forced tunnel VPN and on-premises network perimeters, causes rapid saturation and runs VPN infrastructure out of capacity. In this post-crisis reality, using VPN to access Microsoft 365 is no longer just a performance impediment, but a hard wall that not only impacts Microsoft 365 but critical business operations that still have to rely on the VPN to operate.

Microsoft has been working closely with customers and the wider industry to provide effective, modern solutions to these problems from within our own services, and to align with industry best practice. [Connectivity principles](#) for the Microsoft 365 service have been designed to work efficiently for remote users while still allowing an organization to maintain security and control over their connectivity. These solutions can also be implemented quickly with limited work yet achieve a significant positive effect on the problems outlined above.

For customers who connect their remote worker devices to the corporate network or cloud infrastructure over VPN, Microsoft recommends that the key Microsoft 365 scenarios **Microsoft Teams**, **SharePoint**, and **Exchange Online** are routed over a *VPN split tunnel* configuration. This becomes especially important as the frontline strategy to facilitate continued employee productivity during large-scale work-from-home events such as the COVID-19 crisis.

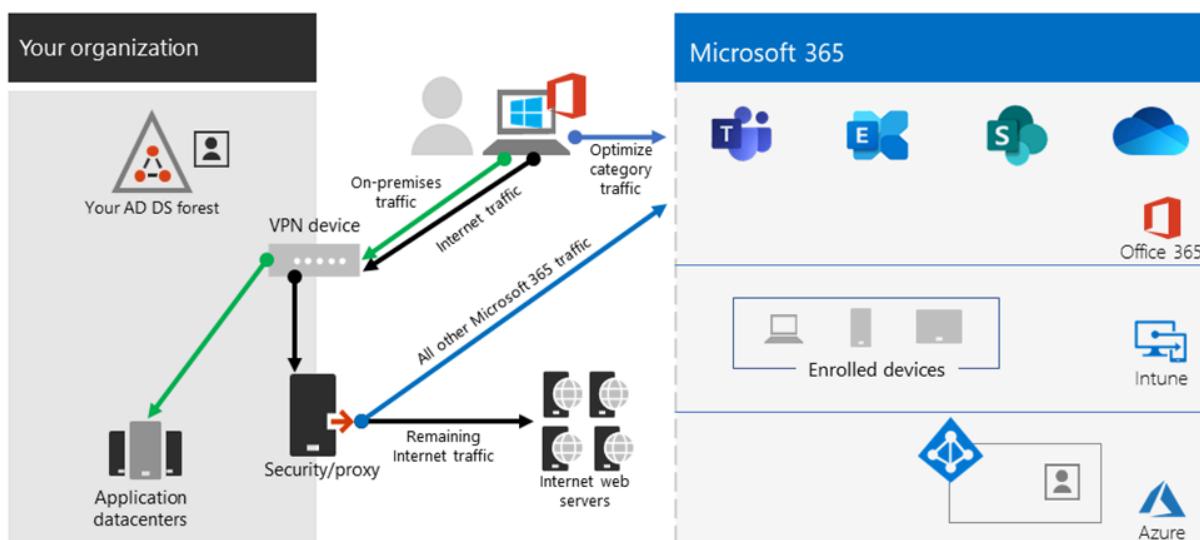


Figure 2: A VPN split tunnel solution with defined Microsoft 365 exceptions sent directly to the service. All other traffic traverses the VPN tunnel regardless of destination.

The essence of this approach is to provide a method for enterprises to mitigate the risk of VPN infrastructure saturation and dramatically improve Microsoft 365 performance in the shortest timeframe possible. Configuring VPN clients to allow the most critical, high volume Microsoft 365 traffic to bypass the VPN tunnel achieves the following benefits:

- Immediately mitigates the root cause of a majority of customer-reported performance and network capacity issues in enterprise VPN architectures impacting Microsoft 365 user experience

The recommended solution specifically targets Microsoft 365 service endpoints categorized as **Optimize** in the article [Microsoft 365 URLs and IP address ranges](#). Traffic to these endpoints is highly sensitive to latency and bandwidth throttling, and enabling it to bypass the VPN tunnel can dramatically improve the end-user experience as well as reduce the corporate network load. Microsoft 365 connections that don't constitute the majority of bandwidth or user experience footprint can continue to be routed through the VPN tunnel along with the rest of the Internet-bound traffic. For more information, see [The VPN split tunnel strategy](#).

- Can be configured, tested, and implemented rapidly by customers and with no additional infrastructure or application requirements

Depending on the VPN platform and network architecture, implementation can take as little as a few hours. For more information, see [Implement VPN split tunneling](#).

- Preserves the security posture of customer VPN implementations by not changing how other connections are routed, including traffic to the Internet

The recommended configuration follows the **least privilege** principle for VPN traffic exceptions and allows customers to implement split tunnel VPN without exposing users or infrastructure to additional security risks. Network traffic routed directly to Microsoft 365 endpoints is encrypted, validated for integrity by Office client application stacks and scoped to IP addresses dedicated to Microsoft 365 services that are hardened at both the application and network level. For more information, see [Alternative ways for security professionals and IT to achieve modern security controls in today's unique remote work scenarios \(Microsoft Security Team blog\)](#) ↗.

- Is natively supported by most enterprise VPN platforms

Microsoft continues to collaborate with industry partners producing commercial VPN solutions to help partners develop targeted guidance and configuration templates for their solutions in alignment with the above recommendations. For more information, see [HOWTO guides for common VPN platforms](#).

 **Tip**

Microsoft recommends focusing split tunnel VPN configuration on documented dedicated IP ranges for Microsoft 365 services. FQDN or AppID-based split tunnel configurations, while possible on certain VPN client platforms, may not fully cover key Microsoft 365 scenarios and may conflict with IP based VPN routing rules. For this reason, Microsoft does not recommend using Microsoft 365 FQDNs to configure split tunnel VPN. The use of FQDN configuration may be useful in other related scenarios, such as .pac file customizations or to implement proxy bypass.

For full implementation guidance, see [Implementing VPN split tunneling for Microsoft 365](#).

For a step-by-step process to configure Microsoft 365 for remote workers, see [Set up your infrastructure for remote work](#).

The VPN split tunnel strategy

Traditional corporate networks are often designed to work securely for a precloud world where most important data, services, applications are hosted on premises and are directly connected to the internal corporate network, as are the majority of users. Thus network infrastructure is built around these elements in that branch offices are connected to the head office via *Multiprotocol Label Switching (MPLS)* networks, and remote users must connect to the corporate network over a VPN to access both on premises endpoints and the Internet. In this model, all traffic from remote users traverses the corporate network and is routed to the cloud service through a common egress point.

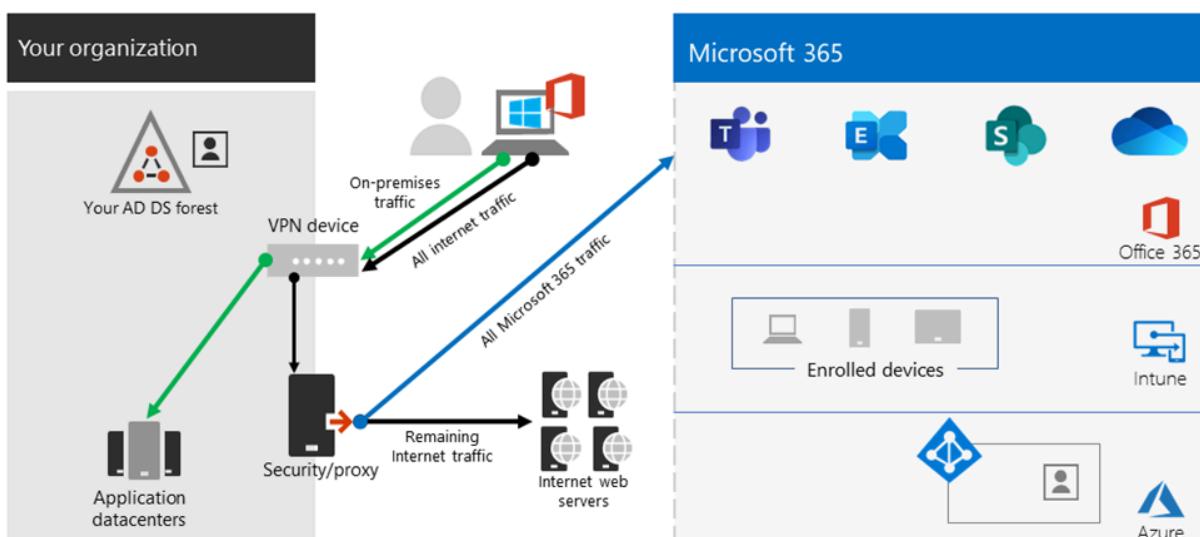


Figure 2: A common VPN solution for remote users where all traffic is forced back into the corporate network regardless of destination.

As organizations move data and applications to the cloud, this model has begun to become less effective as it quickly becomes cumbersome, expensive, and unscalable, significantly impacting network performance and efficiency of users and restricting the ability of the organization to adapt to changing needs. Numerous Microsoft customers have reported that a few years ago 80% of network traffic was to an internal destination, but in 2020 80% plus of traffic connects to an external cloud-based resource.

The COVID-19 crisis aggravated this problem to require immediate solutions for the vast majority of organizations. Many customers have found that the forced VPN model isn't scalable or performant enough for 100% remote work scenarios such as that which this crisis has necessitated. Rapid solutions are required for these organizations to operate efficiently.

For the Microsoft 365 service, Microsoft has designed the connectivity requirements for the service with this problem squarely in mind, where a focused, tightly controlled and relatively static set of service endpoints can be optimized simply and quickly so as to deliver high performance for users accessing the service, and reducing the burden on the VPN infrastructure so it can be used by traffic that still requires it.

Microsoft 365 categorizes the required endpoints for Microsoft 365 into three categories: **Optimize**, **Allow**, and **Default**. **Optimize** endpoints are our focus here and have the following characteristics:

- Are Microsoft owned and managed endpoints, hosted on Microsoft infrastructure
- Are dedicated to core Microsoft 365 workloads such as Exchange Online, SharePoint, Skype for Business Online, and Microsoft Teams
- Have IPs provided
- Low rate of change and are expected to remain small in number (currently 20 IP subnets)
- Are high volume and/or latency sensitive
- Are able to have required security elements provided in the service rather than inline on the network
- Account for around 70-80% of the volume of traffic to the Microsoft 365 service

This tightly scoped set of endpoints can be split out of the forced VPN tunnel and sent securely and directly to the Microsoft 365 service via the user's local interface. This is known as **split tunneling**.

Security elements such as DLP, AV protection, authentication, and access control can all be delivered much more efficiently against these endpoints at different layers within the service. As we also divert the bulk of the traffic volume away from the VPN solution, this frees the VPN capacity up for business critical traffic that still relies on it. It also should

remove the need in many cases to go through a lengthy and costly upgrade program to deal with this new way of operating.

VPN Split Tunnel for *Optimize Microsoft 365* endpoints

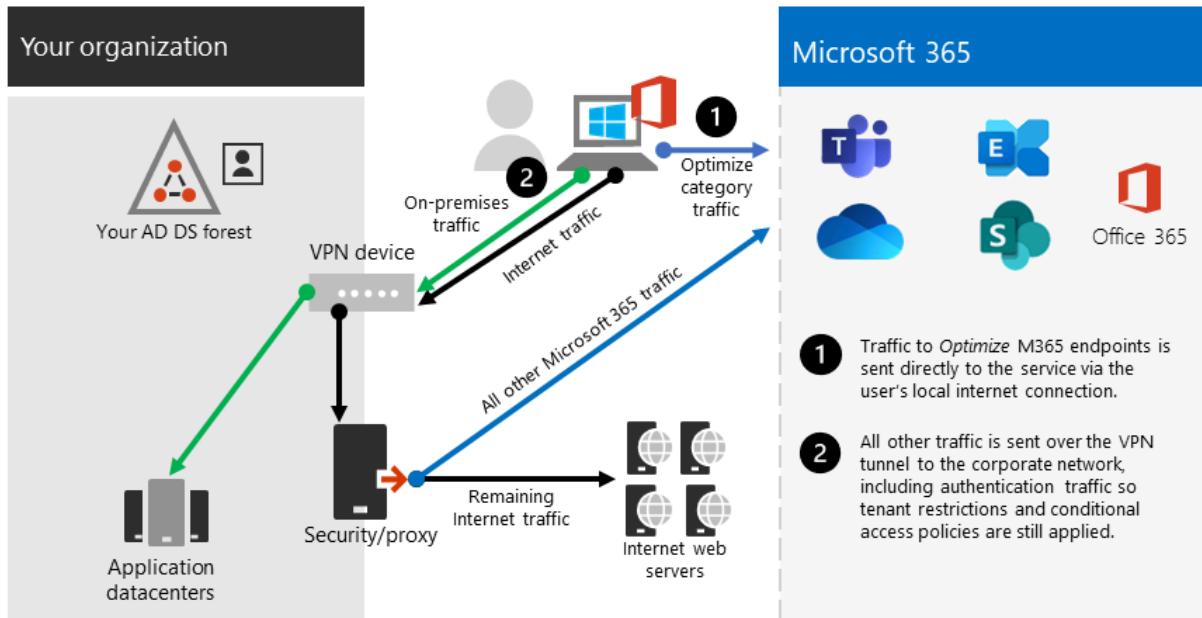


Figure 3: A VPN split tunnel solution with defined Microsoft 365 exceptions sent direct to the service. All other traffic is forced back into the corporate network regardless of destination.

From a security perspective, Microsoft has an array of security features which can be used to provide similar, or even enhanced security than that delivered by inline inspection by on premises security stacks. The Microsoft Security team's blog post [Alternative ways for security professionals and IT to achieve modern security controls in today's unique remote work scenarios](#) has a clear summary of features available and you'll find more detailed guidance within this article. You can also read about Microsoft's implementation of VPN split tunneling at [Running on VPN: How Microsoft is keeping its remote workforce connected](#).

In many cases, this implementation can be achieved in a matter of hours, allowing rapid resolution to one of the most pressing problems facing organizations as they rapidly shift to full scale remote working. For VPN split tunnel implementation guidance, see [Implementing VPN split tunneling for Microsoft 365](#).

FAQ

The Microsoft Security Team has published [Alternative ways for security professionals and IT to achieve modern security controls in today's unique remote work scenarios](#), a blog post, that outlines key ways for security professionals and IT can achieve modern

security controls in today's unique remote work scenarios. In addition, below are some of the common customer questions and answers on this subject.

How do I stop users accessing other tenants I don't trust where they could exfiltrate data?

The answer is a [feature called tenant restrictions](#). Authentication traffic isn't high volume nor especially latency sensitive so can be sent through the VPN solution to the on-premises proxy where the feature is applied. An allowlist of trusted tenants is maintained here and if the client attempts to obtain a token to a tenant that isn't trusted, the proxy simply denies the request. If the tenant is trusted, then a token is accessible if the user has the right credentials and rights.

So even though a user can make a TCP/UDP connection to the Optimize marked endpoints, without a valid token to access the tenant in question, they simply cannot log in and access/move any data.

Does this model allow access to consumer services such as personal OneDrive accounts?

No, it does not, the Microsoft 365 endpoints aren't the same as the consumer services (Onedrive.live.com as an example) so the split tunnel won't allow a user to directly access consumer services. Traffic to consumer endpoints will continue to use the VPN tunnel and existing policies will continue to apply.

How do I apply DLP and protect my sensitive data when the traffic no longer flows through my on-premises solution?

To help you prevent the accidental disclosure of sensitive information, Microsoft 365 has a rich set of [built-in tools](#). You can use the built-in [DLP capabilities](#) of Teams and SharePoint to detect inappropriately stored or shared sensitive information. If part of your remote work strategy involves a bring-your-own-device (BYOD) policy, you can use [app-based Conditional Access](#) to prevent sensitive data from being downloaded to users' personal devices

How do I evaluate and maintain control of the user's authentication when they are connecting directly?

In addition to the tenant restrictions feature noted in Q1, [conditional access policies](#) can be applied to dynamically assess the risk of an authentication request and react appropriately. Microsoft recommends the [Zero Trust model](#) is implemented over time and we can use Microsoft Entra Conditional Access policies to maintain control in a mobile and cloud-first world. Conditional access policies can be used to make a real-time decision on whether an authentication request is successful based on numerous factors such as:

- Device, is the device known/trusted/Domain joined?
- IP – is the authentication request coming from a known corporate IP address? Or from a country/region we don't trust?
- Application – Is the user authorized to use this application?

We can then trigger policy such as approve, trigger MFA or block authentication based on these policies.

How do I protect against viruses and malware?

Again, Microsoft 365 provides protection for the Optimize marked endpoints in various layers in the service itself, [outlined in this document](#). As noted, it's vastly more efficient to provide these security elements in the service itself rather than try to do it in line with devices that may not fully understand the protocols/traffic. By default, SharePoint [automatically scans file uploads](#) for known malware

For the Exchange endpoints listed above, [Exchange Online Protection](#) and [Microsoft Defender for Microsoft 365](#) do an excellent job of providing security of the traffic to the service.

Can I send more than just the Optimize traffic direct?

Priority should be given to the Optimize marked endpoints as these will give maximum benefit for a low level of work. However, if you wish, the Allow marked endpoints are required for the service to work and have IP addresses provided for the endpoints that can be used if necessary.

There are also various vendors who offer cloud-based proxy/security solutions called *secure web gateways* which provide central security, control, and corporate policy application for general web browsing. These solutions can work well in a cloud-first world, if highly available, performant, and provisioned close to your users by allowing secure Internet access to be delivered from a cloud-based location close to the user. This removes the need for a hairpin through the VPN/corporate network for general browsing traffic, while still allowing central security control.

Even with these solutions in place however, Microsoft still strongly recommends that Optimize marked Microsoft 365 traffic is sent direct to the service.

For guidance on allowing direct access to an Azure Virtual Network, see [Remote work using Azure VPN Gateway Point-to-site](#).

Why is port 80 required? Is traffic sent in the clear?

Port 80 is only used for things like redirect to a port 443 session, no customer data is sent or is accessible over port 80. [Encryption](#) outlines encryption for data in transit and at rest for Microsoft 365, and [Types of traffic](#) outlines how we use SRTP to protect Teams media traffic.

Does this advice apply to users in China using a worldwide instance of Microsoft 365?

No, it does not. The one caveat to the above advice is users in the PRC who are connecting to a worldwide instance of Microsoft 365. Due to the common occurrence of cross border network congestion in the region, direct Internet egress performance can be variable. Most customers in the region operate using a VPN to bring the traffic into the corporate network and utilize their authorized MPLS circuit or similar to egress outside the country/region via an optimized path. This is outlined further in the article [Microsoft 365 performance optimization for China users](#).

Does split-tunnel configuration work for Teams running in a browser?

Yes, with caveats. Most Teams functionality is supported in the browsers listed in [Get clients for Microsoft Teams](#).

In addition, Microsoft Edge 96 and above supports VPN split tunneling for peer-to-peer traffic by enabling the Edge [WebRtcRespectOsRoutingTableEnabled](#) policy. At this time, other browsers may not support VPN split tunneling for peer-to-peer traffic.

Related articles

[Implementing VPN split tunneling for Microsoft 365](#)

[Common VPN split tunneling scenarios for Microsoft 365](#)

[Securing Teams media traffic for VPN split tunneling](#)

[Special considerations for Stream and live events in VPN environments](#)

[Microsoft 365 performance optimization for China users](#)

[Microsoft 365 Network Connectivity Principles](#)

[Assessing Microsoft 365 network connectivity](#)

[Microsoft 365 network and performance tuning](#)

[Alternative ways for security professionals and IT to achieve modern security controls in today's unique remote work scenarios \(Microsoft Security Team blog\)](#) ↗

[Enhancing VPN performance at Microsoft: using Windows 10 VPN profiles to allow auto-on connections](#) ↗

[Running on VPN: How Microsoft is keeping its remote workforce connected](#) ↗

[Microsoft global network](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

Common VPN split tunneling scenarios for Microsoft 365

Article • 12/20/2023

ⓘ Note

This article is part of a set of articles that address Microsoft 365 optimization for remote users.

- For an overview of using VPN split tunneling to optimize Microsoft 365 connectivity for remote users, see [Overview: VPN split tunneling for Microsoft 365](#).
- For detailed guidance on implementing VPN split tunneling, see [Implementing VPN split tunneling for Microsoft 365](#).
- For guidance on securing Teams media traffic in VPN split tunneling environments, see [Securing Teams media traffic for VPN split tunneling](#).
- For information about how to configure Stream and live events in VPN environments, see [Special considerations for Stream and live events in VPN environments](#).
- For information about optimizing Microsoft 365 worldwide tenant performance for users in China, see [Microsoft 365 performance optimization for China users](#).

In the list below, you'll see the most common VPN scenarios seen in enterprise environments. Most customers traditionally operate model 1 (VPN Forced Tunnel). This section will help you to quickly and securely transition to **model 2**, which is achievable with relatively little effort, and has enormous benefits to network performance and user experience.

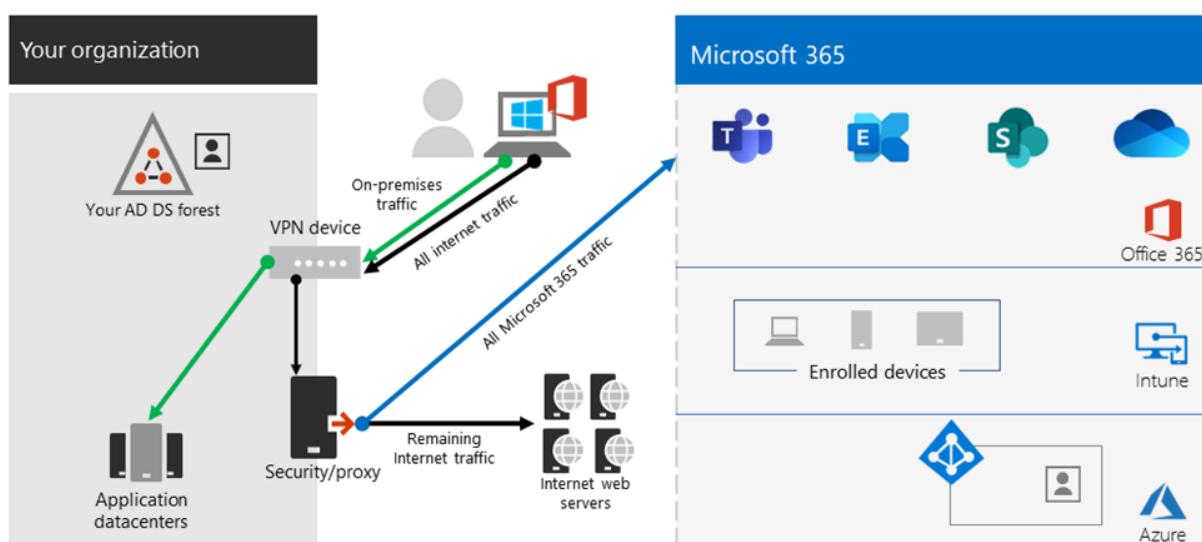
[] Expand table

Model	Description
1. VPN Forced Tunnel	100% of traffic goes into VPN tunnel, including on-premise, Internet, and all O365/M365
2. VPN Forced Tunnel with few exceptions	VPN tunnel is used by default (default route points to VPN), with few, most important exempt scenarios that are allowed to go direct

Model	Description
3. VPN Forced Tunnel with broad exceptions	VPN tunnel is used by default (default route points to VPN), with broad exceptions that are allowed to go direct (such as all Microsoft 365, All Salesforce, All Zoom)
4. VPN Selective Tunnel	VPN tunnel is used only for corpnet-based services. Default route (Internet and all Internet-based services) goes direct.
5. No VPN	A variation of #2. Instead of legacy VPN, all corpnet services are published through modern security approaches (like Zscaler ZPA, Microsoft Entra ID Proxy/MCAS, etc.)

1. VPN Forced Tunnel

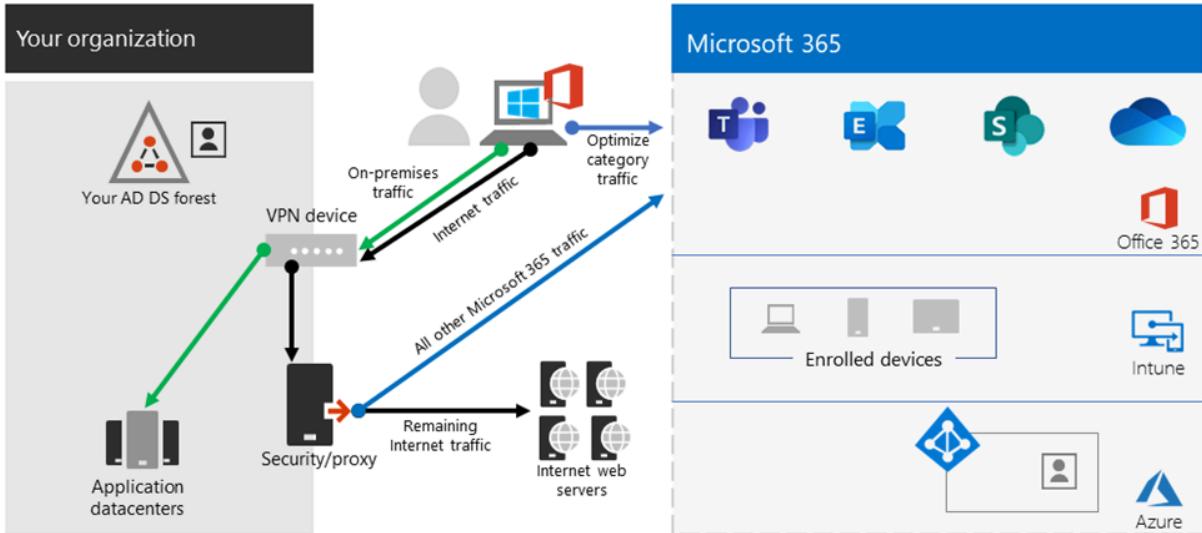
The most common starting scenario for most enterprise customers. A forced VPN is used, which means 100% of traffic is directed into the corporate network whether the endpoint resides within the corporate network or not. Any external (Internet) bound traffic such as Microsoft 365 or Internet browsing is then hair-pinned back out of the on-premises security equipment such as proxies. In the current climate with nearly 100% of users working remotely, this model therefore puts high load on the VPN infrastructure and is likely to significantly hinder performance of all corporate traffic and thus the enterprise to operate efficiently at a time of crisis.



2. VPN Forced Tunnel with a small number of trusted exceptions

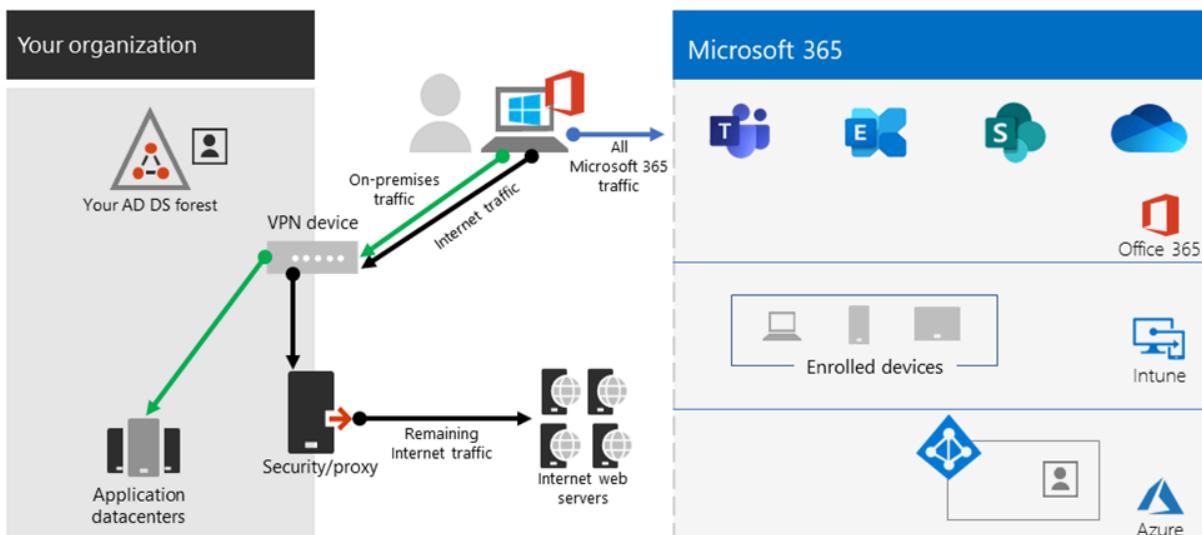
Significantly more efficient for an enterprise to operate under. This model allows a few controlled and defined endpoints that are high load and latency sensitive to bypass the

VPN tunnel and go direct to the Microsoft 365 service. This significantly improves the performance for the offloaded services, and also decreases the load on the VPN infrastructure, thus allowing elements that still require it to operate with lower contention for resources. It's this model that this article concentrates on assisting with the transition to as it allows for simple, defined actions to be taken quickly with numerous positive outcomes.



3. VPN Forced Tunnel with broad exceptions

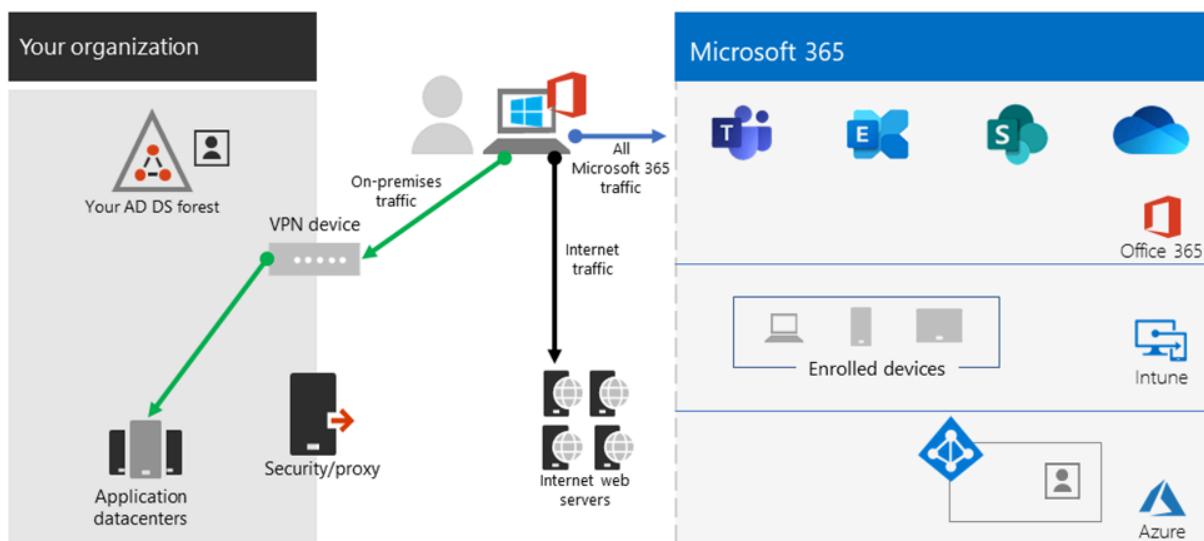
Broadens the scope of model 2. Rather than just sending a small group of defined endpoints direct, it instead sends all traffic directly to trusted services such Microsoft 365 and SalesForce. This further reduces the load on the corporate VPN infrastructure and improves the performance of the services defined. As this model is likely to take more time to assess the feasibility of and implement, It's likely a step that can be taken iteratively at a later date once model two is successfully in place.



4. VPN selective Tunnel

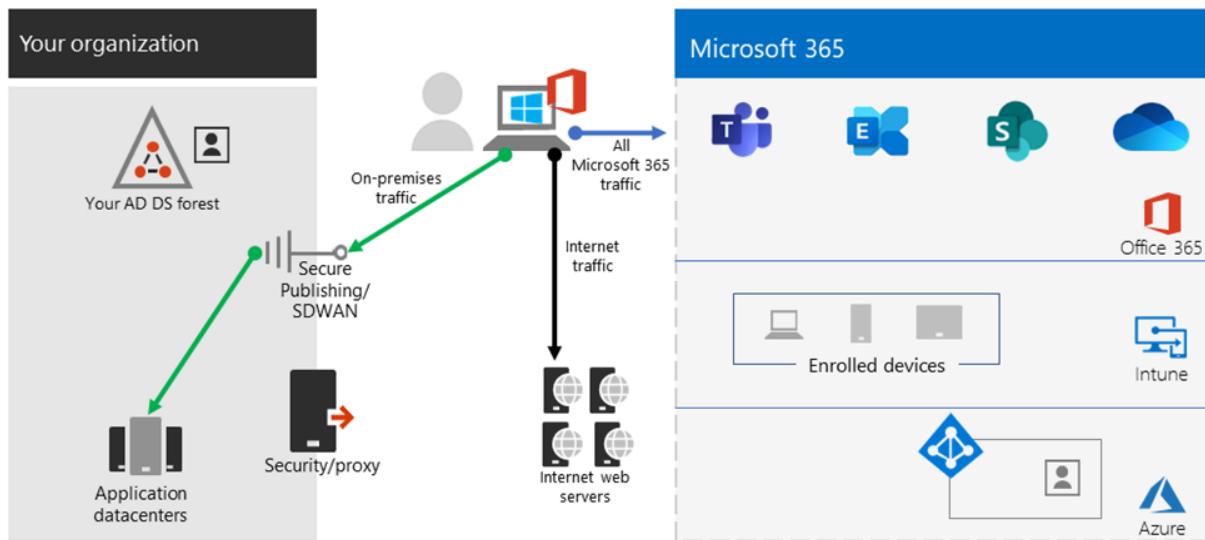
Reverses the third model in that only traffic identified as having a corporate IP address is sent down the VPN tunnel and thus the Internet path is the default route for everything else. This model requires an organization to be well on the path to [Zero Trust](#) in able to safely implement this model. It should be noted that this model or some variation thereof will likely become the necessary default over time as more services move away from the corporate network and into the cloud.

Microsoft uses this model internally. You can find more information on Microsoft's implementation of VPN split tunneling at [Running on VPN: How Microsoft is keeping its remote workforce connected](#).



5. No VPN

A more advanced version of model number 2, whereby any internal services are published through a modern security approach or SDWAN solution such as Microsoft Entra ID Proxy, Defender for Cloud Apps, Zscaler ZPA, etc.



Related articles

[Overview: VPN split tunneling for Microsoft 365](#)

[Implementing VPN split tunneling for Microsoft 365](#)

[Securing Teams media traffic for VPN split tunneling](#)

[Special considerations for Stream and live events in VPN environments](#)

[Microsoft 365 performance optimization for China users](#)

[Microsoft 365 Network Connectivity Principles](#)

[Assessing Microsoft 365 network connectivity](#)

[Microsoft 365 network and performance tuning](#)

[Alternative ways for security professionals and IT to achieve modern security controls in today's unique remote work scenarios \(Microsoft Security Team blog\)](#) ↗

[Enhancing VPN performance at Microsoft: using Windows 10 VPN profiles to allow auto-on connections](#) ↗

[Running on VPN: How Microsoft is keeping its remote workforce connected](#) ↗

[Microsoft global network](#)

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Implementing VPN split tunneling for Microsoft 365

Article • 12/21/2023

ⓘ Note

This article is part of a set of articles that address Microsoft 365 optimization for remote users.

- For an overview of using VPN split tunneling to optimize Microsoft 365 connectivity for remote users, see [Overview: VPN split tunneling for Microsoft 365](#).
- For a detailed list of VPN split tunneling scenarios, see [Common VPN split tunneling scenarios for Microsoft 365](#).
- For guidance on securing Teams media traffic in VPN split tunneling environments, see [Securing Teams media traffic for VPN split tunneling](#).
- For information about how to configure Stream and live events in VPN environments, see [Special considerations for Stream and live events in VPN environments](#).
- For information about optimizing Microsoft 365 worldwide tenant performance for users in China, see [Microsoft 365 performance optimization for China users](#).

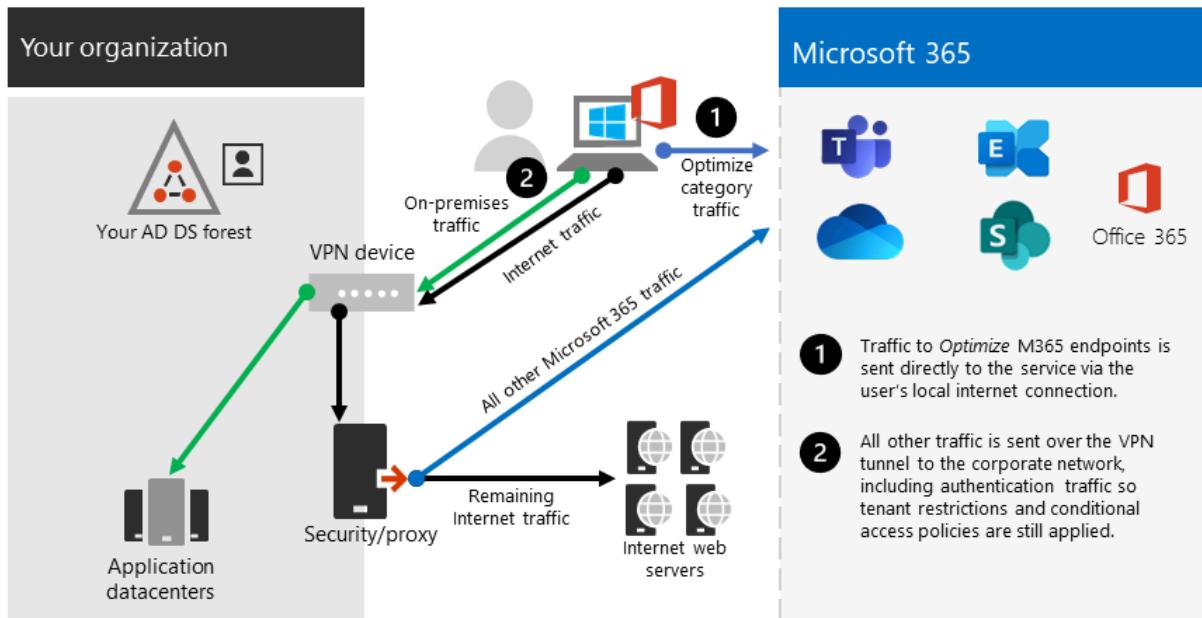
Microsoft's recommended strategy for optimizing remote worker's connectivity is focused on rapidly mitigating problems and providing high performance with a few simple steps. These steps adjust the legacy VPN approach for a few defined endpoints that bypass bottlenecked VPN servers. An equivalent or even superior security model can be applied at different layers to remove the need to secure all traffic at the egress of the corporate network. In most cases, this can be effectively achieved within hours and is then scalable to other workloads as requirements demand and time allows.

Implement VPN split tunneling

In this article, you'll find the simple steps required to migrate your VPN client architecture from a *VPN forced tunnel* to a *VPN forced tunnel with a few trusted exceptions*, [VPN split tunnel model #2](#) in [Common VPN split tunneling scenarios for Microsoft 365](#).

The diagram below illustrates how the recommended VPN split tunnel solution works:

VPN Split Tunnel for *Optimize* Microsoft 365 endpoints



1. Identify the endpoints to optimize

In the [Microsoft 365 URLs and IP address ranges](#) article, Microsoft clearly identifies the key endpoints you need to optimize and categorizes them as **Optimize**. There are currently just four URLs and 20 IP subnets that need to be optimized. This small group of endpoints accounts for around 70% - 80% of the volume of traffic to the Microsoft 365 service including the latency sensitive endpoints such as those for Teams media. Essentially this is the traffic that we need to take special care of and is also the traffic that will put incredible pressure on traditional network paths and VPN infrastructure.

URLs in this category have the following characteristics:

- Are Microsoft owned and managed endpoints, hosted on Microsoft infrastructure
- Have IPs provided
- Low rate of change and are expected to remain small in number (currently 20 IP subnets)
- Are bandwidth and/or latency sensitive
- Are able to have required security elements provided in the service rather than inline on the network
- Account for around 70-80% of the volume of traffic to the Microsoft 365 service

For more information about Microsoft 365 endpoints and how they are categorized and managed, see [Managing Microsoft 365 endpoints](#).

Optimize URLs

The current Optimize URLs can be found in the table below. Under most circumstances, you should only need to use URL endpoints in a [browser PAC file](#) where the endpoints are configured to be sent direct, rather than to the proxy.

[+] Expand table

Optimize URLs	Port/Protocol	Purpose
https://outlook.office365.com	TCP 443	This is one of the primary URLs Outlook uses to connect to its Exchange Online server and has a high volume of bandwidth usage and connection count. Low network latency is required for online features including: instant search, other mailbox calendars, free / busy lookup, manage rules and alerts, Exchange online archive, emails departing the outbox.
https://outlook.office.com	TCP 443	This URL is used for Outlook Online Web Access to connect to Exchange Online server, and is sensitive to network latency. Connectivity is particularly required for large file upload and download with SharePoint Online.
<code>https://<tenant\>.sharepoint.com</code>	TCP 443	This is the primary URL for SharePoint Online and has high-bandwidth usage.
<code>https://<tenant\>-my.sharepoint.com</code>	TCP 443	This is the primary URL for OneDrive for Business and has high bandwidth usage and possibly high connection count from the OneDrive for Business Sync tool.
Teams Media IPs (no URL)	UDP 3478, 3479, 3480, and 3481	Relay Discovery allocation and real-time traffic. These are the endpoints used for Skype for Business and Microsoft Teams Media traffic (calls, meetings, etc.). Most endpoints are provided when the Microsoft Teams client establishes a call (and are contained within the required IPs listed for the service). Use of the UDP protocol is required for optimal media quality.

In the above examples, **tenant** should be replaced with your Microsoft 365 tenant name. For example, **contoso.onmicrosoft.com** would use **contoso.sharepoint.com** and **contoso-my.sharepoint.com**.

Optimize IP address ranges

At the time of writing the IP address ranges that these endpoints correspond to are as follows. It's **very strongly** advised you use a [script such as this](#) example, the [Microsoft 365 IP and URL web service](#) or the [URL/IP page](#) to check for any updates when applying the configuration and put a policy in place to do so regularly. If utilizing continuous access evaluation, refer to [Continuous access evaluation IP address variation](#). Routing optimized IPs through a trusted IP or VPN may be required to prevent blocks related to *insufficient_claims* or *Instant IP Enforcement check failed* in certain scenarios.

markdown

```
104.146.128.0/17
13.107.128.0/22
13.107.136.0/22
13.107.18.10/31
13.107.6.152/31
13.107.64.0/18
131.253.33.215/32
132.245.0.0/16
150.171.32.0/22
150.171.40.0/22
204.79.197.215/32
23.103.160.0/20
40.104.0.0/15
40.108.128.0/17
40.96.0.0/13
52.104.0.0/14
52.112.0.0/14
52.96.0.0/14
52.122.0.0/15
```

2. Optimize access to these endpoints via the VPN

Now that we have identified these critical endpoints, we need to divert them away from the VPN tunnel and allow them to use the user's local Internet connection to connect directly to the service. The manner in which this is accomplished will vary depending on the VPN product and machine platform used but most VPN solutions will allow some simple configuration of policy to apply this logic. For information VPN platform-specific split tunnel guidance, see [HOWTO guides for common VPN platforms](#).

If you wish to test the solution manually, you can execute the following PowerShell example to emulate the solution at the route table level. This example adds a route for each of the Teams Media IP subnets into the route table. You can test Teams media performance before and after, and observe the difference in routes for the specified endpoints.

Example: Add Teams Media IP subnets into the route table

PowerShell

```
$intIndex = "" # index of the interface connected to the internet
$gateway = "" # default gateway of that interface
$destPrefix = "52.120.0.0/14", "52.112.0.0/14", "13.107.64.0/18" # Teams
Media endpoints
# Add routes to the route table
foreach ($prefix in $destPrefix) {New-NetRoute -DestinationPrefix $prefix -
InterfaceIndex $intIndex -NextHop $gateway}
```

In the above script, `$intIndex` is the index of the interface connected to the internet (find by running `get-netadapter` in PowerShell; look for the value of `ifIndex`) and `$gateway` is the default gateway of that interface (find by running `ipconfig` in a command prompt or `(Get-NetIPConfiguration | Foreach IPv4DefaultGateway).NextHop` in PowerShell).

Once you have added the routes, you can confirm that the route table is correct by running `route print` in a command prompt or PowerShell. The output should contain the routes you added, showing the interface index (22 in this example) and the gateway for that interface (192.168.1.1 in this example):

22	52.120.0.0/14	192.168.1.1	256	4260	ActiveStore
22	52.112.0.0/14	192.168.1.1	256	4260	ActiveStore
22	13.107.64.0/18	192.168.1.1	256	4260	ActiveStore
80	0.0.0.0/0	0.0.0.0	1	55	ActiveStore
22	0.0.0.0/0	192.168.1.1	0	4260	ActiveStore

To add routes for *all* current IP address ranges in the Optimize category, you can use the following script variation to query the [Microsoft 365 IP and URL web service](#) for the current set of Optimize IP subnets and add them to the route table.

Example: Add all Optimize subnets into the route table

PowerShell

```
$intIndex = "" # index of the interface connected to the internet
$gateway = "" # default gateway of that interface
# Query the web service for IPs in the Optimize category
$ep = Invoke-RestMethod ("https://endpoints.office.com/endpoints/worldwide?
clientrequestid=" + ([GUID]::NewGuid()).Guid)
# Output only IPv4 Optimize IPs to $optimizeIps
$destPrefix = $ep | where {$_.category -eq "Optimize"} | Select-Object -
ExpandProperty ips | Where-Object { $_ -like '*.*' }
# Add routes to the route table
foreach ($prefix in $destPrefix) {New-NetRoute -DestinationPrefix $prefix -
InterfaceIndex $intIndex -NextHop $gateway}
```

If you inadvertently added routes with incorrect parameters or simply wish to revert your changes, you can remove the routes you just added with the following command:

PowerShell

```
foreach ($prefix in $destPrefix) {Remove-NetRoute -DestinationPrefix $prefix  
-InterfaceIndex $intIndex -NextHop $gateway}
```

The VPN client should be configured so that traffic to the **Optimize** IPs are routed in this way. This allows the traffic to utilize local Microsoft resources such as Microsoft 365 Service Front Doors [such as the Azure Front Door](#) that delivers Microsoft 365 services and connectivity endpoints as close to your users as possible. This allows us to deliver high performance levels to users wherever they are in the world and takes full advantage of [Microsoft's world class global network](#), which is likely within a few milliseconds of your users' direct egress.

HOWTO guides for common VPN platforms

This section provides links to detailed guides for implementing split tunneling for Microsoft 365 traffic from the most common partners in this space. We'll add additional guides as they become available.

- **Windows 10 VPN client:** [Optimizing Microsoft 365 traffic for remote workers with the native Windows 10 VPN client](#)
- **Cisco Anyconnect:** [Optimize Anyconnect Split Tunnel for Office365](#)
- **Palo Alto GlobalProtect:** [Optimizing Microsoft 365 Traffic via VPN Split Tunnel Exclude Access Route](#)
- **F5 Networks BIG-IP APM:** [Optimizing Microsoft 365 traffic on Remote Access through VPNs when using BIG-IP APM](#)
- **Citrix Gateway:** [Optimizing Citrix Gateway VPN split tunnel for Office365](#)
- **Pulse Secure: VPN Tunneling:** [How to configure split tunneling to exclude Microsoft 365 applications](#)
- **Check Point VPN:** [How to configure Split Tunnel for Microsoft 365 and other SaaS Applications](#)

Related articles

[Overview: VPN split tunneling for Microsoft 365](#)

[Common VPN split tunneling scenarios for Microsoft 365](#)

[Securing Teams media traffic for VPN split tunneling](#)

[Special considerations for Stream and live events in VPN environments](#)

[Microsoft 365 performance optimization for China users](#)

[Microsoft 365 Network Connectivity Principles](#)

[Assessing Microsoft 365 network connectivity](#)

[Microsoft 365 network and performance tuning](#)

[Alternative ways for security professionals and IT to achieve modern security controls in today's unique remote work scenarios \(Microsoft Security Team blog\)](#) ↗

[Enhancing VPN performance at Microsoft: using Windows 10 VPN profiles to allow auto-on connections](#) ↗

[Running on VPN: How Microsoft is keeping its remote workforce connected](#) ↗

[Microsoft global network](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

Securing Teams media traffic for VPN split tunneling

Article • 12/21/2023

ⓘ Note

This article is part of a set of articles that address Microsoft 365 optimization for remote users.

- For an overview of using VPN split tunneling to optimize Microsoft 365 connectivity for remote users, see [Overview: VPN split tunneling for Microsoft 365](#).
- For detailed guidance on implementing VPN split tunneling, see [Implementing VPN split tunneling for Microsoft 365](#).
- For a detailed list of VPN split tunneling scenarios, see [Common VPN split tunneling scenarios for Microsoft 365](#).
- For information about how to configure Stream and live events in VPN environments, see [Special considerations for Stream and live events in VPN environments](#).
- For information about optimizing Microsoft 365 worldwide tenant performance for users in China, see [Microsoft 365 performance optimization for China users](#).

Some Microsoft Teams administrators might require detailed information on how call flows operate in Teams using a split tunneling model and how connections are secured.

Configuration

For both calls and meetings, as long as the required Optimize IP subnets for Teams media are correctly in place in the route table, when Teams calls the [GetBestRoute](#) function to determine which local interface corresponds to the route it should use for a particular destination, the local interface will be returned for Microsoft destinations in the Microsoft IP blocks listed above.

Some VPN client software allows routing manipulation based on URL. However, Teams media traffic has no URL associated with it, so control of routing for this traffic must be done using IP subnets.

In certain scenarios, often unrelated to Teams client configuration, media traffic still traverses the VPN tunnel even with the correct routes in place. If you encounter this scenario, then using a firewall rule to block the Teams IP subnets or ports from using the VPN should suffice.

Important

To ensure Teams media traffic is routed via the desired method in all VPN scenarios, please ensure users are running Microsoft Teams client version **1.3.00.13565** or greater. This version includes improvements in how the client detects available network paths.

Signaling traffic is performed over HTTPS and isn't as latency sensitive as the media traffic and is marked as **Allow** in the URL/IP data and thus can safely be routed through the VPN client if desired.

Note

Microsoft Edge **96 and above** also supports VPN split tunneling for peer-to-peer traffic. This means customers can gain the benefit of VPN split tunneling for Teams web clients on Edge, for instance. Customers who want to set it up for websites running on Edge can achieve it by taking the additional step of disabling the Edge [WebRtcRespectOsRoutingTableEnabled](#) policy.

Security

One common argument for avoiding split tunnels is that it's less secure to do so, i.e any traffic that doesn't go through the VPN tunnel won't benefit from whatever encryption scheme is applied to the VPN tunnel, and is therefore less secure.

The main counter-argument to this is that media traffic is already encrypted via *Secure Real-Time Transport Protocol (SRTP)*, a profile of Real-Time Transport Protocol (RTP) that provides confidentiality, authentication, and replay attack protection to RTP traffic. SRTP itself relies on a randomly generated session key, which is exchanged via the TLS secured signaling channel. This is covered in great detail within [**this security guide**](#), but the primary section of interest is media encryption.

Media traffic is encrypted using SRTP, which uses a session key generated by a secure random number generator and exchanged using the signaling TLS channel. In addition,

media flowing in both directions between the Mediation Server and its internal next hop is also encrypted using SRTP.

Skype for Business Online generates username/passwords for secure access to media relays over *Traversal Using Relays around NAT (TURN)*. Media relays exchange the username/password over a TLS-secured SIP channel. It's worth noting that even though a VPN tunnel may be used to connect the client to the corporate network, the traffic still needs to flow in its SRTP form when it leaves the corporate network to reach the service.

Information on how Teams mitigates common security concerns such as voice or *Session Traversal Utilities for NAT (STUN)* amplification attacks can be found in [5.1 Security Considerations for Implementers](#).

You can also read about modern security controls in remote work scenarios at [Alternative ways for security professionals and IT to achieve modern security controls in today's unique remote work scenarios \(Microsoft Security Team blog\)](#) ↗.

Testing

Once the policy is in place, you should confirm it's working as expected. There are multiple ways of testing the path is correctly set to use the local Internet connection:

- Run the [Microsoft 365 connectivity test](#) ↗ that will run connectivity tests for you including trace routes as above. We're also adding in VPN tests into this tooling that should also provide additional insights.
- A simple **tracert** to an endpoint within scope of the split tunnel should show the path taken, for example:

```
PowerShell
```

```
tracert worldaz.tr.teams.microsoft.com
```

You should then see a path via the local ISP to this endpoint that should resolve to an IP in the Teams ranges we have configured for split tunneling.

- Take a network capture using a tool such as Wireshark. Filter on UDP during a call and you should see traffic flowing to an IP in the Teams **Optimize** range. If the VPN tunnel is being used for this traffic, then the media traffic won't be visible in the trace.

Additional support logs

If you need further data to troubleshoot, or are requesting assistance from Microsoft support, obtaining the following information should allow you to expedite finding a solution. Microsoft support's **TSS Windows CMD-based universal TroubleShooting Script toolset** can help you to collect the relevant logs in a simple manner. The tool and instructions on use can be found at <https://aka.ms/TssTools>.

Related articles

[Overview: VPN split tunneling for Microsoft 365](#)

[Implementing VPN split tunneling for Microsoft 365](#)

[Common VPN split tunneling scenarios for Microsoft 365](#)

[Special considerations for Stream and live events in VPN environments](#)

[Microsoft 365 performance optimization for China users](#)

[Microsoft 365 Network Connectivity Principles](#)

[Assessing Microsoft 365 network connectivity](#)

[Microsoft 365 network and performance tuning](#)

[Alternative ways for security professionals and IT to achieve modern security controls in today's unique remote work scenarios \(Microsoft Security Team blog\)](#)

[Enhancing VPN performance at Microsoft: using Windows 10 VPN profiles to allow auto-on connections](#)

[Running on VPN: How Microsoft is keeping its remote workforce connected](#)

[Microsoft global network](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Special considerations for Stream and Teams events in VPN environments

Article • 10/10/2023

ⓘ Note

This article is part of a set of articles that address Microsoft 365 optimization for remote users. The following endpoints are specific to Worldwide Commercial and Government Community Cloud (GCC) environments; the endpoints listed here are not applicable to U.S. Government GCC High or U.S. Government DoD environments.

- For an overview of using VPN split tunneling to optimize Microsoft 365 connectivity for remote users, see [Overview: VPN split tunneling for Microsoft 365](#).
- For detailed guidance on implementing VPN split tunneling, see [Implementing VPN split tunneling for Microsoft 365](#).
- For a detailed list of VPN split tunneling scenarios, see [Common VPN split tunneling scenarios for Microsoft 365](#).
- For guidance on securing Teams media traffic in VPN split tunneling environments, see [Securing Teams media traffic for VPN split tunneling](#).
- For information about optimizing Microsoft 365 worldwide tenant performance for users in China, see [Microsoft 365 performance optimization for China users](#).

Microsoft 365 Live Events attendee traffic (this includes attendees to Teams-produced live events and those produced with an external encoder via Teams, Stream, or Viva Engage), Microsoft Teams Town hall attendee traffic and on-demand Stream attendee traffic is currently categorized as **Default** versus **Optimize** in the [URL/IP list for the service](#). These endpoints are categorized as **Default** because they're hosted on CDNs that might also be used by other services. Customers generally prefer to proxy this type of traffic and apply any security elements normally done on endpoints such as these.

Many customers have asked for URL/IP data needed to connect their attendees to Stream or Teams events directly from their local internet connection, rather than route the high-volume and latency-sensitive traffic via the VPN infrastructure. Typically, this

isn't possible without both dedicated namespaces and accurate IP information for the endpoints, which isn't provided for Microsoft 365 endpoints categorized as **Default**.

Use the following steps to enable direct connectivity for the Stream or Teams events services from clients using a forced tunnel VPN. This solution is intended to provide customers with an option to avoid routing Events attendee traffic over VPN while there's high network traffic due to work-from-home scenarios. If possible, we recommend accessing the service through an inspecting proxy.

Note

Using this solution, there might be service elements that do not resolve to the IP addresses provided and thus traverse the VPN, but the bulk of high-volume traffic like streaming data should. There might be other elements outside the scope of Live Events/Stream which get caught by this offload, but these should be limited as they must meet both the FQDN *and* the IP match before going direct.

Important

We recommend you weigh the risk of sending more traffic that bypasses the VPN over the performance gain for Live Events.

To implement the forced tunnel exception for Teams Events and Stream, the following steps should be applied:

1. Configure external DNS resolution

Clients need external, recursive DNS resolution to be available so that the following host names can be resolved to IP addresses.

- *.azureedge.net
- *.media.azure.net
- *.bmc.cdn.office.net
- *.ml.cdn.office.net

***.azureedge.net** is used for Stream events ([Configure encoders for live streaming in Microsoft Stream - Microsoft Stream | Microsoft Docs](#)).

***.media.azure.net** and ***.bmc.cdn.office.net** are used for Teams-produced Live Events (Quick Start events and RTMP-In supported events) scheduled from the Teams client.

`*.media.azure.net`, `*.bmc.cdn.office.net` and `*.ml.cdn.office.net` are used for Teams Town hall events.

Some of these endpoints are shared with other elements outside of Stream or Teams events. We don't recommend just using these FQDNs to configure VPN offload even if technically possible in your VPN solution (for example, if it works at the FQDN rather than IP).

FQDNs aren't required in the VPN configuration, they're purely for use in PAC files in combination with the IPs to send the relevant traffic direct.

2. Implement PAC file changes (where required)

For organizations that utilize a PAC file to route traffic through a proxy while on VPN, this is normally achieved using FQDNs. However, with Stream/Live Events/Town hall, the host names provided contain wildcards such as `*.azureedge.net`, which also encompasses other elements for which it isn't possible to provide full IP listings. Thus, if the request is sent direct based on DNS wildcard match alone, traffic to these endpoints will be blocked as there's no route via the direct path for it in [Step 3](#) later in this article.

To solve this, we can provide the following IPs and use them in combination with the host names in an example PAC file as described in [Step 1](#). The PAC file checks if the URL matches those used for Stream/Live Events/Town hall and then if it does, it then also checks to see if the IP returned from a DNS lookup matches those provided for the service. If *both* match, then the traffic is routed direct. If either element (FQDN/IP) doesn't match, then the traffic is sent to the proxy. As a result, the configuration ensures that anything that resolves to an IP outside of the scope of both the IP and defined namespaces traverses the proxy via the VPN as normal.

Gathering the current lists of CDN Endpoints

Teams events use multiple CDN providers to stream to customers, to provide the best coverage, quality, and resiliency. Currently, both Azure CDN from Microsoft and from Verizon are used. Over time this could be changed due to situations such as regional availability. This article is a source to enable you to keep up to date on IP ranges.

For Azure CDN from Microsoft, you can download the list from [Download Azure IP Ranges and Service Tags – Public Cloud from Official Microsoft Download Center](#) - you'll need to look specifically for the service tag `AzureFrontdoor.Frontend` in the JSON; `addressPrefixes` will show the IPv4/IPv6 subnets. Over time the IPs can change, but the service tag list is always updated before they're put in use.

For Azure CDN from Verizon (Edgecast) you can find an exhaustive list using [Edge Nodes - List](#) (select Try It) - you'll need to look specifically for the **Premium_Verizon** section. Note that this API shows all Edgecast IPs (origin and Anycast). Currently there isn't a mechanism for the API to distinguish between origin and Anycast.

To implement this in a PAC file, you can use the following example that sends the Microsoft 365 Optimize traffic direct (which is recommended best practice) via FQDN, and the critical Stream/Live Events traffic direct via a combination of the FQDN and the returned IP address. The placeholder name *Contoso* would need to be edited to your specific tenant's name where *contoso* is from contoso.onmicrosoft.com

Example PAC file

Here's an example of how to generate the PAC files:

1. Save the script below to your local hard disk as *Get-TLEPacFile.ps1*.
2. Go to the [Verizon URL](#) and download the resulting JSON (copy paste it into a file like *cdnedgenodes.json*)
3. Put the file into the same folder as the script.
4. In a PowerShell window, run the following command. Change out the tenant name for something else if you want the SPO URLs. This is Type 2, so **Optimize** and **Allow** (Type 1 is Optimize only).

PowerShell

```
.\Get-TLEPacFile.ps1 -Instance Worldwide -Type 2 -TenantName <contoso>
-CdnEdgeNodesFilePath .\cdnedgenodes.json -FilePath TLE.pac
```

5. The TLE.pac file will contain all the namespaces and IPs (IPv4/IPv6).

Get-TLEPacFile.ps1

PowerShell

```
# Copyright (c) Microsoft Corporation. All rights reserved.
# Licensed under the MIT License.

<#PSScriptInfo

.VERSION 1.0.5

.AUTHOR Microsoft Corporation
```

```
.GUID 7f692977-e76c-4582-97d5-9989850a2529

.COMPANYNAME Microsoft

.COPYRIGHT
Copyright (c) Microsoft Corporation. All rights reserved.
Licensed under the MIT License.

.TAGS PAC Microsoft Microsoft365 365

.LICENSEURI

.PROJECTURI http://aka.ms/ipurlws

.ICONURI

.EXTERNALMODULEDEPENDENCIES

.REQUIREDSCRIPTS

.EXTERNALSCRIPTDEPENDENCIES

.RELEASENOTES

#>

<#

.SYNOPSIS

Create a PAC file for Microsoft 365 prioritized connectivity

.DESCRIPTION

This script will access updated information to create a PAC file to
prioritize Microsoft 365 Urls for
better access to the service. This script will allow you to create different
types of files depending
on how traffic needs to be prioritized.

.PARAMETER Instance

The service instance inside Microsoft 365.

.PARAMETER ClientRequestId

The client request id to connect to the web service to query up to date
Urls.

.PARAMETER DirectProxySettings

The direct proxy settings for priority traffic.

.PARAMETER DefaultProxySettings
```

The default proxy settings for non priority traffic.

.PARAMETER Type

The type of prioritization to give. Valid values are 1 and 2, which are 2 different modes of operation.

Type 1 will send Optimize traffic to the direct route. Type 2 will send Optimize and Allow traffic to the direct route.

.PARAMETER Lowercase

Flag this to include lowercase transformation into the PAC file for the host name matching.

.PARAMETER TenantName

The tenant name to replace wildcardUrls in the webservice.

.PARAMETER ServiceAreas

The service areas to filter endpoints by in the webservice.

.PARAMETER FilePath

The file to print the content to.

.EXAMPLE

```
Get-TLEPacFile.ps1 -ClientRequestId b10c5ed1-bad1-445f-b386-b919946339a7 -  
DefaultProxySettings "PROXY 4.4.4.4:70" -FilePath type1.pac
```

.EXAMPLE

```
Get-TLEPacFile.ps1 -ClientRequestId b10c5ed1-bad1-445f-b386-b919946339a7 -  
Instance China -Type 2 -DefaultProxySettings "PROXY 4.4.4.4:70" -FilePath  
type2.pac
```

.EXAMPLE

```
Get-TLEPacFile.ps1 -ClientRequestId b10c5ed1-bad1-445f-b386-b919946339a7 -  
Instance Worldwide -Lowercase -TenantName tenantName -ServiceAreas  
Sharepoint
```

#>

```
#Requires -Version 2
```

```
[CmdletBinding(SupportsShouldProcess=$True)]  
Param (  
    [Parameter(Mandatory = $false)]  
    [ValidateSet('Worldwide', 'Germany', 'China', 'USGovDoD',  
    'USGovGCCHigh')]  
    [String] $Instance = "Worldwide",
```

```

[Parameter(Mandatory = $false)]
[ValidateNotNullOrEmpty()]
[guid] $ClientRequestId = [Guid]::NewGuid().Guid,

[Parameter(Mandatory = $false)]
[ValidateNotNullOrEmpty()]
[String] $DirectProxySettings = 'DIRECT',
[Parameter(Mandatory = $false)]
[ValidateNotNullOrEmpty()]
[String] $DefaultProxySettings = 'PROXY 10.10.10.10:8080',
[Parameter(Mandatory = $false)]
[ValidateRange(1, 2)]
[int] $Type = 1,
[Parameter(Mandatory = $false)]
[switch] $Lowercase = $false,
[Parameter(Mandatory = $false)]
[ValidateNotNullOrEmpty()]
[string] $TenantName,
[Parameter(Mandatory = $false)]
[ValidateSet('Exchange', 'SharePoint', 'Common', 'Skype')]
[string[]] $ServiceAreas,
[Parameter(Mandatory = $false)]
[ValidateNotNullOrEmpty()]
[string] $FilePath,
[Parameter(Mandatory = $false)]
[ValidateNotNullOrEmpty()]
[string] $CdnEdgeNodesFilePath
)

#####
##### Global constants #####
#####

$baseServiceUrl = "https://endpoints.office.com/endpoints/$Instance/?ClientRequestId={$ClientRequestId}"
$directProxyVarName = "direct"
$defaultProxyVarName = "proxyServer"
$bl = "`r`n"

#####
##### Functions to create PAC files #####
#####


```

```

function Get-PacClauses
{
    param(
        [Parameter(Mandatory = $false)]
        [string[]] $Urls,
        [Parameter(Mandatory = $true)]
        [ValidateNotNullOrEmpty()]
        [String] $ReturnVarName
    )

    if (!$Urls)
    {
        return ""
    }

    $clauses =  (($Urls | ForEach-Object { "shExpMatch(host, `"$_.`")" }) -Join "$bl      || ")
    @"
        if($clauses)
        {
            return $ReturnVarName;
        }
    "@
}

function Get-PacString
{
    param(
        [Parameter(Mandatory = $true)]
        [ValidateNotNullOrEmpty()]
        [array[]] $MapVarUrls
    )

    @@
    // This PAC file will provide proxy config to Microsoft 365 services
    // using data from the public web service for all endpoints
    function FindProxyForURL(url, host)
    {
        var $directProxyVarName = "$DirectProxySettings";
        var $defaultProxyVarName = "$DefaultProxySettings";

        $( if ($Lowercase) { "    host = host.toLowerCase(); " })

        $($($MapVarUrls | ForEach-Object { Get-PACClauses -ReturnVarName $_.Item1 -Urls $_.Item2 }) -Join "$bl$bl" )

        $( if (!$ServiceAreas -or $ServiceAreas.Contains('Skype')) { Get-TLEPacConfiguration })

        return $defaultProxyVarName;
    }
    "@ -replace "($bl){3,}","$bl$bl" # Collapse more than one blank line in the PAC file so it looks better.
}

```

```

}

#####
#### Functions to get and filter endpoints
#####
#####

function Get-TLEPacConfiguration {
    param ()
    $PreBlock = @"
// Don't Proxy Teams Live Events traffic

if(shExpMatch(host, "*.azureedge.net")
|| shExpMatch(host, "*.bmc.cdn.office.net")
|| shExpMatch(host, "*.ml.cdn.office.net")
|| shExpMatch(host, "*.media.azure.net"))
{
    var resolved_ip = dnsResolveEx(host);

"@
$TLESb = New-Object 'System.Text.StringBuilder'
$TLESb.Append($PreBlock) | Out-Null

    if (![string]::IsNullOrEmpty($CdnEdgeNodesFilePath) -and (Test-Path -Path $CdnEdgeNodesFilePath)) {
        $CdnData = Get-Content -Path $CdnEdgeNodesFilePath -Raw -ErrorAction SilentlyContinue | ConvertFrom-Json | Select-Object -ExpandProperty value | Where-Object { $_.name -eq 'Premium_Verizon' } | Select-Object -First 1 -ExpandProperty properties |
            Select-Object -ExpandProperty ipAddressGroups
        $CdnData | Select-Object -ExpandProperty ipv4Addresses | ForEach-Object {
            if ($TLESb.Length -eq $PreBlock.Length) {
                $TLESb.Append("        if(") | Out-Null
            }
            else {
                $TLESb.AppendLine() | Out-Null
                $TLESb.Append("        || ") | Out-Null
            }
            $TLESb.Append("isInNetEx(resolved_ip,
`"$( $_.BaseIpAddress ) / $( $_.prefixLength )`")") | Out-Null
        }
        $CdnData | Select-Object -ExpandProperty ipv6Addresses | ForEach-Object {
            if ($TLESb.Length -eq $PreBlock.Length) {
                $TLESb.Append("        if(") | Out-Null
            }
            else {
                $TLESb.AppendLine() | Out-Null
                $TLESb.Append("        || ") | Out-Null
            }
            $TLESb.Append("isInNetEx(resolved_ip,
`"$( $_.BaseIpAddress ) / $( $_.prefixLength )`")") | Out-Null
        }
    }
}

```

```

    }
    $AzureIPsUrl = Invoke-WebRequest -Uri "https://www.microsoft.com/en-us/download/confirmation.aspx?id=56519" -UseBasicParsing -ErrorAction SilentlyContinue |
        Select-Object -ExpandProperty Links | Select-Object -
        ExpandProperty href |
            Where-Object { $_.EndsWith('.json') -and $_ -match 'ServiceTags' }
    } | Select-Object -First 1
    if ($AzureIPsUrl) {
        Invoke-RestMethod -Uri $AzureIPsUrl -ErrorAction SilentlyContinue |
        Select-Object -ExpandProperty values |
            Where-Object { $_.name -eq 'AzureFrontDoor.Frontend' } | Select-Object -First 1 -ExpandProperty properties |
                Select-Object -ExpandProperty addressPrefixes | ForEach-Object {
                    if ($TLESb.Length -eq $PreBlock.Length) {
                        $TLESb.Append("      if(") | Out-Null
                    }
                    else {
                        $TLESb.AppendLine() | Out-Null
                        $TLESb.Append("      || ") | Out-Null
                    }
                    $TLESb.Append("isInNetEx(resolved_ip, `"$_.`")") | Out-Null
                }
            }
        if ($TLESb.Length -gt $PreBlock.Length) {
            $TLESb.AppendLine(")") | Out-Null
            $TLESb.AppendLine("      {") | Out-Null
            $TLESb.AppendLine("          return $directProxyVarName;") | Out-Null
        }
        $TLESb.AppendLine("      }") | Out-Null
    }
    else {
        $TLESb.AppendLine("      // no addresses found for service via script") | Out-Null
    }
    $TLESb.AppendLine("    }") | Out-Null
    return $TLESb.ToString()
}

function Get-Regex
{
    param(
        [Parameter(Mandatory = $true)]
        [ValidateNotNullOrEmpty()]
        [string] $Fqdn
    )

        return "^" + $Fqdn.Replace(".", "\.").Replace("*", ".*").Replace("?", ".?") + "$"
}

function Match-RegexList
{
    param(
        [Parameter(Mandatory = $true)]

```

```

    [ValidateNotNullOrEmpty()]
    [string] $ToMatch,

    [Parameter(Mandatory = $false)]
    [string[]] $MatchList
)

if (!$MatchList)
{
    return $false
}
foreach ($regex in $MatchList)
{
    if ($regex -ne $ToMatch -and $ToMatch -match (Get-Regex $regex))
    {
        return $true
    }
}
return $false
}

function Get-Endpoints
{
    $url = $baseServiceUrl
    if ($TenantName)
    {
        $url += "&TenantName=$TenantName"
    }
    if ($ServiceAreas)
    {
        $url += "&ServiceAreas=" + ($ServiceAreas -Join ",")
    }
    return Invoke-RestMethod -Uri $url
}

function Get-Urls
{
    param(
        [Parameter(Mandatory = $false)]
        [psobject[]] $Endpoints
    )

    if ($Endpoints)
    {
        return $Endpoints | Where-Object { $_.urls } | ForEach-Object {
            $_.urls } | Sort-Object -Unique
    }
    return @()
}

function Get-UrlVarTuple
{
    param(
        [Parameter(Mandatory = $true)]
        [ValidateNotNullOrEmpty()])

```

```

    [string] $VarName,
    [Parameter(Mandatory = $false)]
    [string[]] $Urls
)
return New-Object 'Tuple[string,string[]]'($VarName, $Urls)
}

function Get-MapVarUrls
{
    Write-Verbose "Retrieving all endpoints for instance $Instance from web
service."
    $Endpoints = Get-Endpoints

    if ($Type -eq 1)
    {
        $directUrls = Get-Urls ($Endpoints | Where-Object { $_.category -eq
"Optimize" })
        $nonDirectPriorityUrls = Get-Urls ($Endpoints | Where-Object {
$_.category -ne "Optimize" }) | Where-Object { Match-RegexList $_
$directUrls }
        return @(
            Get-UrlVarTuple -VarName $defaultProxyVarName -Urls
$nonDirectPriorityUrls
            Get-UrlVarTuple -VarName $directProxyVarName -Urls $directUrls
        )
    }
    elseif ($Type -eq 2)
    {
        $directUrls = Get-Urls ($Endpoints | Where-Object { $_.category -in
@("Optimize", "Allow")})
        $nonDirectPriorityUrls = Get-Urls ($Endpoints | Where-Object {
$_.category -notin @("Optimize", "Allow") }) | Where-Object { Match-
RegexList $_ $directUrls }
        return @(
            Get-UrlVarTuple -VarName $defaultProxyVarName -Urls
$nonDirectPriorityUrls
            Get-UrlVarTuple -VarName $directProxyVarName -Urls $directUrls
        )
    }
}

#####
#####

### Main script
#####

$content = Get-PacString (Get-MapVarUrls)

if ($FilePath)
{
    $content | Out-File -FilePath $FilePath -Encoding ascii
}
else

```

```
{  
    $content  
}
```

The script will automatically parse the Azure list based on the [download URL](#) and keys off of **AzureFrontDoor.Frontend**, so there's no need to get that manually.

Again, we don't recommend performing VPN offload using just the FQDNs; utilizing **both** the FQDNs and the IP addresses in the function helps scope the use of this offload to a limited set of endpoints including Live Events/Stream. The way the function is structured will result in a DNS lookup being done for the FQDN that matches those listed by the client directly, i.e. DNS resolution of the remaining namespaces remains unchanged.

If you wish to limit the risk of offloading endpoints not related to Teams events and Stream, you can remove the *.azureedge.net domain from the configuration which is where most of this risk lies as this is a shared domain used for all Azure CDN customers. The downside of this is that any event using an external encoder powered by Stream won't be optimized, but events produced/organized within Teams will be.

3. Configure routing on the VPN to enable direct egress

The final step is to add a direct route for the Teams event IPs described in [Gathering the current lists of CDN Endpoints](#) into the VPN configuration to ensure the traffic isn't sent via the forced tunnel into the VPN. Detailed information on how to do this for Microsoft 365 Optimize endpoints can be found in the [Implement VPN split tunneling](#) section of [Implementing VPN split tunneling for Microsoft 365](#). The process is exactly the same for the Stream or Teams events IPs listed in this document.

Note that only the IPs (not FQDNs) from [Gathering the current lists of CDN Endpoints](#) should be used for VPN configuration.

FAQ

Will this send all my traffic to the service direct?

No, this will send the latency-sensitive streaming traffic for a Teams Event or Stream video direct, any other traffic will continue to use the VPN tunnel if they don't resolve to the IPs published.

Do I need to use the IPv6 Addresses?

No, the connectivity can be IPv4 only if required.

Why are these IPs not published in the Microsoft 365 URL/IP service?

Microsoft has strict controls around the format and type of information that is in the service to ensure customers can reliably use the information to implement secure and optimal routing based on endpoint category.

The **Default** endpoint category has no IP information provided for numerous reasons (Default endpoints might be outside of the control of Microsoft, might change too frequently, or might be in blocks shared with other elements). For this reason, Default endpoints are designed to be sent via FQDN to an inspecting proxy, like normal web traffic.

In this case, the above endpoints are CDNs that might be used by non-Microsoft controlled elements other than Live Events or Stream, and thus sending the traffic direct will also mean anything else which resolves to these IPs will also be sent direct from the client. Due to the unique nature of the current global crisis and to meet the short-term needs of our customers, Microsoft has provided the information above for customers to use as they see fit.

Microsoft is working to reconfigure the Teams events endpoints to allow them to be included in the Allow/Optimize endpoint categories in the future.

Do I only need to allow access to these IPs?

No, access to all of the **Required** marked endpoints in [the URL/IP service](#) is essential for the service to operate. In addition, any Optional endpoint marked for Stream (ID 41-45) is required.

What scenarios will this advice cover?

1. Live events produced within the Teams App
2. Viewing Stream hosted content
3. External device (encoder) produced events
4. Teams Town hall

Does this advice cover presenter traffic?

It doesn't; the advice above is purely for those consuming the service. Presenting from within Teams will see the presenter's traffic flowing to the Optimize marked UDP endpoints listed in URL/IP service row 11 with detailed VPN offload advice outlined in the [Implement VPN split tunneling](#) section of [Implementing VPN split tunneling for Microsoft 365](#).

Does this configuration risk traffic other than Town hall, Live Events & Stream being sent direct?

Yes, due to shared FQDNs used for some elements of the service, this is unavoidable. This traffic is normally sent via a corporate proxy which can apply inspection. In a VPN split tunnel scenario, using both the FQDNs and IPs will scope this risk down to a minimum, but it will still exist. Customers can remove the `*.azurededge.net` domain from the offload configuration and reduce this risk to a bare minimum but this will remove the offload of Stream-supported Live Events (Teams-scheduled, Stream encoder events, Viva Engage events produced in Teams, Viva Engage-scheduled Stream encoder events, and Stream scheduled events or on-demand viewing from Stream). Events scheduled and produced in Teams (including Town hall) are unaffected.

Related articles

[Overview: VPN split tunneling for Microsoft 365](#)

[Implementing VPN split tunneling for Microsoft 365](#)

[Common VPN split tunneling scenarios for Microsoft 365](#)

[Securing Teams media traffic for VPN split tunneling](#)

[Microsoft 365 performance optimization for China users](#)

[Microsoft 365 Network Connectivity Principles](#)

[Assessing Microsoft 365 network connectivity](#)

[Microsoft 365 network and performance tuning](#)

[Alternative ways for security professionals and IT to achieve modern security controls in today's unique remote work scenarios \(Microsoft Security Team blog\)](#) ↗

[Enhancing VPN performance at Microsoft: using Windows 10 VPN profiles to allow auto-on connections](#) ↗

[Running on VPN: How Microsoft is keeping its remote workforce connected](#) ↗

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Microsoft 365 global tenant performance optimization for China users

Article • 04/10/2024

ⓘ Important

This guidance is specific to usage scenarios in which **enterprise Microsoft 365 users located in China** connect to a **global Microsoft 365 tenant**. This guidance does **not** apply to tenants in Microsoft 365 operated by 21Vianet.

ⓘ Note

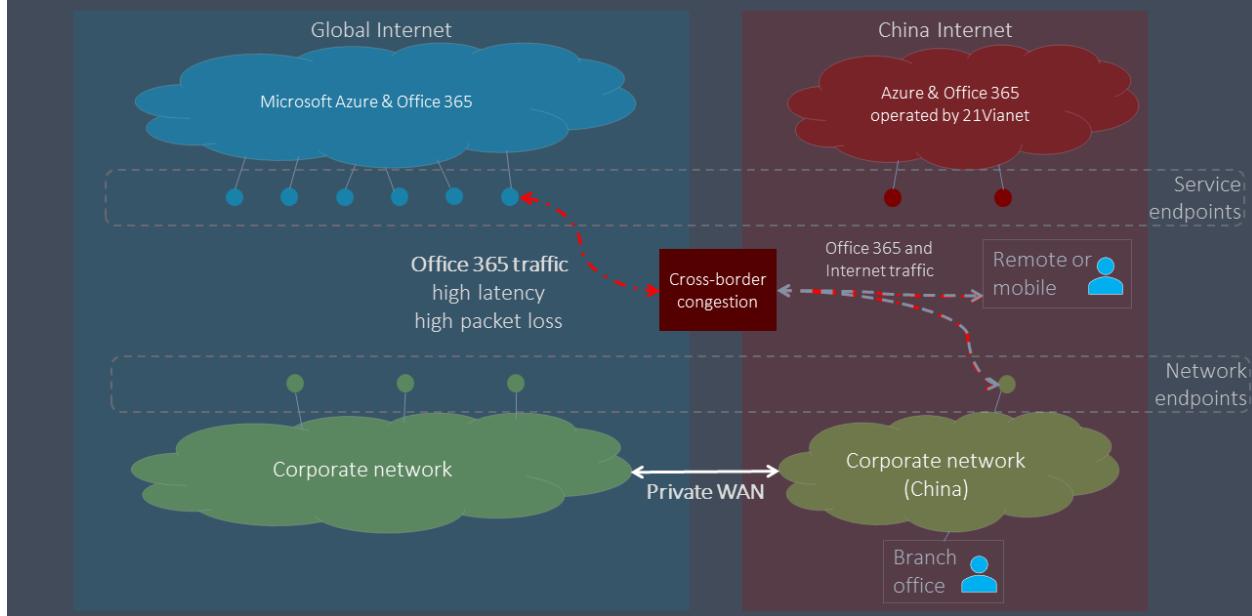
This article is part of a set of articles that address Microsoft 365 optimization for remote users.

- For an overview of using VPN split tunneling to optimize Microsoft 365 connectivity for remote users, see [Overview: VPN split tunneling for Microsoft 365](#).
- For detailed guidance on implementing VPN split tunneling, see [Implementing VPN split tunneling for Microsoft 365](#).
- For a detailed list of VPN split tunneling scenarios, see [Common VPN split tunneling scenarios for Microsoft 365](#).
- For guidance on securing Teams media traffic in VPN split tunneling environments, see [Securing Teams media traffic for VPN split tunneling](#).
- For information about how to configure Stream and live events in VPN environments, see [Special considerations for Stream and live events in VPN environments](#).

For enterprises with global Microsoft 365 tenants and a corporate presence in China, Microsoft 365 client performance for China-based users can be complicated by factors unique to China Telco's Internet architecture.

China ISPs have regulated offshore connections to the global public Internet that go through perimeter devices that are prone to high-levels of cross-border network congestion. This congestion creates packet loss and latency for all Internet traffic going into and out of China.

Global Office 365 access from China, unoptimized



Packet loss and latency are detrimental to the performance of network services, especially services that require large data exchanges (such as large file transfers) or requiring near real-time performance (audio and video applications).

The goal of this article is to provide best practices for mitigating the impact of China cross-border network congestion on Microsoft 365 services. This article doesn't address other common last-mile performance issues such as issues of high packet latency due to complex routing within China carriers.

Corporate network best practices

Many enterprises with global Microsoft 365 tenants and users in China have implemented private networks that carry corporate network traffic between China office locations and offshore locations around the world. These enterprises can leverage this network infrastructure to avoid cross-border network congestion and optimize their Microsoft 365 service performance in China.

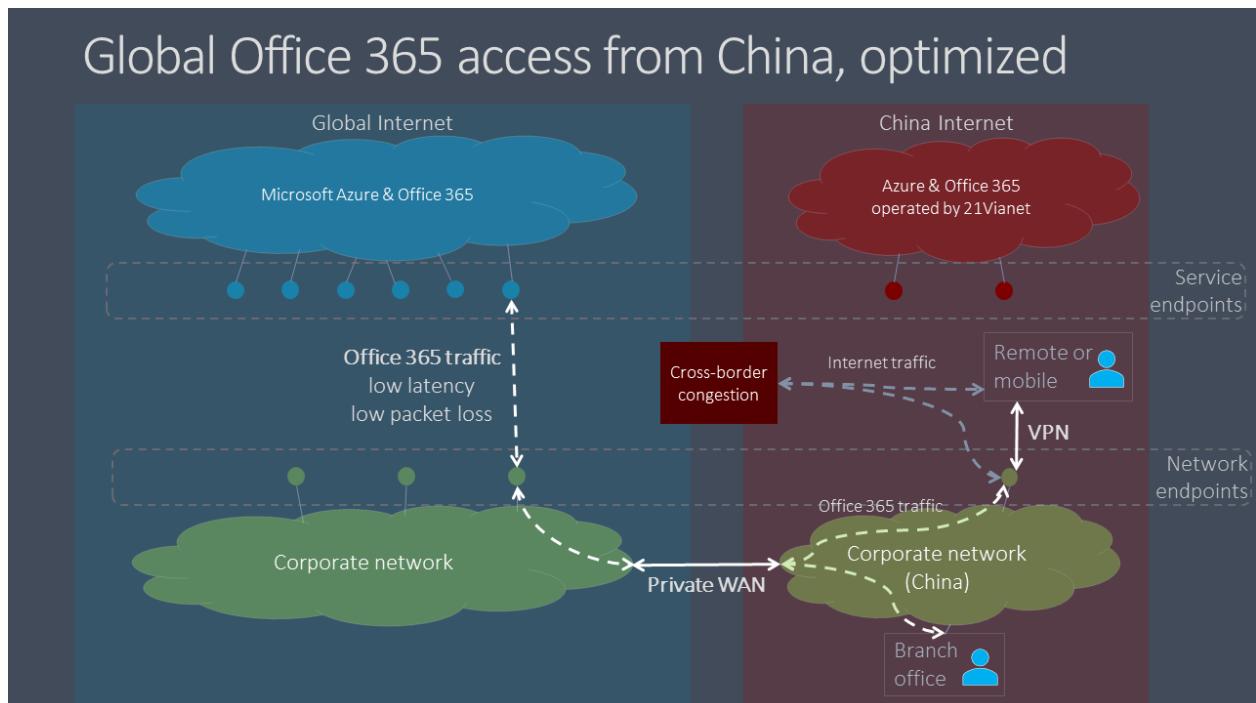
ⓘ Important

As with all private WAN implementations, you should always consult regulatory requirements for your country and/or region to ensure that your network configuration is in compliance.

As a first step, it's crucial that you follow our benchmark network guidance at [Network planning and performance tuning for Microsoft 365](#). The primary goal should be to avoid accessing global Microsoft 365 services from the Internet in China if possible.

- Leverage your existing private network to carry Microsoft 365 network traffic between China office networks and offshore locations that egress on the public Internet outside China. Almost any location outside China will provide a clear benefit. Network administrators can further optimize by egressing in areas with low-latency interconnect with the [Microsoft global network](#). Hong Kong Special Administrative Region, Singapore, Japan, and South Korea are examples.
- Configure user devices to access the corporate network over a VPN connection to allow Microsoft 365 traffic to transit the corporate network's private offshore link. Ensure that VPN clients are either not configured to use split tunneling, or that user devices are configured to ignore split tunneling for Microsoft 365 traffic. For additional information on optimizing VPN connectivity for Teams and real-time media traffic, see [this section](#).
- Configure your network to route all Microsoft 365 traffic across your private offshore link. If you must minimize the volume of traffic on your private link, you can choose to only route endpoints in the **Optimize** category, and allow requests to **Allow** and **Default** endpoints to transit the Internet. This improves performance and minimize bandwidth consumption by limiting optimized traffic to critical services that are most sensitive to high latency and packet loss.
- If possible, use UDP instead of TCP for live media streaming traffic, such as for Teams. UDP offers better live media streaming performance than TCP.

For information about how to selectively route Microsoft 365 traffic, see [Managing Office 365 endpoints](#). For a list of all worldwide Office 365 URLs and IP addresses, see [Office 365 URLs and IP address ranges](#).



User best practices

Users in China who connect to global Microsoft 365 tenants from remote locations such as homes, coffee shops, hotels, and branch offices with no connection to enterprise networks can experience poor network performance because traffic between their devices and Microsoft 365 must transit China's congested cross-border network circuits.

If cross-border private networks and/or VPN access into the corporate network aren't an option, per-user performance issues can still be mitigated by training your China-based users to follow these best practices.

- Utilize rich Office clients that support caching (Outlook, Teams, OneDrive, etc.), and avoid web-based clients. Office client caching and offline access features can dramatically reduce the impact of network congestion and latency.
- If your Microsoft 365 tenant has been configured with the *Audio Conferencing* feature, Teams users can join meetings via the public switched telephone network (PSTN). For more information, see [Audio Conferencing in Office 365](#).
- If users experience network performance issues, they should report to their IT department for troubleshooting, and escalate to Microsoft support if trouble with Microsoft 365 services is suspected. Not all issues are caused by cross-border network performance.

Optimizing Microsoft Teams meetings network performance for users in China

For organizations with global Microsoft 365 tenants and a presence in China, Microsoft 365 client performance for China-based users can be complicated by factors unique to the China Internet architecture. Many companies and schools have reported good results by following this guidance. However, the scope is limited to user network locations that are under control of the IT networking setup, for example, office locations or home/mobile endpoints with VPN connectivity. Microsoft Teams calls and meetings are often used from external locations, such as home offices, mobile locations, on the road, and coffee shops. Because calls and meetings rely on real-time media traffic, these Teams experiences are particularly sensitive to network congestion.

As a result, Microsoft has partnered with telecommunications providers to carry Teams and Skype for Business Online real-time media traffic using a higher-quality, preferential network path between domestic and public internet connections in China and the Teams and Skype services in the Microsoft 365 global cloud. This capability has resulted in a more than ten-fold improvement in packet loss and other key metrics impacting your user's experience.

 **Important**

Currently, these improvements do not address attending Microsoft Live Events meetings such as large broadcast or “town hall” style meetings using Teams or Microsoft Stream. The network improvements will benefit users who are presenting or producing a Live Events meeting, because that experience acts as a regular Teams meeting for the producer or presenter.

Organization network best practices for Teams meetings

You need to consider how to leverage these network improvements, given that the previous guidance to consider a private network extension to avoid cross-border network congestion. There are two general options for organization office networks:

1. Do nothing new. Continue to follow the earlier guidance around private network bypass to avoid cross-border congestion. Teams real-time media traffic will leverage that setup, as before.
2. Implement a split/hybrid pattern.
 - Use the previous guidance for all traffic flagged for optimization except Teams meetings and calling real-time media traffic.
 - Route Teams meeting and calling real-time media traffic over the public internet. See the following information for specifics on identifying the real-time media network traffic.

Sending Teams real-time media audio and video traffic over the public internet, which uses the higher quality connectivity, can result in considerable cost savings, because it's free versus paying to send that traffic over a private network. There might be similar additional benefits if users are also using SDWAN or VPN clients. Some organizations might also prefer to have more of their data traverse public internet connections as a general practice.

The same options could apply to SDWAN or VPN configurations. For example, a user is using an SDWAN or VPN to route Microsoft 365 traffic to the corporate network and then leveraging the private extension of that network to avoid cross-border congestion. The user's SDWAN or VPN can now be configured to exclude Teams meeting and calling real-time traffic from the VPN routing. This VPN configuration is referred to as split tunneling. See [VPN split tunneling for Office 365](#) for more information.

You can also continue to use your SDWAN or VPN for all Microsoft 365 traffic, including for Microsoft Teams real-time traffic. Microsoft has no recommendations on the use of SDWAN or VPN solutions.

Home, mobile, and user network best practices for Teams meetings

Users in China can take advantage of these improvements simply by connecting to the public internet service in China with a landline or mobile connection. Teams real-time media audio and video traffic on the public internet directly benefits from improved connectivity and quality.

However, data from other Microsoft 365 services — and other traffic in Teams, such as chat or files — won't directly benefit from these improvements. Users outside the organization network might still experience poor network performance for this traffic. As discussed in this article, you can mitigate these effects by using a VPN or SDWAN. You can also have your users use rich desktop clients over web clients, which support in-app caching to mitigate network issues.

Identifying Teams real-time media network traffic

For configuring a network device or a VPN/SDWAN setup, you need to exclude only the Teams real-time media audio and video traffic. The traffic details can be found for ID 11 on the official list of [Office 365 URLs and IP address ranges](#). All other network configurations should remain as-is.

Microsoft is continually working to improve the Microsoft 365 user experience and the performance of clients over the widest possible range of network architectures and characteristics. Visit the [Office 365 Networking Tech Community](#) to start or join a conversation, find resources, and submit feature requests and suggestions

Related articles

[Overview: VPN split tunneling for Microsoft 365](#)

[Implementing VPN split tunneling for Microsoft 365](#)

[Common VPN split tunneling scenarios for Microsoft 365](#)

[Securing Teams media traffic for VPN split tunneling](#)

[Special considerations for Stream and live events in VPN environments](#)

[Microsoft 365 Network Connectivity Principles](#)

[Assessing Microsoft 365 network connectivity](#)

Microsoft 365 network and performance tuning

Alternative ways for security professionals and IT to achieve modern security controls in today's unique remote work scenarios (Microsoft Security Team blog) ↗

Enhancing VPN performance at Microsoft: using Windows 10 VPN profiles to allow auto-on connections ↗

Running on VPN: How Microsoft is keeping its remote workforce connected ↗

Microsoft global network

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Optimize Microsoft 365 traffic for remote workers with the Windows VPN client

Article • 05/06/2024 • Applies to: Windows 11, Windows 10

This article describes how to configure the recommendations in the article [VPN split tunneling for Microsoft 365](#) for the Windows VPN client. This guidance enables VPN administrators to optimize Microsoft 365 usage while ensuring that all other traffic goes over the VPN connection and through existing security gateways or tooling.

The recommendations can be implemented for the built-in Windows VPN client using a *Force Tunneling with Exclusions* approach, defining IP-based exclusions even when using *force tunneling*. Certain traffic can be *split* to use the physical interface, while still forcing all other traffic via the VPN interface. Traffic addressed to defined destinations (like those listed in the Microsoft 365 optimized categories) follows a much more direct and efficient path, without the need to traverse or *hairpin* via the VPN tunnel and back out of the organization's network. For cloud-services like Microsoft 365, this makes a significant difference in performance and usability for remote users.

Note

The term *force tunneling with exclusions* is sometimes confusingly called *split tunnels* by other vendors and in some online documentation. For Windows VPN, the term *split tunneling* is defined differently, as described in the article [VPN routing decisions](#).

Solution Overview

The solution is based upon the use of a VPN Configuration Service Provider Reference profile ([VPNV2 CSP](#)) and the embedded [ProfileXML](#). These are used to configure the VPN profile on the device. Various provisioning approaches can be used to create and deploy the VPN profile as discussed in the article [Step 6. Configure Windows 10 client Always On VPN connections](#).

Typically, these VPN profiles are distributed using a Mobile Device Management solution like Intune, as described in [VPN profile options](#) and [Configure the VPN client by using Intune](#).

To enable the use of force tunneling in Windows 10 or Windows 11 VPN, the `<RoutingPolicyType>` setting is typically configured with a value of `ForceTunnel` in your existing Profile XML (or script) by way of the following entry, under the `<NativeProfile>` `</NativeProfile>` section:

XML

```
<RoutingPolicyType>ForceTunnel</RoutingPolicyType>
```

In order to define specific force tunnel exclusions, you then need to add the following lines to your existing Profile XML (or script) for each required exclusion, and place them outside of the `<NativeProfile>` `</NativeProfile>` section as follows:

XML

```
<Route>
  <Address>[IP addresses or subnet]</Address>
  <PrefixSize>[IP Prefix]</PrefixSize>
  <ExclusionRoute>true</ExclusionRoute>
</Route>
```

Entries defined by the `[IP Addresses or Subnet]` and `[IP Prefix]` references will consequently be added to the routing table as *more specific route entries* that will use the Internet-connected interface as the default gateway, as opposed to using the VPN interface. You must define a unique and separate `<Route>` `</Route>` section for each required exclusion.

An example of a correctly formatted Profile XML configuration for force tunnel with exclusions is the following:

XML

```
<VPNProfile>
  <NativeProfile>
    <RoutingPolicyType>ForceTunnel</RoutingPolicyType>
  </NativeProfile>
  <Route>
    <Address>203.0.113.0</Address>
    <PrefixSize>24</PrefixSize>
    <ExclusionRoute>true</ExclusionRoute>
  </Route>
  <Route>
    <Address>198.51.100.0</Address>
    <PrefixSize>22</PrefixSize>
    <ExclusionRoute>true</ExclusionRoute>
```

```
</Route>  
</VPNProfile>
```

ⓘ Note

The IP addresses and prefix size values in this example are used purely as examples only and should not be used.

Solution Deployment

For Microsoft 365, it's therefore necessary to add exclusions for all IP addresses documented within the optimize categories described in [Office 365 URLs and IP address ranges](#) to ensure that they're excluded from VPN force tunneling.

This can be achieved manually by adding the IP addresses defined within the *optimize* category entries to an existing Profile XML (or script) file, or alternatively the following script can be used which dynamically adds the required entries to an existing PowerShell script, or XML file, based upon directly querying the REST-based web service to ensure the correct IP address ranges are always used.

An example of a PowerShell script that can be used to update a force tunnel VPN connection with Microsoft 365 exclusions is provided below.

PowerShell

```
# Copyright (c) Microsoft Corporation. All rights reserved.  
#  
# THIS SAMPLE CODE AND INFORMATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF  
ANY KIND,  
# WHETHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED  
# WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE.  
# IF THIS CODE AND INFORMATION IS MODIFIED, THE ENTIRE RISK OF USE OR  
RESULTS IN  
# CONNECTION WITH THE USE OF THIS CODE AND INFORMATION REMAINS WITH THE  
USER.  
  
<#  
.SYNOPSIS  
    Applies or updates recommended Microsoft 365 optimize IP address  
exclusions to an existing force tunnel Windows 10 and Windows 11 VPN profile  
.DESCRIPTION  
    Connects to the Microsoft 365 worldwide commercial service instance  
endpoints to obtain the latest published IP address ranges  
    Compares the optimized IP addresses with those contained in the supplied  
VPN Profile (PowerShell or XML file)  
    Adds or updates IP addresses as necessary and saves the resultant file
```

```

with "-NEW" appended to the file name
.PARAMETERS
    Filename and path for a supplied Windows 10 or Windows 11 VPN profile
    file in either PowerShell or XML format
.NOTES
    Requires at least Windows 10 Version 1803 with KB4493437, 1809 with
    KB4490481, or later
.VERSION
    1.0
#>

param (
    [string]$VPNprofilefile
)

$usage=@"

```

This script uses the following parameters:

VPNprofilefile - The full path and name of the VPN profile PowerShell script
or XML file

EXAMPLES

To check a VPN profile PowerShell script file:

```
Update-VPN-Profile-Office365-Exclusion-Routes.ps1 -VPNprofilefile [FULLPATH
AND NAME OF POWERSHELL SCRIPT FILE]
```

To check a VPN profile XML file:

```
Update-VPN-Profile-Office365-Exclusion-Routes.ps1 -VPNprofilefile [FULLPATH
AND NAME OF XML FILE]
```

```
"@

# Check if filename has been provided #
if ($VPNprofilefile -eq "")
{
    Write-Host "`nWARNING: You must specify either a PowerShell script or XML
filename!" -ForegroundColor Red

    $usage
    exit
}

$FileExtension = [System.IO.Path]::GetExtension($VPNprofilefile)

# Check if XML file exists and is a valid XML file #
if ( $VPNprofilefile -ne "" -and $FileExtension -eq ".xml")
{
    if ( Test-Path $VPNprofilefile )
    {
        $xml = New-Object System.Xml.XmlDocument
        try
```

```

    {
        $xml.Load((Get-ChildItem -Path $VPNprofilefile).FullName)

    }
    catch [System.Xml.XmlException]
    {
        Write-Verbose "$VPNprofilefile : $($_.ToString())"
        Write-Host "`nWARNING: The VPN profile XML file is not a valid
xml file or incorrectly formatted!" -ForegroundColor Red
        $usage
        exit
    }
}else
{
    Write-Host "`nWARNING: VPN profile XML file does not exist or cannot
be found!" -ForegroundColor Red
    $usage
    exit
}
}

# Check if VPN profile PowerShell script file exists and contains a
VPNPROFILE XML section #
if ( $VPNprofilefile -ne "" -and $FileExtension -eq ".ps1")
{
    if ( (Test-Path $VPNprofilefile) )
    {
        if (-Not $($Select-String -Path $VPNprofilefile -Pattern "
<VPNPROFILE>") )
        {
            Write-Host "`nWARNING: PowerShell script file does not contain a
valid VPN profile XML section or is incorrectly formatted!" -ForegroundColor
Red
            $usage
            exit
        }
    }else
    {
        Write-Host "`nWARNING: PowerShell script file does not exist or
cannot be found!" -ForegroundColor Red
        $usage
        exit
    }
}

# Define Microsoft 365 endpoints and service URLs #
$ws = "https://endpoints.office.com"
$baseServiceUrl = "https://endpoints.office.com"

# Path where client ID and latest version number will be stored #
$datapath = $Env:TEMP + "\endpoints_clientid_latestversion.txt"

# Fetch client ID and version if data file exists; otherwise create new file
#
if (Test-Path $datapath)

```

```

{
    $content = Get-Content $datapath
    $clientRequestId = $content[0]
    $lastVersion = $content[1]

} else
{
    $clientRequestId = [GUID]::NewGuid().Guid
    $lastVersion = "0000000000"
    $($clientRequestId, $lastVersion) | Out-File $datapath
}

# Call version method to check the latest version, and pull new data if
version number is different #
$version = Invoke-RestMethod -Uri ($ws + "/version?clientRequestId=" +
$clientRequestId)

if ($version[0].latest -gt $lastVersion)
{

    Write-Host
    Write-Host "A new version of Microsoft 365 worldwide commercial service
instance endpoints has been detected!" -ForegroundColor Cyan

    # Write the new version number to the data file #
    $($clientRequestId, $version[0].latest) | Out-File $datapath
}

# Invoke endpoints method to get the new data #
$uri = "$baseServiceUrl" + "/endpoints/worldwide?
clientRequestId=$clientRequestId"

# Invoke endpoints method to get the data for the VPN profile comparison #
$endpointSets = Invoke-RestMethod -Uri ($uri)
$Optimize = $endpointSets | Where-Object { $_.category -eq "Optimize" }
$optimizeIpsv4 = $Optimize.ips | Where-Object { ($_).contains(".") } | Sort-
Object -Unique

# Temporarily include additional IP address until Teams client update is
released
$optimizeIpsv4 += "13.107.60.1/32"

# Process PowerShell script file start #
if ($VPNprofilefile -ne "" -and $FileExtension -eq ".ps1")
{
    Write-host "`nStarting PowerShell script exclusion route check...`n" -
ForegroundColor Cyan

    # Clear Variables to allow re-run testing #

        $ARRVPN=$null          # Array to hold VPN addresses from VPN
profile PowerShell file #
        $In_Opt_Only=$null      # Variable to hold IP addresses that only
appear in the optimize list #
        $In_VPN_Only=$null      # Variable to hold IP addresses that only

```

```

appear in the VPN profile PowerShell file #

# Extract the Profile XML from the ps1 file #

$regex = '(?sm).**.<VPNProfile>\r?\n(.*)\r?\n</VPNProfile>.*'

# Create xml format variable to compare with the optimize list #

$xmlbody=(Get-Content -Raw $VPNprofilefile) -replace $regex, '$1'
$xmlbody=$xmlbody -replace '<VPNProfile>', "<VPNProfile>$xmlbody</VPNProfile>"

# Loop through each address found in VPNPROFILE XML section #
foreach ($Route in $VPNprofilexml.VPNProfile.Route)
{
    $VPNIP=$Route.Address+"/" +$Route.PrefixSize
    [array]$ARRVPN+=$VPNIP
}

# In optimize address list only #
$In_Opt_Only= $optimizeIpsv4 | Where {$ARRVPN -NotContains $_}

# In VPN list only #
$In_VPN_only =$ARRVPN | Where {$optimizeIpsv4 -NotContains $_}
[array]$Inpfile = get-content $VPNprofilefile

if ($In_Opt_Only.Count -gt 0 )
{
    Write-Host "Exclusion route IP addresses are unknown, missing, or
need to be updated in the VPN profile`n" -ForegroundColor Red

[int32]$insline=0

for ($i=0; $i -lt $Inpfile.count; $i++)
{
    if ($Inpfile[$i] -match "</NativeProfile>")
    {
        $insline += $i # Record the position of the line after the
NativeProfile section ends #
    }
}
$OFS = "`r`n"
foreach ($NewIP in $In_Opt_Only)
{
    # Add the missing IP address(es) #
    $IPInfo=$NewIP.Split("/")
    $InpFile[$insline] += $OFS+    <Route>
    $InpFile[$insline] += $OFS+
<Address>+$IPInfo[0].Trim()+"</Address>"
    $InpFile[$insline] += $OFS+
<PrefixSize>+$IPInfo[1].Trim()+"</PrefixSize>"
    $InpFile[$insline] += $OFS+
<ExclusionRoute>true</ExclusionRoute>
    $InpFile[$insline] += $OFS+    </Route>
}
# Update fileName and write new PowerShell file #

```

```

        $NewFileName=(Get-Item $VPNprofilefile).Basename + "-NEW.ps1"
        $OutFile=$(Split-Path $VPNprofilefile -Parent)+"\"+$NewFileName
        $InpFile | Set-Content $OutFile
        Write-Host "Exclusion routes have been added to VPN profile and
output to a separate PowerShell script file; the original file has not been
modified`n" -ForegroundColor Green
    }else
    {
        Write-Host "Exclusion route IP addresses are correct and up to date
in the VPN profile`n" -ForegroundColor Green
        $OutFile=$VPNprofilefile
    }

if ( $In_VPN_Only.Count -gt 0 )
{
    Write-Host "Unknown exclusion route IP addresses have been found in the
VPN profile`n" -ForegroundColor Yellow

    foreach ($OldIP in $In_VPN_Only)
    {
        [array]$Inpfile = get-content $Outfile
        $IPInfo=$OldIP.Split("/")
        Write-Host "Unknown exclusion route IP address"$IPInfo[0]"has
been found in the VPN profile - Do you wish to remove it? (Y/N)`n" -
ForegroundColor Yellow
        $matchstr=<Address>+$IPInfo[0].Trim()+"</Address>"
        $DelAns=Read-host
        if ($DelAns.ToUpper() -eq "Y")
        {
            [int32]$insline=0
            for ($i=0; $i -lt $Inpfile.count; $i++)
            {
                if ($Inpfile[$i] -match $matchstr)
                {
                    $insline += $i # Record the position of the
line for the string match #
                }
            }
            # Remove entries from XML #
            $InpFile[$insline-1]="REMOVETHISLINE"
            $InpFile[$insline]="REMOVETHISLINE"
            $InpFile[$insline+1]="REMOVETHISLINE"
            $InpFile[$insline+2]="REMOVETHISLINE"
            $InpFile[$insline+3]="REMOVETHISLINE"
            $InpFile=$InpFile | Where-Object {$_. -ne
"REMOVETHISLINE"}}

            # Update filename and write new PowerShell file #
            $NewFileName=(Get-Item $VPNprofilefile).Basename +
"-NEW.xml"
            $OutFile=$(Split-Path $VPNprofilefile -
Parent)+"\"+$NewFileName
            $Inpfile | Set-content $OutFile
            Write-Host "`nAddress"$IPInfo[0]"exclusion route has
been removed from the VPN profile and output to a separate PowerShell script

```

```

file; the original file has not been modified`n" -ForegroundColor Green

        }else
        {
            Write-Host "`nExclusion route IP address has *NOT* been
removed from the VPN profile`n" -ForegroundColor Green
        }
    }
}

# Process XML file start #
if ($VPNprofilefile -ne "" -and $FileExtension -eq ".xml")
{
    Write-host "`nStarting XML file exclusion route check...`n" -
ForegroundColor Cyan

    # Clear variables to allow re-run testing #
    $ARRVPN=$null          # Array to hold VPN addresses from the XML
file #
    $In_Opt_Only=$null      # Variable to hold IP Addresses that only
appear in optimize list #
    $In_VPN_Only=$null      # Variable to hold IP Addresses that only
appear in the VPN profile XML file #

    # Extract the Profile XML from the XML file #
    $regex = '(?sm).*^*<VPNProfile>\r?\n(.*)\r?\n</VPNProfile>.*'

    # Create xml format variable to compare with optimize list #
    $xmlbody=(Get-Content -Raw $VPNprofilefile) -replace $regex, '$1'
    [xml]$VPNRulesxml="$xmlbody"

    # Loop through each address found in VPNPROFILE file #
    foreach ($Route in $VPNRulesxml.VPNProfile.Route)
    {
        $VPNIP=$Route.Address+"/"+$Route.PrefixSize
        [array]$ARRVPN=$ARRVPN+$VPNIP
    }

    # In optimize address list only #
    $In_Opt_Only= $optimizeIpsv4 | Where {$ARRVPN -NotContains $_}

    # In VPN list only #
    $In_VPN_only =$ARRVPN | Where {$optimizeIpsv4 -NotContains $_}
    [System.Collections.ArrayList]$Inpfile = get-content $VPNprofilefile

    if ($In_Opt_Only.Count -gt 0 )
    {
        Write-Host "Exclusion route IP addresses are unknown, missing,
or need to be updated in the VPN profile`n" -ForegroundColor Red

        foreach ($NewIP in $In_Opt_Only)
        {
            # Add the missing IP address(es) #
            $IPInfo=$NewIP.Split("/")

```

```

        $routes += "<Route>`n"+`t<Address>"+$IPInfo[0].Trim()+"`n"
    </Address>`n"+`t<PrefixSize>"+$IPInfo[1].Trim()+"`n"
    </PrefixSize>`n"+`t<ExclusionRoute>true</ExclusionRoute>`n"+`n</Route>`n"
    }
    $inspoint = $Inpfile.IndexOf("</VPNProfile>")
    $Inpfile.Insert($inspoint,$routes)

    # Update filename and write new XML file #
    $NewFileName=(Get-Item $VPNprofilefile).Basename + "-NEW.xml"
    $OutFile=$(Split-Path $VPNprofilefile -Parent)+"\"+$NewFileName
    $Inpfile | Set-Content $OutFile
    Write-Host "Exclusion routes have been added to VPN profile and
output to a separate XML file; the original file has not been modified`n`n"
    -ForegroundColor Green

}else
{
    Write-Host "Exclusion route IP addresses are correct and up to
date in the VPN profile`n" -ForegroundColor Green
    $OutFile=$VPNprofilefile
}

if ( $In_VPN_Only.Count -gt 0 )
{
    Write-Host "Unknown exclusion route IP addresses found in the
VPN profile`n" -ForegroundColor Yellow

    foreach ($OldIP in $In_VPN_Only)
    {
        [array]$Inpfile = get-content $OutFile
        $IPInfo=$OldIP.Split("/")
        Write-Host "Unknown exclusion route IP
address"$IPInfo[0]"has been found in the VPN profile - Do you wish to remove
it? (Y/N)`n" -ForegroundColor Yellow
        $matchstr="<Route>"+"<Address>"+$IPInfo[0].Trim()+"`n"
        </Address>"+"<PrefixSize>"+$IPInfo[1].Trim()+"`n</PrefixSize>"+
        <ExclusionRoute>true</ExclusionRoute>`n</Route>`n"
        $DelAns=Read-host
        if ($DelAns.ToUpper() -eq "Y")
        {
            # Remove unknown IP address(es) #
            $inspoint = $Inpfile[0].IndexOf($matchstr)
            $Inpfile[0] = $Inpfile[0].Replace($matchstr,"`n")

            # Update filename and write new XML file #
            $NewFileName=(Get-Item $VPNprofilefile).Basename +
"-NEW.xml"
            $OutFile=$(Split-Path $VPNprofilefile -
Parent)+"\"+$NewFileName
            $Inpfile | Set-Content $OutFile
            Write-Host "`nAddress"$IPInfo[0]"exclusion route has
been removed from the VPN profile and output to a separate XML file; the
original file has not been modified`n" -ForegroundColor Green

    }else
}

```

```

        {
            Write-Host "`nExclusion route IP address has *NOT*
been removed from the VPN profile`n" -ForegroundColor Green
        }
    }
}

```

Other Considerations

You should also be able to adapt this approach to include necessary exclusions for other cloud-services that can be defined by known/static IP addresses; exclusions required for [Cisco WebEx](#) or [Zoom](#) are good examples.

Examples

An example of a PowerShell script that can be used to create a force tunnel VPN connection with Microsoft 365 exclusions is provided below, or refer to the guidance in [Create the ProfileXML configuration files](#) to create the initial PowerShell script:

PowerShell

```

# Copyright (c) Microsoft Corporation. All rights reserved.
#
# THIS SAMPLE CODE AND INFORMATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF
ANY KIND,
# WHETHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED
# WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE.
# IF THIS CODE AND INFORMATION IS MODIFIED, THE ENTIRE RISK OF USE OR
RESULTS IN
# CONNECTION WITH THE USE OF THIS CODE AND INFORMATION REMAINS WITH THE
USER.

<#
.SYNOPSIS
    Configures an AlwaysOn IKEv2 VPN Connection using a basic script
.DESCRIPTION
    Configures an AlwaysOn IKEv2 VPN Connection with proxy PAC information
and force tunneling
.PARAMETERS
    Parameters are defined in a ProfileXML object within the script itself
.NOTES
    Requires at least Windows 10 Version 1803 with KB4493437, 1809 with
KB4490481, or later
.VERSION
    1.0
#>

```

```
<!-- Define Key VPN Profile Parameters --#>
$ProfileName = 'Contoso VPN with Microsoft 365 Exclusions'
$ProfileNameEscaped = $ProfileName -replace ' ', '%20'

<!-- Define VPN ProfileXML --#>
$ProfileXML = '<VPNProfile>
    <RememberCredentials>true</RememberCredentials>
    <DnsSuffix>corp.contoso.com</DnsSuffix>
    <AlwaysOn>true</AlwaysOn>
    <TrustedNetworkDetection>corp.contoso.com</TrustedNetworkDetection>
<NativeProfile>
    <Servers>edge1.contoso.com</Servers>
    <RoutingPolicyType>ForceTunnel</RoutingPolicyType>
    <NativeProtocolType>IKEv2</NativeProtocolType>
    <Authentication>
        <MachineMethod>Certificate</MachineMethod>
    </Authentication>
</NativeProfile>
<Route>
    <Address>13.107.6.152</Address>
    <PrefixSize>31</PrefixSize>
    <ExclusionRoute>true</ExclusionRoute>
</Route>
<Route>
    <Address>13.107.18.10</Address>
    <PrefixSize>31</PrefixSize>
    <ExclusionRoute>true</ExclusionRoute>
</Route>
<Route>
    <Address>13.107.128.0</Address>
    <PrefixSize>22</PrefixSize>
    <ExclusionRoute>true</ExclusionRoute>
</Route>
<Route>
    <Address>23.103.160.0</Address>
    <PrefixSize>20</PrefixSize>
    <ExclusionRoute>true</ExclusionRoute>
</Route>
<Route>
    <Address>40.96.0.0</Address>
    <PrefixSize>13</PrefixSize>
    <ExclusionRoute>true</ExclusionRoute>
</Route>
<Route>
    <Address>40.104.0.0</Address>
    <PrefixSize>15</PrefixSize>
    <ExclusionRoute>true</ExclusionRoute>
</Route>
<Route>
    <Address>52.96.0.0</Address>
    <PrefixSize>14</PrefixSize>
    <ExclusionRoute>true</ExclusionRoute>
</Route>
<Route>
    <Address>131.253.33.215</Address>
```

```
<PrefixSize>32</PrefixSize>
<ExclusionRoute>true</ExclusionRoute>
</Route>
<Route>
<Address>132.245.0.0</Address>
<PrefixSize>16</PrefixSize>
<ExclusionRoute>true</ExclusionRoute>
</Route>
<Route>
<Address>150.171.32.0</Address>
<PrefixSize>22</PrefixSize>
<ExclusionRoute>true</ExclusionRoute>
</Route>
<Route>
<Address>191.234.140.0</Address>
<PrefixSize>22</PrefixSize>
<ExclusionRoute>true</ExclusionRoute>
</Route>
<Route>
<Address>204.79.197.215</Address>
<PrefixSize>32</PrefixSize>
<ExclusionRoute>true</ExclusionRoute>
</Route>
<Route>
<Address>13.107.136.0</Address>
<PrefixSize>22</PrefixSize>
<ExclusionRoute>true</ExclusionRoute>
</Route>
<Route>
<Address>40.108.128.0</Address>
<PrefixSize>17</PrefixSize>
<ExclusionRoute>true</ExclusionRoute>
</Route>
<Route>
<Address>52.104.0.0</Address>
<PrefixSize>14</PrefixSize>
<ExclusionRoute>true</ExclusionRoute>
</Route>
<Route>
<Address>104.146.128.0</Address>
<PrefixSize>17</PrefixSize>
<ExclusionRoute>true</ExclusionRoute>
</Route>
<Route>
<Address>150.171.40.0</Address>
<PrefixSize>22</PrefixSize>
<ExclusionRoute>true</ExclusionRoute>
</Route>
<Route>
<Address>13.107.60.1</Address>
<PrefixSize>32</PrefixSize>
<ExclusionRoute>true</ExclusionRoute>
</Route>
<Route>
<Address>13.107.64.0</Address>
```

```

<PrefixSize>18</PrefixSize>
<ExclusionRoute>true</ExclusionRoute>
</Route>
<Route>
    <Address>52.112.0.0</Address>
    <PrefixSize>14</PrefixSize>
    <ExclusionRoute>true</ExclusionRoute>
</Route>
<Route>
    <Address>52.120.0.0</Address>
    <PrefixSize>14</PrefixSize>
    <ExclusionRoute>true</ExclusionRoute>
</Route>
<Proxy>

<AutoConfigUrl>http://webproxy.corp.contoso.com/proxy.pac</AutoConfigUrl>
    </Proxy>
</VPNProfile>

<!-- Convert ProfileXML to Escaped Format --#>
$ProfileXML = $ProfileXML -replace '<', '&lt;'
$ProfileXML = $ProfileXML -replace '>', '&gt;'
$ProfileXML = $ProfileXML -replace '"', '&quot;'

<!-- Define WMI-to-CSP Bridge Properties --#>
$nodeCSPURI = './Vendor/MSFT/VPNv2'
$namespaceName = "root\cimv2\mdm\dmmap"
$className = "MDM_VPNv2_01"

<!-- Define WMI Session --#>
$session = New-CimSession

<!-- Detect and Delete Previous VPN Profile --#>
try
{
    $deleteInstances = $session.EnumerateInstances($namespaceName,
$className, $options)
    foreach ($deleteInstance in $deleteInstances)
    {
        $InstanceId = $deleteInstance.InstanceID
        if ("$InstanceId" -eq "$ProfileNameEscaped")
        {
            $session.DeleteInstance($namespaceName, $deleteInstance,
$options)
            $Message = "Removed $ProfileName profile $InstanceId"
            Write-Host "$Message"
        } else {
            $Message = "Ignoring existing VPN profile $InstanceId"
            Write-Host "$Message"
        }
    }
}
catch [Exception]
{
    $Message = "Unable to remove existing outdated instance(s) of

```

```

$ProfileName profile: $_
    Write-Host "$Message"
    exit
}

<#-- Create VPN Profile --#>
try
{
    $newInstance = New-Object
    Microsoft.Management.Infrastructure.CimInstance $className, $namespaceName
    $property =
    [Microsoft.Management.Infrastructure.CimProperty]::Create("ParentID",
    "$nodeCSPURI", 'String', 'Key')
    $newInstance.CimInstanceProperties.Add($property)
    $property =
    [Microsoft.Management.Infrastructure.CimProperty]::Create("InstanceID",
    "$ProfileNameEscaped", 'String', 'Key')
    $newInstance.CimInstanceProperties.Add($property)
    $property =
    [Microsoft.Management.Infrastructure.CimProperty]::Create("ProfileXML",
    "$ProfileXML", 'String', 'Property')
    $newInstance.CimInstanceProperties.Add($property)

    $session.CreateInstance($namespaceName, $newInstance, $options)
    $Message = "Created $ProfileName profile."
    Write-Host "$Message"
    Write-Host "$ProfileName profile summary:"
    $session.EnumerateInstances($namespaceName, $className, $options)
}
catch [Exception]
{
    $Message = "Unable to create $ProfileName profile: $_"
    Write-Host "$Message"
    exit
}

$Message = "Script Complete"
Write-Host "$Message"

```

An example of an [Intune-ready XML file](#) that can be used to create a force tunnel VPN connection with Microsoft 365 exclusions is provided below, or refer to the guidance in [Create the ProfileXML configuration files](#) to create the initial XML file.

Note

This XML is formatted for use with Intune and cannot contain any carriage returns or whitespace.

XML

```
<VPNProfile><RememberCredentials>true</RememberCredentials>
<DnsSuffix>corp.contoso.com</DnsSuffix><AlwaysOn>true</AlwaysOn>
<TrustedNetworkDetection>corp.contoso.com</TrustedNetworkDetection>
<NativeProfile><Servers>edge1.contoso.com</Servers>
<RoutingPolicyType>ForceTunnel</RoutingPolicyType>
<NativeProtocolType>IKEv2</NativeProtocolType><Authentication>
<MachineMethod>Certificate</MachineMethod></Authentication></NativeProfile>
<Route><Address>13.107.6.152</Address><PrefixSize>31</PrefixSize>
<ExclusionRoute>true</ExclusionRoute></Route><Route>
<Address>13.107.18.10</Address><PrefixSize>31</PrefixSize>
<ExclusionRoute>true</ExclusionRoute></Route><Route>
<Address>13.107.128.0</Address><PrefixSize>22</PrefixSize>
<ExclusionRoute>true</ExclusionRoute></Route><Route>
<Address>23.103.160.0</Address><PrefixSize>20</PrefixSize>
<ExclusionRoute>true</ExclusionRoute></Route><Route>
<Address>40.96.0.0</Address><PrefixSize>13</PrefixSize>
<ExclusionRoute>true</ExclusionRoute></Route><Route>
<Address>40.104.0.0</Address><PrefixSize>15</PrefixSize>
<ExclusionRoute>true</ExclusionRoute></Route><Route>
<Address>52.96.0.0</Address><PrefixSize>14</PrefixSize>
<ExclusionRoute>true</ExclusionRoute></Route><Route>
<Address>131.253.33.215</Address><PrefixSize>32</PrefixSize>
<ExclusionRoute>true</ExclusionRoute></Route><Route>
<Address>132.245.0.0</Address><PrefixSize>16</PrefixSize>
<ExclusionRoute>true</ExclusionRoute></Route><Route>
<Address>150.171.32.0</Address><PrefixSize>22</PrefixSize>
<ExclusionRoute>true</ExclusionRoute></Route><Route>
<Address>191.234.140.0</Address><PrefixSize>22</PrefixSize>
<ExclusionRoute>true</ExclusionRoute></Route><Route>
<Address>204.79.197.215</Address><PrefixSize>32</PrefixSize>
<ExclusionRoute>true</ExclusionRoute></Route><Route>
<Address>13.107.136.0</Address><PrefixSize>22</PrefixSize>
<ExclusionRoute>true</ExclusionRoute></Route><Route>
<Address>40.108.128.0</Address><PrefixSize>17</PrefixSize>
<ExclusionRoute>true</ExclusionRoute></Route><Route>
<Address>52.104.0.0</Address><PrefixSize>14</PrefixSize>
<ExclusionRoute>true</ExclusionRoute></Route><Route>
<Address>104.146.128.0</Address><PrefixSize>17</PrefixSize>
<ExclusionRoute>true</ExclusionRoute></Route><Route>
<Address>150.171.40.0</Address><PrefixSize>22</PrefixSize>
<ExclusionRoute>true</ExclusionRoute></Route><Route>
<Address>13.107.60.1</Address><PrefixSize>32</PrefixSize>
<ExclusionRoute>true</ExclusionRoute></Route><Route>
<Address>13.107.64.0</Address><PrefixSize>18</PrefixSize>
<ExclusionRoute>true</ExclusionRoute></Route><Route>
<Address>52.112.0.0</Address><PrefixSize>14</PrefixSize>
<ExclusionRoute>true</ExclusionRoute></Route><Route>
<Address>52.120.0.0</Address><PrefixSize>14</PrefixSize>
<ExclusionRoute>true</ExclusionRoute></Route><Proxy>
<AutoConfigUrl>http://webproxy.corp.contoso.com/proxy.pac</AutoConfigUrl>
</Proxy></VPNProfile>
```

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Azure ExpressRoute for Microsoft 365

Article • 03/15/2024

This article applies to Microsoft 365 Enterprise.

Learn how Azure ExpressRoute is used with Microsoft 365 and how to plan the network implementation project that will be required if you meet specific requirements for deploying Azure ExpressRoute for use with Microsoft 365.

Note

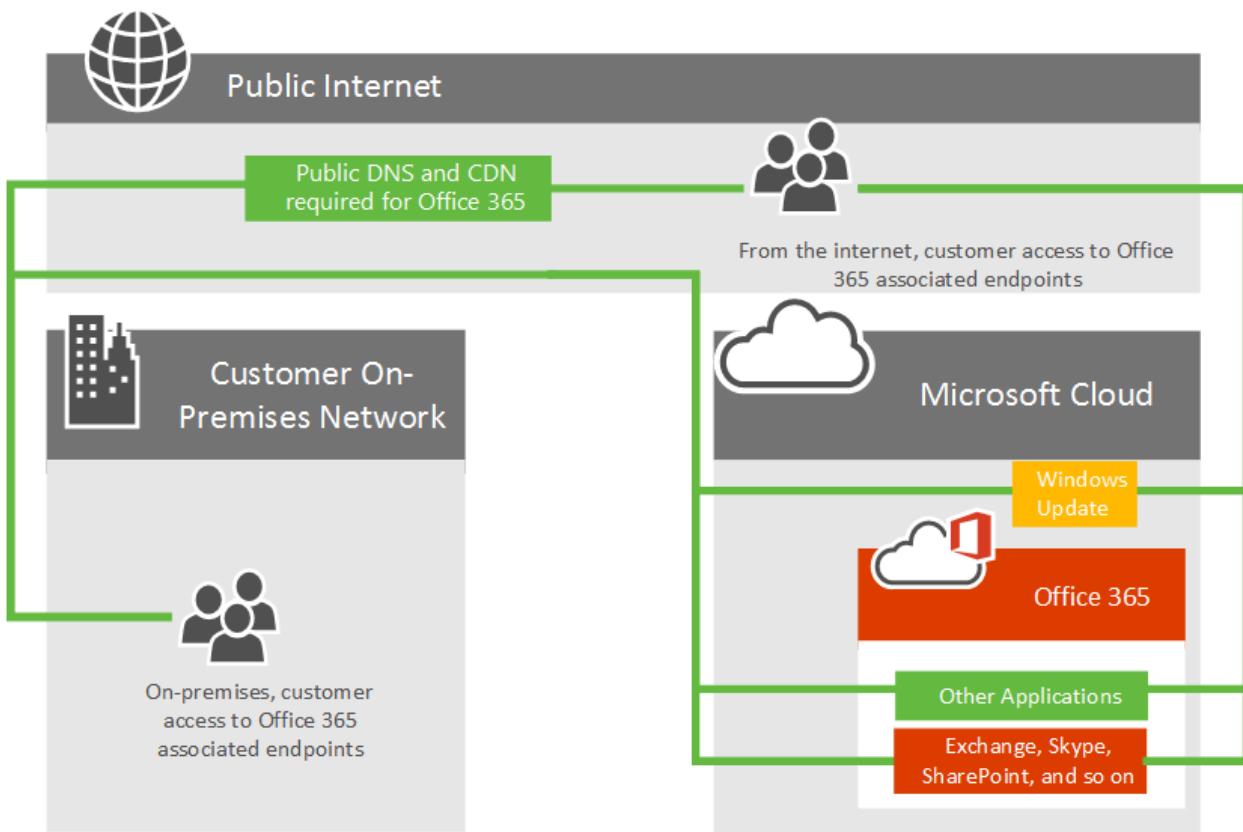
We **do not recommend** ExpressRoute for Microsoft 365 because it does not provide the best connectivity model for the service in most circumstances. As such, Microsoft authorization is required to use this connectivity model. We review every customer request and authorize ExpressRoute for Microsoft 365 only in the rare scenarios where it is necessary. Please read the [ExpressRoute for Microsoft 365 guide](#) for more information and following a comprehensive review of the document with your productivity, network, and security teams, work with your Microsoft account team to submit an exception if needed. Unauthorized subscriptions trying to create route filters for Microsoft 365 will receive an [error message](#).

Planning Azure ExpressRoute for Microsoft 365

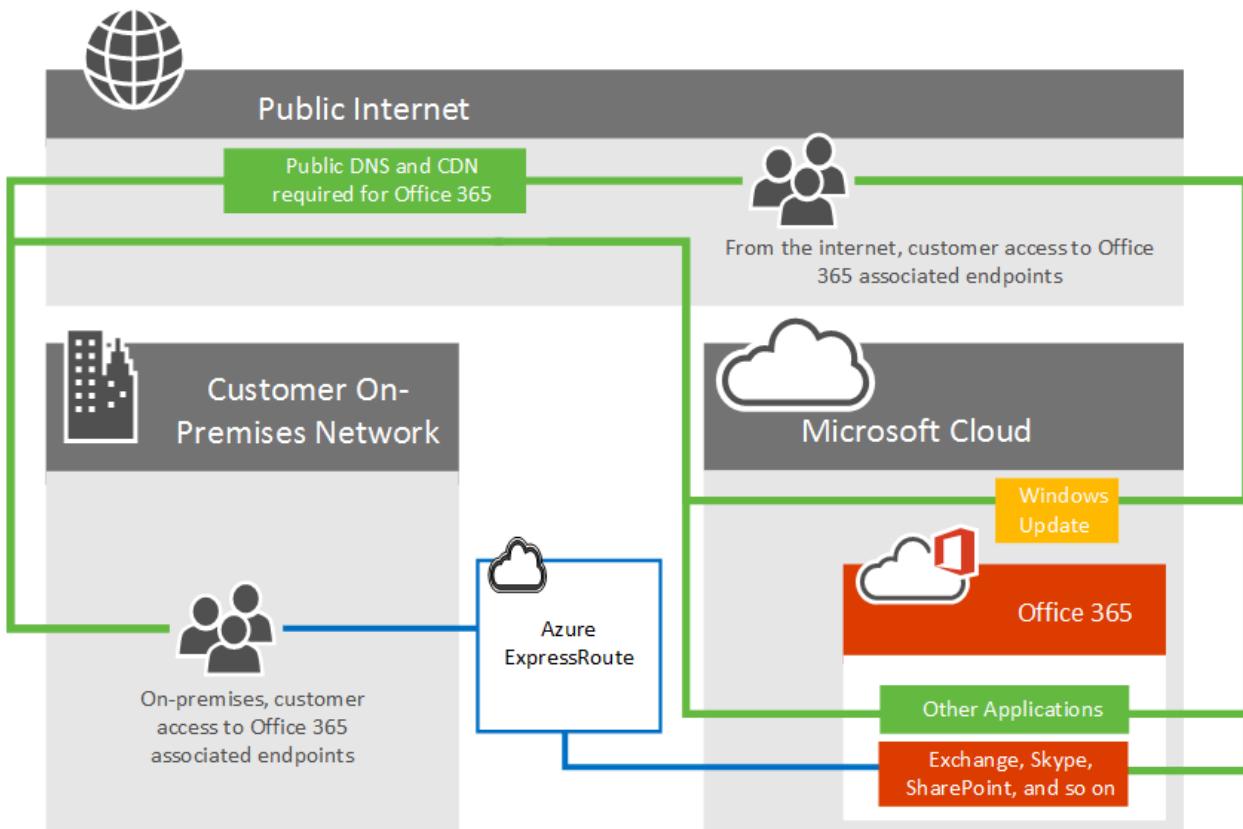
In addition to internet connectivity, you may choose to route a subset of your Microsoft 365 network traffic over Azure ExpressRoute.

Regardless of whether you have an existing MPLS WAN, ExpressRoute can be added to your network architecture in one of three ways; through a supported cloud exchange colocation provider, an Ethernet point-to-point connection provider, or through an MPLS connection provider. See what [providers are available in your region](#). The direct ExpressRoute connection enables connectivity to the applications outlined in [What Microsoft 365 services are included?](#). Network traffic for all other applications and services will continue to traverse the internet.

Consider the following high level network diagram, which shows a typical Microsoft 365 customer connecting to Microsoft's datacenters over the internet for access to all Microsoft applications such as Microsoft 365, Windows Update, and TechNet. Customers use a similar network path regardless of whether they're connecting from an on-premises network or from an independent internet connection.



Now look at the updated diagram, which depicts a Microsoft 365 customer who uses both the internet and ExpressRoute to connect to Microsoft 365. Notice that some connections such as Public DNS and Content Delivery Network nodes still require the public internet connection. Also notice the customer's users who aren't located in their ExpressRoute connected building are connecting over the Internet.



What Microsoft 365 services are included?

The following table lists the Microsoft 365 services that are supported over ExpressRoute. Review the [Microsoft 365 endpoints article](#) to understand which network requests for these applications require internet connectivity.

[] [Expand table](#)

Applications included
Exchange Online ¹ Exchange Online Protection ¹ Delve ¹
Skype for Business Online ¹ Microsoft Teams ¹
SharePoint ¹ OneDrive ¹ Project Online ¹
Portal and shared ¹ Microsoft Entra ID ¹ Microsoft Entra Connect ¹ Office ¹

¹ Each of these applications has internet connectivity requirements not supported over ExpressRoute. See the [Microsoft 365 endpoints article](#) for more information.

The services that aren't included with ExpressRoute for Microsoft 365 are Microsoft 365 Apps for enterprise client downloads, On-premises Identity Provider Sign-In, and Microsoft 365 (operated by 21 Vianet) service in China.

! Note

Microsoft Defender for Endpoint does not provide integration with Azure ExpressRoute. While this does not stop customers from defining ExpressRoute rules that enable connectivity from a private network to Microsoft Defender for Endpoint cloud services, it is up to the customer to maintain rules as the service or cloud infrastructure evolves.

Outlook for Android, iOS, and Mac do not support integration with Azure ExpressRoute and have a required IP range to function properly. As such, any rules that impact AutoDiscover services need to be maintained by the customer.

Implementing ExpressRoute for Microsoft 365

Implementing ExpressRoute requires the involvement of network and application owners and requires careful planning to determine the new [network routing architecture](#), bandwidth requirements, where security is implemented, high availability, and so on. To implement ExpressRoute, you'll need to:

1. Fully understand the need ExpressRoute satisfies in your Microsoft 365 connectivity planning. Understand what applications use the internet or ExpressRoute and fully plan your network capacity, security, and high availability needs in the context of using both the internet and ExpressRoute for Microsoft 365 traffic.
2. Determine the egress and peering locations for both internet and ExpressRoute traffic¹.
3. Determine the capacity required on the internet and ExpressRoute connections.
4. Have a plan in place for implementing security and other standard perimeter controls¹.
5. Have a valid Microsoft Azure account to subscribe to ExpressRoute.
6. Select a connectivity model and an [approved provider](#). Keep in mind, customers can select multiple connectivity models or partners and the partner doesn't need to be the same as your existing network provider.
7. Validate deployment prior to directing traffic to ExpressRoute.
8. Optionally [implement QoS](#) and evaluate regional expansion.

¹ Important performance considerations. Decisions here can dramatically impact latency, which is a critical for applications such as Skype for Business.

For additional references, see [What is Azure ExpressRoute?](#)

To purchase ExpressRoute for Microsoft 365, you'll need to work with one or more [approved providers](#) to provision the desired number and size circuits with an ExpressRoute Premium subscription. There are no additional licenses to purchase from Microsoft 365.

Here's a short link you can use to come back: <https://aka.ms/expressrouteoffice365>

Ready to sign up for [ExpressRoute for Microsoft 365](#)?

Related articles

[Assessing Microsoft 365 network connectivity](#)

[Implementing ExpressRoute for Microsoft 365](#)

[Media Quality and Network Connectivity Performance in Skype for Business Online ↗](#)

[Microsoft 365 performance tuning using baselines and performance history](#)

[Performance troubleshooting plan for Microsoft 365](#)

[Microsoft 365 URLs and IP address ranges](#)

[Microsoft 365 network and performance tuning](#)

See also

[Microsoft 365 Enterprise overview](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Implementing ExpressRoute for Microsoft 365

Article • 06/26/2024

This article applies to Microsoft 365 Enterprise.

ExpressRoute for Microsoft 365 provides an alternate routing path to many internet facing Microsoft 365 services. The architecture of ExpressRoute for Microsoft 365 is based on advertising public IP prefixes of Microsoft 365 services that are already accessible over the Internet into your provisioned ExpressRoute circuits for subsequent redistribution of those IP prefixes into your network. With ExpressRoute you effectively enable several different routing paths, through the internet and through ExpressRoute, for many Microsoft 365 services. This state of routing on your network might represent a significant change to how your internal network topology is designed.

Note

We **do not recommend** ExpressRoute for Microsoft 365 because it does not provide the best connectivity model for the service in most circumstances. As such, Microsoft authorization is required to use this connectivity model. We review every customer request and authorize ExpressRoute for Microsoft 365 only in the rare scenarios where it is necessary. Please read the [ExpressRoute for Microsoft 365 guide](#) for more information and following a comprehensive review of the document with your productivity, network, and security teams, work with your Microsoft account team to submit an exception if needed. Unauthorized subscriptions trying to create route filters for Microsoft 365 will receive an [error message](#).

You have to carefully plan your ExpressRoute for Microsoft 365 implementation to accommodate for the network complexities of having routing available via both a dedicated circuit with routes injected into your core network and the internet. If you and your team don't perform the detailed planning and testing in this guide, there's a high risk you'll experience intermittent or a total loss of connectivity to Microsoft 365 services when the ExpressRoute circuit is enabled.

To have a successful implementation, you'll need to analyze your infrastructure requirements, go through detailed network assessment and design, carefully plan the rollout in a staged and controlled manner, and build a detailed validation and testing

plan. For a large, distributed environment it's not uncommon to see implementations span several months. This guide is designed to help you plan ahead.

Large successful deployments might take six months in planning and often include team members from many areas in the organization including networking, Firewall and Proxy server administrators, Microsoft 365 administrators, security, end-user support, project management, and executive sponsorship. Your investment in the planning process will reduce the likelihood that you'll experience deployment failures resulting in downtime or complex and expensive troubleshooting.

We expect the following prerequisites to be completed before this implementation guide is started.

1. You've completed a network assessment to determine if ExpressRoute is recommended and approved.
2. You've selected an ExpressRoute network service provider. Find details about the [ExpressRoute partners and peering locations](#).
3. You've already read and understand the [ExpressRoute documentation](#) and your internal network is able to meet ExpressRoute prerequisites end to end.
4. Your team has read all of the public guidance and documentation at <https://aka.ms/expressrouteoffice365>, <https://aka.ms/ert>, and watched the [Azure ExpressRoute for Microsoft 365 Training](#) series on Channel 9 to gain an understanding of critical technical details including:
 - The internet dependencies of SaaS services.
 - How to avoid asymmetric routes and handle complex routing.
 - How to incorporate perimeter security, availability, and application level controls.

Begin by gathering requirements

Start by determining which features and services you plan to adopt within your organization. You need to determine which features of the different Microsoft 365 services will be used and which locations on your network will host people using those features. With the catalog of scenarios, you need to add the network attributes that each of those scenarios require; such as inbound and outbound network traffic flows and if the Microsoft 365 endpoints are available over ExpressRoute or not.

To gather your organization's requirements:

- Catalog the inbound and outbound network traffic for the Microsoft 365 services your organization is using. Consult Microsoft 365 URLs and IP address ranges page for the description of flows that different Microsoft 365 scenarios require.
- Gather documentation of existing network topology showing details of your internal WAN backbone and topology, connectivity of satellite sites, last mile user connectivity, routing to network perimeter egress points, and proxy services.
 - Identify inbound service endpoints on the network diagrams that Microsoft 365 and other Microsoft services will connect to, showing both internet and proposed ExpressRoute connection paths.
 - Identify all geographic user locations and WAN connectivity between locations along with which locations currently have an egress to the internet and which locations are proposed to have an egress to an ExpressRoute peering location.
 - Identify all edge devices, such as proxies, firewalls, and so on, and catalog their relationship to flows going over the Internet and ExpressRoute.
 - Document whether end users will access Microsoft 365 services via Direct Routing or indirect application proxy for both Internet and ExpressRoute flows.
- Add the location of your tenant and meet-me locations to your network diagram.
- Estimate the expected and observed network performance and latency characteristics from major user locations to Microsoft 365. Keep in mind that Microsoft 365 is a global and distributed set of services and users will be connecting to locations that may be different from the location of their tenant. For this reason, it's recommended to measure and optimize for latency between the user and the closest edge of Microsoft global network over ExpressRoute and Internet connections. You can use your findings from the network assessment to aid with this task.
- List company network security and high availability requirements that need to be met with the new ExpressRoute connection. For example, how do users continue to get access to Microsoft 365 in the event of the Internet egress or ExpressRoute circuit failure.
- Document which inbound and outbound Microsoft 365 network flows will use the Internet path and which will use ExpressRoute. The specifics of geographical locations of your users and details of your on-premises network topology may require the plan to be different from one user location to another.

Catalog your outbound and inbound network traffic

To minimize routing and other network complexities, we recommend that you only use ExpressRoute for Microsoft 365 for the network traffic flows that are required to go over a dedicated connection due to regulatory requirements or as the result of the network assessment. Additionally, we recommend that you stage the scope of ExpressRoute routing and approach outbound and inbound network traffic flows as different and distinct stages of the implementation project. Deploy ExpressRoute for Microsoft 365 for just user initiated outbound network traffic flows and leave inbound network traffic flows across the Internet can help to control the increase in topological complexity and risks of introducing additional asymmetric routing possibilities.

Your network traffic catalog should contain listings of all the inbound and outbound network connections that you'll have between your on-premises network and Microsoft.

- Outbound network traffic flows are any scenarios where a connection is initiated from your on-premises environment, such as from internal clients or servers, with a destination of the Microsoft services. These connections may be direct to Microsoft 365 or indirect, such as when the connection goes through proxy servers, firewalls, or other networking devices on the path to Microsoft 365.
- Inbound network traffic flows are any scenarios where a connection is initiated from the Microsoft cloud to an on-premises host. These connections typically need to go through firewall and other security infrastructure that customer security policy requires for externally originated flows.

Read the [Ensuring route symmetry](#) section to determine which services will send inbound traffic and look for the column marked **ExpressRoute for Microsoft 365** in the [Microsoft 365 endpoints](#)  reference article to determine the rest of the connectivity information.

For each service that requires an outbound connection, you'll want to describe the planned connectivity for the service including network routing, proxy configuration, packet inspection, and bandwidth needs.

For each service that requires an inbound connection, you'll need some additional information. Servers in the Microsoft cloud will establish connections to your on-premises network. To ensure the connections are made correctly, you'll want to describe all aspects of this connectivity, including; the public DNS entries for the services that will accept these inbound connections, the CIDR formatted IPv4 IP addresses, which ISP equipment is involved, and how inbound NAT or source NAT is handled for these connections.

Inbound connections should be reviewed regardless of whether they're connecting over the internet or ExpressRoute to ensure asymmetric routing hasn't been introduced. In

some cases, on-premises endpoints that Microsoft 365 services initiate inbound connections to might also need to be accessed by other Microsoft and non-Microsoft services. It's paramount that enabling ExpressRoute routing to these services for Microsoft 365 purposes doesn't break other scenarios. In many cases, customers might need to implement specific changes to their internal network, such as source-based NAT, to ensure that inbound flows from Microsoft remain symmetric after ExpressRoute is enabled.

Here's a sample of the level of detail required. In this case Exchange Hybrid would route to the on-premises system over ExpressRoute.

[\[+\] Expand table](#)

Connection property	Value
Network traffic direction	Inbound
Service	Exchange Hybrid
Public Microsoft 365 endpoint (source)	Exchange Online (IP addresses)
Public On-Premises Endpoint (destination)	5.5.5.5
Public (Internet) DNS entry	Autodiscover.contoso.com
Will this on-premises endpoint be used for by other (non-Microsoft 365) Microsoft services	No
Will this on-premises endpoint be used by users/systems on the Internet	Yes
Internal systems published through public endpoints	Exchange Server client access role (on-premises) 192.168.101, 192.168.102, 192.168.103
IP advertisement of the public endpoint	To Internet: 5.5.0.0/16 To ExpressRoute: 5.5.5.0/24
Security/Perimeter Controls	Internet path: DeviceID_002 ExpressRoute path: DeviceID_003
High Availability	Active/Active across 2 geo-redundant / ExpressRoute circuits - Chicago and Dallas
Path symmetry control	Method: Source NAT Internet path: Source NAT inbound connections to 192.168.5.5 ExpressRoute path: Source NAT

Connection property	Value
	connections to 192.168.1.0 (Chicago) and 192.168.2.0 (Dallas)

Here's a sample of a service that is outbound only:

[\[+\] Expand table](#)

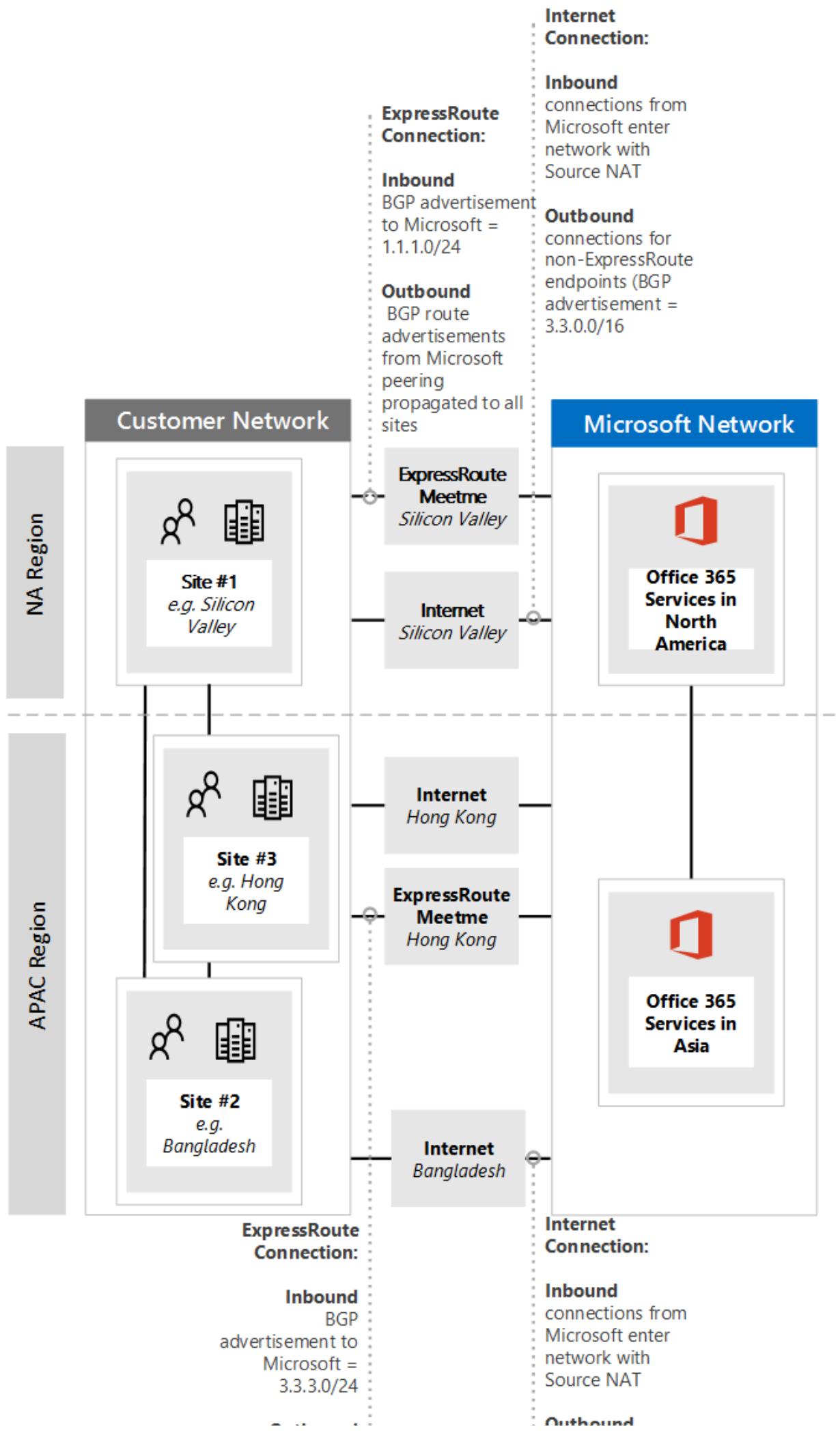
Connection property	Value
Network traffic direction	Outbound
Service	SharePoint
On-premises endpoint (source)	User workstation
Public Microsoft 365 endpoint (destination)	SharePoint (IP addresses)
Public (Internet) DNS entry	*.sharepoint.com (and more FQDNs)
CDN Referrals	cdn.sharepointonline.com (and more FQDNs) - IP addresses maintained by CDN providers
IP advertisement and NAT in use	Internet path/Source NAT: 1.1.1.0/24 ExpressRoute path/Source NAT: 1.1.2.0/24 (Chicago) and 1.1.3.0/24 (Dallas)
Connectivity method	Internet: via layer 7 proxy (.pac file) ExpressRoute: direct routing (no proxy)
Security/Perimeter Controls	Internet path: DeviceID_002 ExpressRoute path: DeviceID_003
High Availability	Internet path: Redundant internet egress ExpressRoute path: Active/Active 'hot potato' routing across 2 geo-redundant ExpressRoute circuits - Chicago and Dallas
Path symmetry control	Method: Source NAT for all connections

Your network topology design with regional connectivity

Once you understand the services and their associated network traffic flows, you can create a network diagram that incorporates these new connectivity requirements and illustrates the changes you'll make to use ExpressRoute for Microsoft 365. Your diagram should include:

1. All user locations where Microsoft 365 and other services will be accessed from.
2. All internet and ExpressRoute egress points.
3. All outbound and inbound devices that manage connectivity in and out of the network, including routers, firewalls, application proxy servers, and intrusion detection/prevention.
4. Internal destinations for all inbound traffic, such as internal ADFS servers that accept connections from the ADFS web application proxy servers.
5. Catalog of all IP subnets that will be advertised
6. Identify each location where people will access Microsoft 365 from and list the meet-me locations that will be used for ExpressRoute.
7. Locations and portions of your internal network topology, where Microsoft IP prefixes learned from ExpressRoute will be accepted, filtered, and propagated to.
8. The network topology should illustrate the geographic location of each network segment and how it connects to the Microsoft network over ExpressRoute and/or the Internet.

The diagram below shows each location where people will be using Microsoft 365 from along with the inbound and outbound routing advertisements to Microsoft 365.

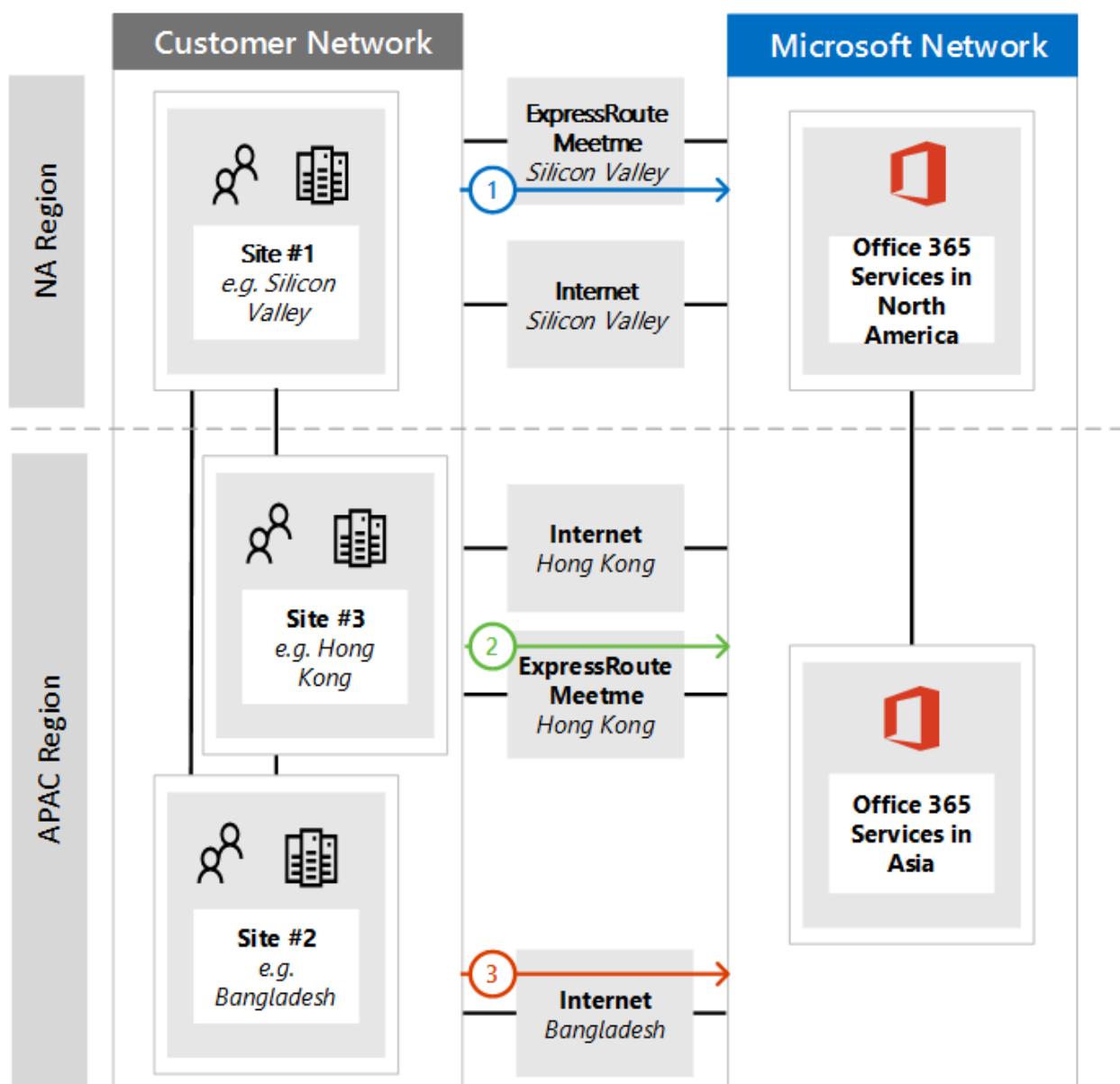


Outbound
BGP route
advertisements
from Microsoft
peering
propagated to all
sites

Outbound
connections for
non-
ExpressRoute
endpoints (BGP
advertisement =
2.2.0.0/16)

For outbound traffic, the people access Microsoft 365 in one of three ways:

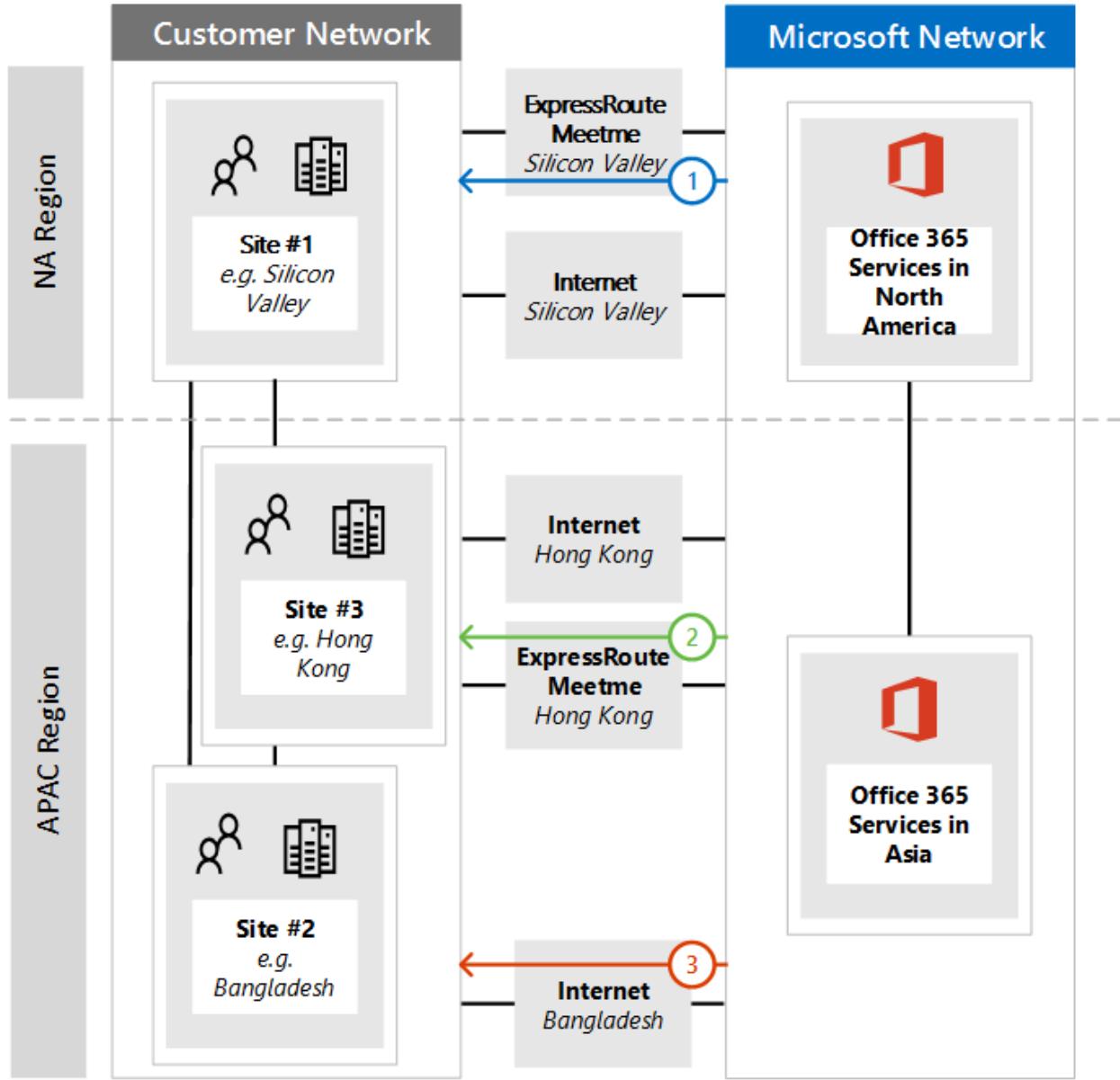
1. Through a meet-me location in North America for the people in California.
2. Through a meet-me location in Hong Kong Special Administrative Region for the people in Hong Kong SAR.
3. Through the internet in Bangladesh where there are fewer people and no ExpressRoute circuit provisioned.



Similarly, the inbound network traffic from Microsoft 365 returns in one of three ways:

1. Through a meet-me location in North America for the people in California.

2. Through a meet-me location in Hong Kong Special Administrative Region for the people in Hong Kong SAR.
3. Through the internet in Bangladesh where there are fewer people and no ExpressRoute circuit provisioned.



Determine the appropriate meet-me location

The selection of meet-me locations, which are the physical location where your ExpressRoute circuit connects your network to the Microsoft network, is influenced by the locations where people will access Microsoft 365 from. As a SaaS offering, Microsoft 365 doesn't operate under the IaaS or PaaS regional model in the same way Azure does. Instead, Microsoft 365 is a distributed set of collaboration services, where users might need to connect to endpoints across multiple datacenters and regions, which may not necessarily be in the same location or region where the user's tenant is hosted.

This means the most important consideration you need to make when selecting meet-me locations for ExpressRoute for Microsoft 365 is where the people in your organization will be connecting from. The general recommendation for optimal Microsoft 365 connectivity is to implement routing, so that user requests to Microsoft 365 services are handed off into the Microsoft network over the shortest network path, this is also often being referred to as 'hot potato' routing. For example, if most of the Microsoft 365 users are in one or two locations, selecting meet-me locations that are in the closest proximity to the location of those users will create the optimal design. If your company has large user populations in many different regions, you might want to consider having multiple ExpressRoute circuits and meet-me locations. For some of your user locations, the shortest/most optimal path into Microsoft network and Microsoft 365, might not be through your internal WAN and ExpressRoute meet-me points, but via the Internet.

Often, there are multiple meet-me locations that could be selected within a region with relative proximity to your users. Fill out the following table to guide your decisions.

Planned ExpressRoute meet-me locations in California and New York

[\[+\] Expand table](#)

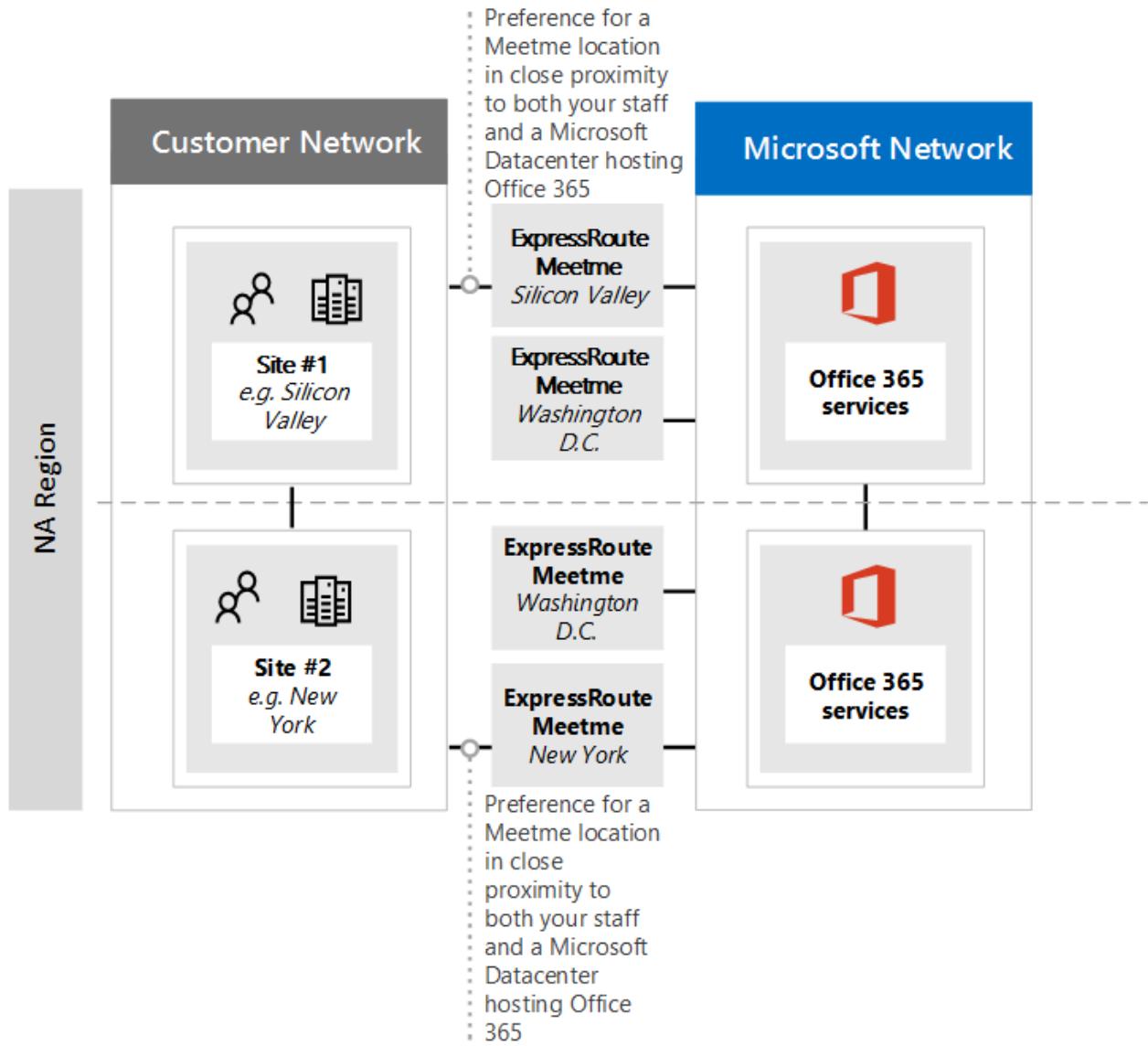
Location	Number of people	Expected latency to Microsoft network over Internet egress	Expected latency to Microsoft network over ExpressRoute
Los Angeles	10,000	~15ms	~10ms (via Silicon Valley)
Washington DC	15,000	~20ms	~10ms (via New York)
Dallas	5,000	~15ms	~40ms (via New York)

Once the global network architecture showing the Microsoft 365 region, ExpressRoute network service provider meet-me locations, and the quantity of people by location has been developed, it can be used to identify if any optimizations can be made. It may also show global hairpin network connections where traffic routes to a distant location in order to get the meet-me location. If a hairpin on the global network is discovered, it should be remediated before continuing. Either find another meet-me location, or use selective Internet breakout egress points to avoid the hairpin.

The first diagram shows an example of a customer with two physical locations in North America. You can see the information about office locations, Microsoft 365 tenant

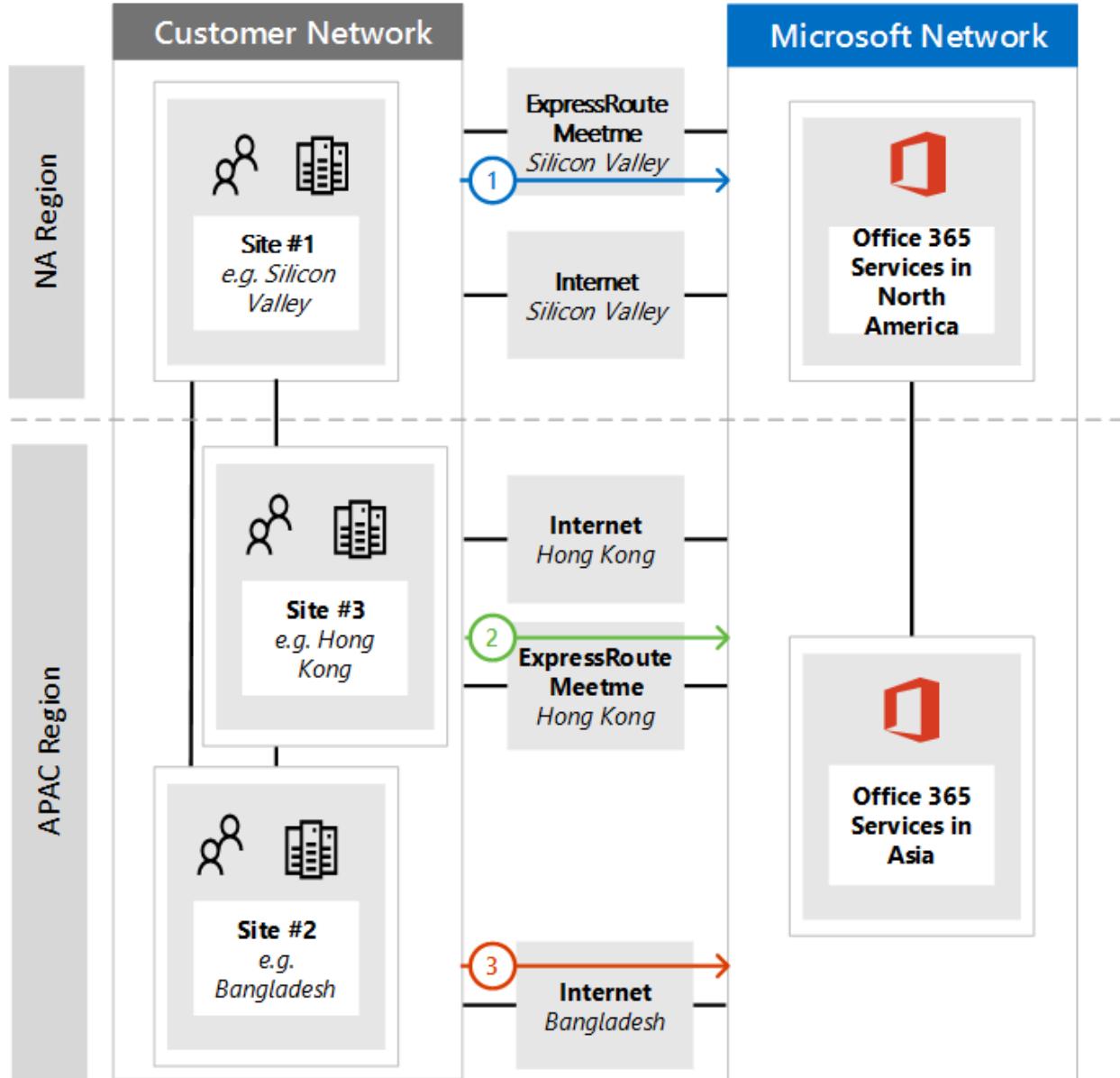
locations, and several choices for ExpressRoute meet-me locations. In this example, the customer has selected the meet-me location based on two principles, in order:

1. Closest proximity to the people in their organization.
2. Closest in proximity to a Microsoft datacenter where Microsoft 365 is hosted.



Expanding this concept slightly further, the second diagram shows an example multi-national customer faced with similar information and decision making. This customer has a small office in Bangladesh with only a small team of 10 people focused on growing their footprint in the region. There's a meet-me location in Chennai and a Microsoft datacenter with Microsoft 365 hosted in Chennai so a meet-me location would make sense; however, for 10 people, the expense of the extra circuit is burdensome. As you look at your network, you'll need to determine if the latency involved in sending your network traffic across your network is more effective than spending the capital to acquire another ExpressRoute circuit.

Alternatively, the 10 people in Bangladesh might experience better performance with their network traffic sent over the internet to the Microsoft network than they would routing on their internal network as we showed in the introductory diagrams and reproduced below.



Create your ExpressRoute for Microsoft 365 implementation plan

Your implementation plan should encompass both the technical details of configuring ExpressRoute and the details of configuring all the other infrastructure on your network, such as the following.

- Plan which services split between ExpressRoute and Internet.
- Plan for bandwidth, security, high availability, and failover.

- Design inbound and outbound routing, including proper routing path optimizations for different locations
- Decide how far ExpressRoute routes will be advertised into your network and what is the mechanism for clients to select Internet or ExpressRoute path; for example, direct routing or application proxy.
- Plan DNS record changes, including [Sender Policy Framework](#) entries.
- Plan NAT strategy including outbound and inbound source NAT.

Plan your routing with both internet and ExpressRoute network paths

- For your initial deployment, all inbound services, such as inbound email or hybrid connectivity, are recommended to use the internet.
- Plan end-user client LAN routing, such as [configuring a PAC/WPAD file](#), default route, proxy servers, and BGP route advertisements.
- Plan perimeter routing, including proxy servers, firewalls, and cloud proxies.

Plan your bandwidth, security, high availability, and failover

Create a plan for bandwidth required for each major Microsoft 365 workload. Separately estimate Exchange Online, SharePoint, and Skype for Business Online bandwidth requirements. You can use the estimation calculators we've provided for Exchange Online and Skype for Business as a starting place; however, a pilot test with a representative sample of the user profiles and locations is required to fully understand the bandwidth needs of your organization.

Add how security is handled at each internet and ExpressRoute egress location to your plan, remember all ExpressRoute connections to Microsoft 365 use public peering and must still be secured in accordance with your company security policies of connecting to external networks.

Add details to your plan about which people will be affected by what type of outage and how those people will be able to perform their work at full capacity in the simplest manner.

Plan bandwidth requirements including Skype for Business requirements on Jitter, Latency, Congestion, and Headroom

Skype for Business Online also has specific extra network requirements, which are detailed in the article [Media Quality and Network Connectivity Performance in Skype for Business Online ↗](#).

Read the section [Bandwidth planning for Azure ExpressRoute](#). When performing a bandwidth assessment with your pilot users, you can use our guide [Microsoft 365 performance tuning using baselines and performance history ↗](#).

Plan for high availability requirements

Create a plan for high availability to meet your needs and incorporate this into your updated network topology diagram. Read the section [High availability and failover with Azure ExpressRoute](#).

Plan for network security requirements

Create a plan to meet your network security requirements and incorporate this into your updated network topology diagram. Read the section [Applying security controls to Azure ExpressRoute for Microsoft 365 scenarios](#).

Design outbound service connectivity

ExpressRoute for Microsoft 365 has *outbound* network requirements that may be unfamiliar. Specifically, the IP addresses that represent your users and networks to Microsoft 365 and act as the source endpoints for outbound network connections to Microsoft must follow specific requirements outlined below.

1. The endpoints must be public IP addresses that are registered to your company or to carrier providing ExpressRoute connectivity to you.
2. The endpoints must be advertised to Microsoft and validated/accepted by ExpressRoute.
3. The endpoints must not be advertised to the Internet with the same or more preferred routing metric.
4. The endpoints must not be used for connectivity to Microsoft services that aren't configured over ExpressRoute.

If your network design doesn't meet these requirements, there's a high risk your users will experience connectivity failures to Microsoft 365 and other Microsoft services due to route black holing or asymmetric routing. This occurs when requests to Microsoft services are routed over ExpressRoute, but responses are routed back across the internet, or vice versa, and the responses are dropped by stateful network devices such as firewalls.

The most common method you can use to meet the above requirements is to use source NAT, either implemented as a part of your network or provided by your ExpressRoute carrier. Source NAT allows you to abstract the details and private IP addressing of your internet network from ExpressRoute and; coupled with proper IP route advertisements, provide an easy mechanism to ensure path symmetry. If you're using stateful network devices that are specific to ExpressRoute peering locations, you must implement separate NAT pools for each ExpressRoute peering to ensure path symmetry.

Read more about the [ExpressRoute NAT requirements](#).

Add the changes for the outbound connectivity to the network topology diagram.

Design inbound service connectivity

Most enterprise Microsoft 365 deployments assume some form of inbound connectivity from Microsoft 365 to on-premises services, such as for Exchange, SharePoint, and Skype for Business hybrid scenarios, mailbox migrations, and authentication using ADFS infrastructure. When ExpressRoute you enable an extra routing path between your on-premises network and Microsoft for outbound connectivity, these inbound connections might inadvertently be impacted by asymmetric routing, even if you intend to have those flows continue to use the Internet. A few precautions described below are recommended to ensure there's no impact to Internet based inbound flows from Microsoft 365 to on-premises systems.

To minimize the risks of asymmetric routing for inbound network traffic flows, all of the inbound connections should use source NAT before they're routed into segments of your network, which have routing visibility into ExpressRoute. If the incoming connections are allowed onto a network segment with routing visibility into ExpressRoute without source NAT, requests originating from Microsoft 365 will enter from the internet, but the response going back to Microsoft 365 will prefer the ExpressRoute network path back to the Microsoft network, causing asymmetric routing.

You might consider one of the following implementation patterns to satisfy this requirement:

1. Perform source NAT before requests are routed into your internal network using networking equipment such as firewalls or load balancers on the path from the Internet to your on-premises systems.
2. Ensure that ExpressRoute routes aren't propagated to the network segments where inbound services, such as front-end servers or reverse proxy systems, handling Internet connections reside.

Explicitly accounting for these scenarios in your network and keeping all inbound network traffic flows over the Internet helps to minimize deployment and operational risk of asymmetric routing.

There might be cases where you may choose to direct some inbound flows over ExpressRoute connections. For these scenarios, take the following extra considerations into account.

1. Microsoft 365 can only target on-premises endpoints that use public IPs. This means that even if the on-premises inbound endpoint is only exposed to Microsoft 365 over ExpressRoute, it still needs to have public IP associated with it.
2. All DNS name resolution that Microsoft 365 services perform to resolve on-premises endpoints happen using public DNS. This means that you must register inbound service endpoints' FQDN to IP mappings on the Internet.
3. In order to receive inbound network connections over ExpressRoute, the public IP subnets for these endpoints must be advertised to Microsoft over ExpressRoute.
4. Carefully evaluate these inbound network traffic flows to ensure that proper security and network controls are applied to them in accordance with your company security and network policies.
5. Once your on-premises inbound endpoints are advertised to Microsoft over ExpressRoute, ExpressRoute will effectively become the preferred routing path to those endpoints for all Microsoft services, including Microsoft 365. This means that those endpoint subnets must only be used for communications with Microsoft 365 services and no other services on the Microsoft network. Otherwise, your design will cause asymmetric routing where inbound connections from other Microsoft services prefer to route inbound over ExpressRoute, while the return path will use the Internet.
6. In the event an ExpressRoute circuit or meet-me location is down, you'll need to ensure the on-premises inbound endpoints are still available to accept requests over a separate network path. This may mean advertising subnets for those endpoints through multiple ExpressRoute circuits.

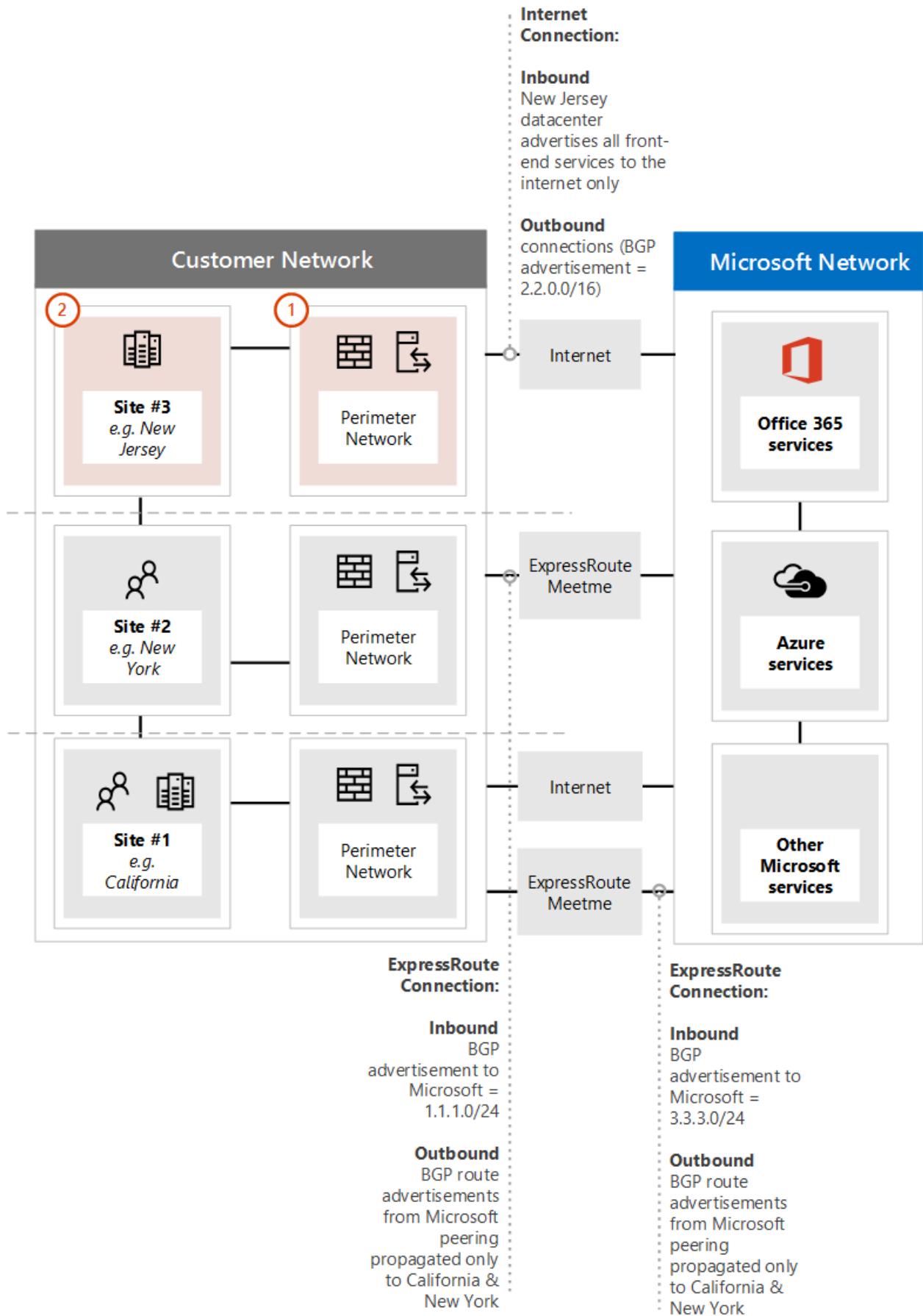
7. We recommend applying source NAT for all inbound network traffic flows entering your network through ExpressRoute, especially when these flows cross stateful network devices such as firewalls.
8. Some on-premises services, such as ADFS proxy or Exchange autodiscover, may receive inbound requests from both Microsoft 365 services and users from the Internet. For these requests Microsoft 365 will target the same FQDN as user requests over the Internet. Allowing inbound user connections from the internet to those on-premises endpoints, while forcing Microsoft 365 connections to use ExpressRoute, represents significant routing complexity. For the vast majority of customers implementing such complex scenarios over ExpressRoute isn't recommended due to operational considerations. This additional overhead includes, managing risks of asymmetric routing and will require you to carefully manage routing advertisements and policies across multiple dimensions.

Update your network topology plan to show how you would avoid asymmetric routes

You want to avoid asymmetric routing to ensure people in your organization can seamlessly use Microsoft 365 as well as other important services on the internet. There are two common configurations customers have that cause asymmetric routing. Now's a good time to review the network configuration you're planning to use and check if one of these asymmetric routing scenarios could exist.

To begin, we'll examine a few different situations associated with the following network diagram. In this diagram, all servers that receive inbound requests, such as ADFS or on-premises hybrid servers are in the New Jersey data center and are advertised to the internet.

1. While the perimeter network is secure, there's no Source NAT available for incoming requests.
2. The servers in the New Jersey data center are able to see both internet and ExpressRoute routes.

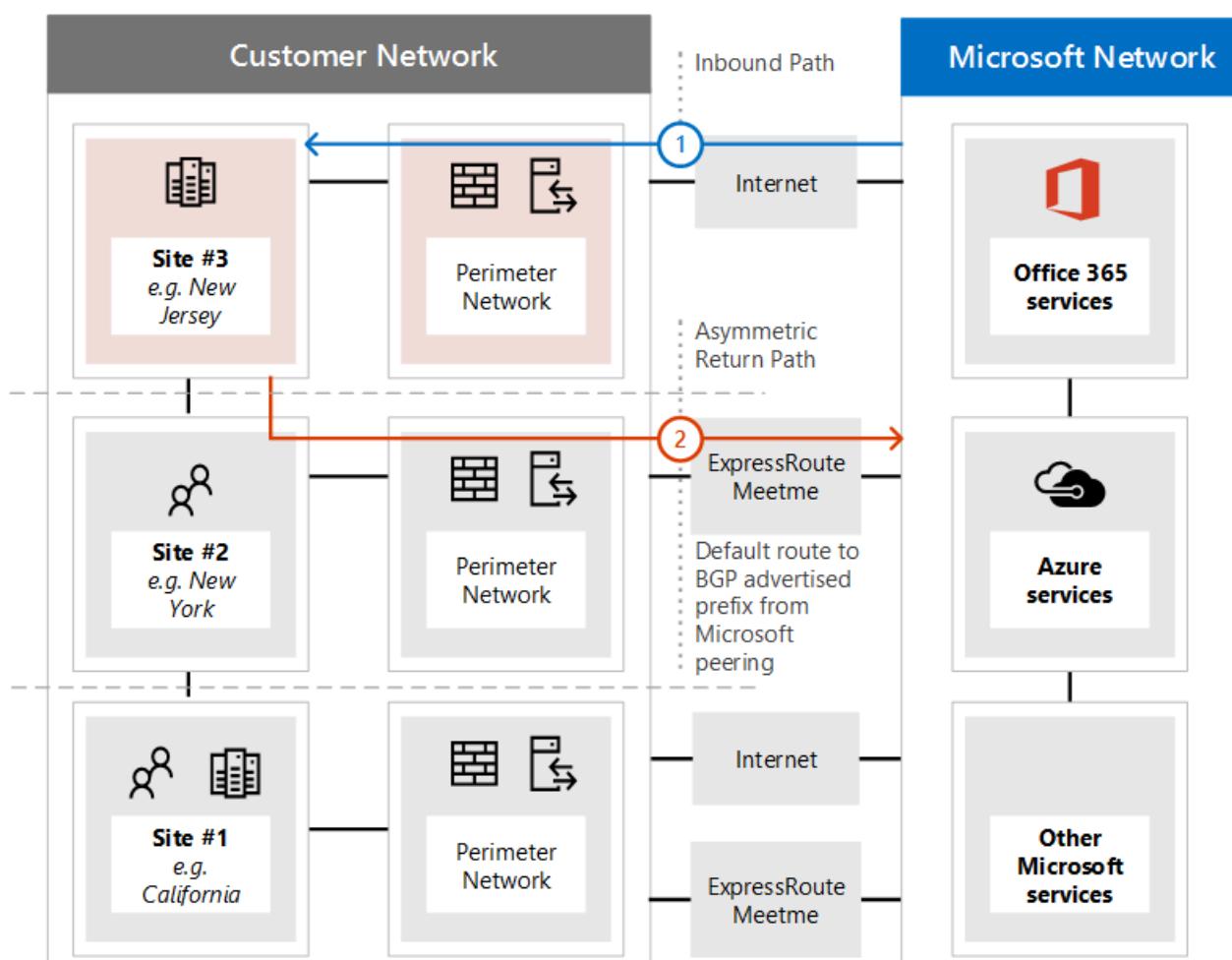


We also have suggestions on how to fix them.

Problem 1: Cloud to on-premises connection over the Internet

The following diagram illustrates the asymmetric network path taken when your network configuration doesn't provide NAT for inbound requests from the Microsoft cloud over the internet.

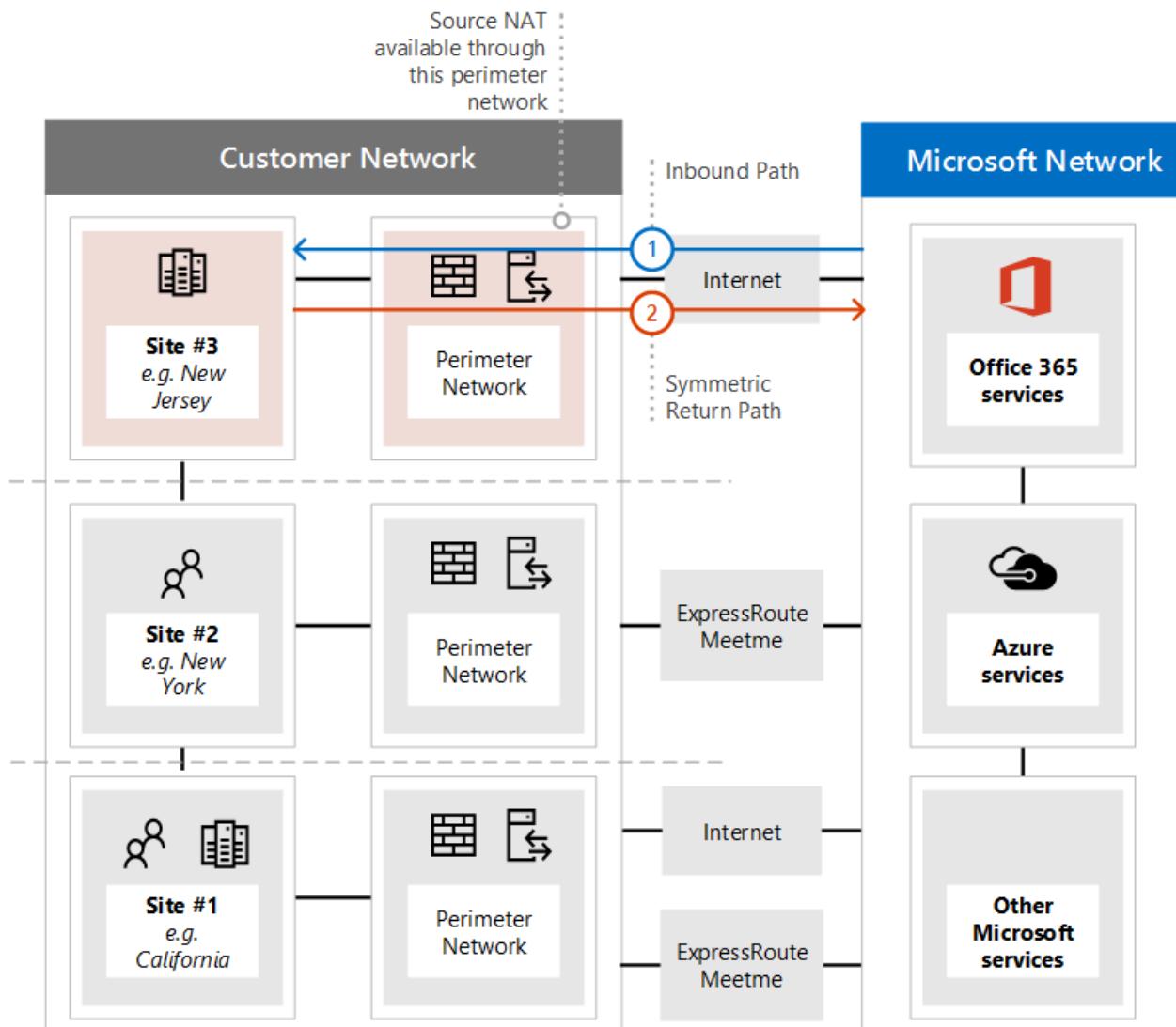
1. The inbound request from Microsoft 365 retrieves the IP address of the on-premises endpoint from public DNS and sends the request to your perimeter network.
2. In this faulty configuration, there's no Source NAT configured or available at the perimeter network where the traffic is sent resulting in the actual source IP address being used as the return destination.
 - The server on your network routes the return traffic to Microsoft 365 through any available ExpressRoute network connection.
 - The result is an Asymmetric path for that flow to Microsoft 365, resulting in a broken connection.



Solution 1a: Source NAT

Simply adding a source NAT to the inbound request resolves this misconfigured network. In this diagram:

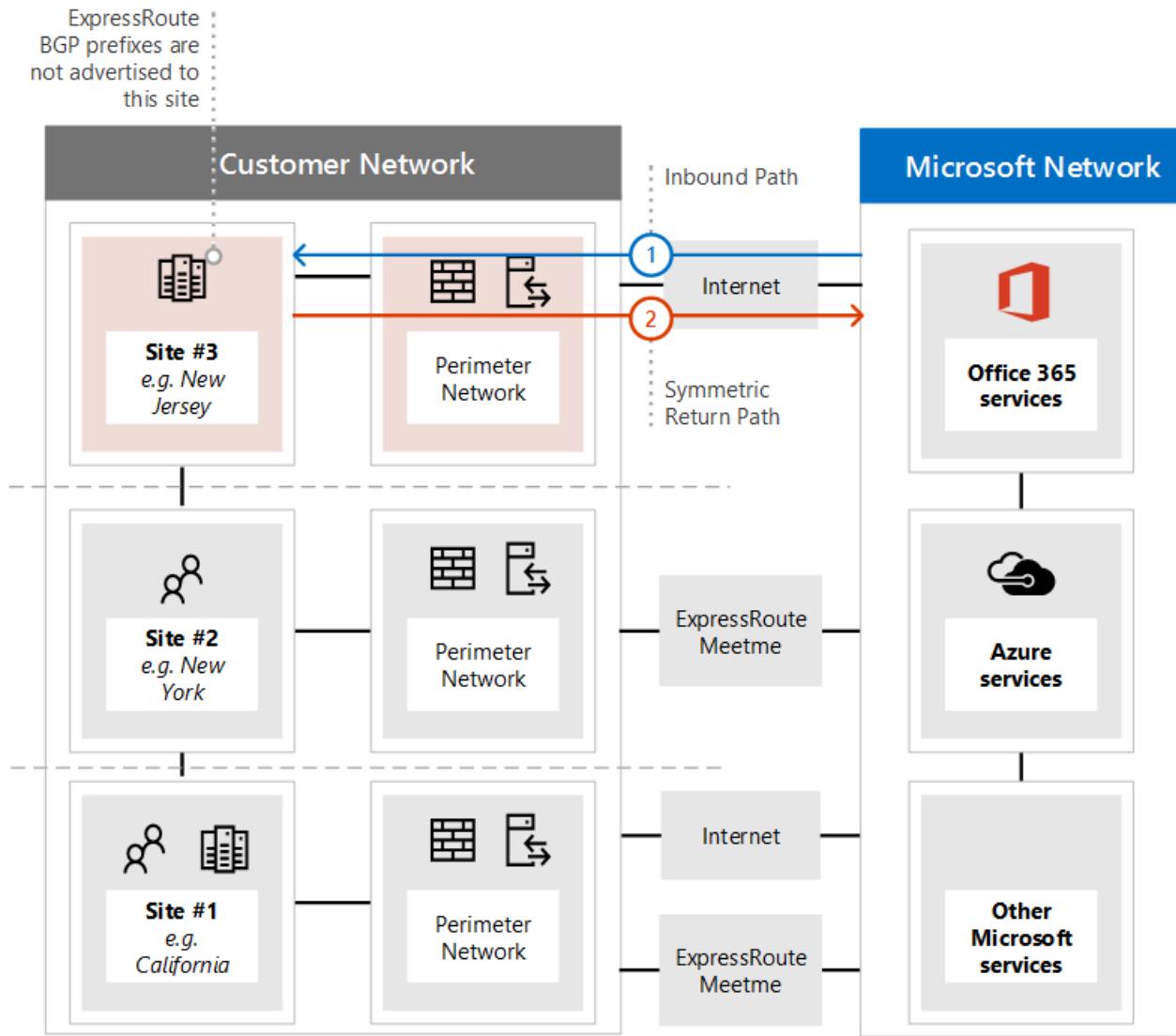
1. The incoming request continues to enter through the New Jersey data center's perimeter network. This time Source NAT is available.
2. The response from the server routes back toward the IP associated with the Source NAT instead of the original IP address, resulting in the response returning along the same network path.



Solution 1b: Route Scoping

Alternatively, you can choose to not allow the ExpressRoute BGP prefixes to be advertised, removing the alternate network path for those computers. In this diagram:

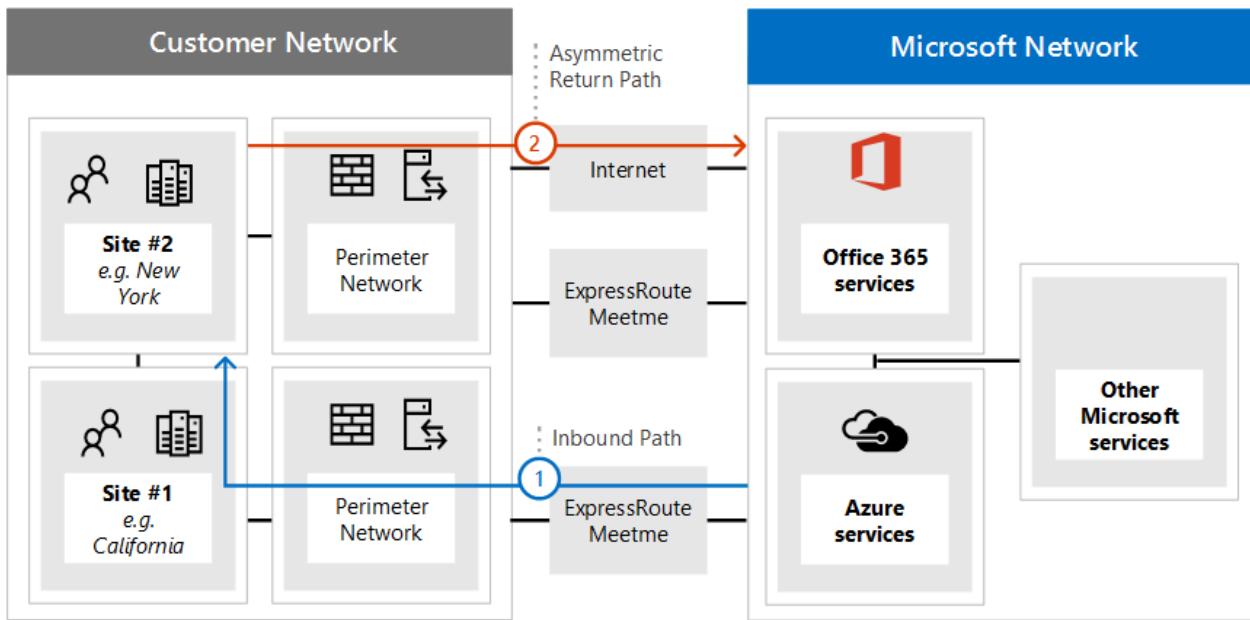
1. The incoming request continues to enter through the New Jersey data center's perimeter network. This time the prefixes advertised from Microsoft over the ExpressRoute circuit aren't available to the New Jersey data center.
2. The response from the server routes back toward the IP associated with the original IP address over the only route available, resulting in the response returning along the same network path.



Problem 2: Cloud to on-premises connection over ExpressRoute

The following diagram illustrates the asymmetric network path taken when your network configuration doesn't provide NAT for inbound requests from the Microsoft cloud over ExpressRoute.

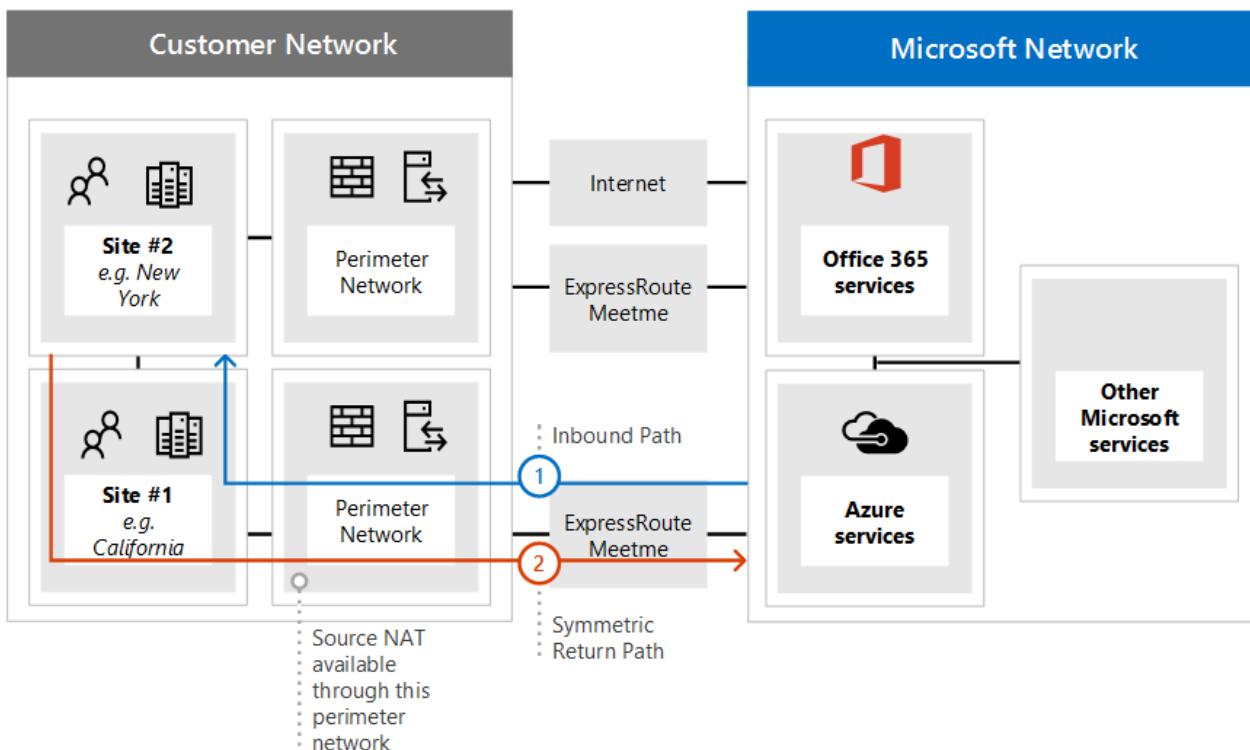
1. The inbound request from Microsoft 365 retrieves the IP address from DNS and sends the request to your perimeter network.
2. In this faulty configuration, there's no Source NAT configured or available at the perimeter network where the traffic is sent resulting in the actual source IP address being used as the return destination.
 - The computer on your network routes the return traffic to Microsoft 365 through any available ExpressRoute network connection.
 - The result is an Asymmetric connection to Microsoft 365.



Solution 2: Source NAT

Simply adding a source NAT to the inbound request resolves this misconfigured network. In this diagram:

1. The incoming request continues to enter through the New York data center's perimeter network. This time Source NAT is available.
2. The response from the server routes back toward the IP associated with the Source NAT instead of the original IP address, resulting in the response returning along the same network path.



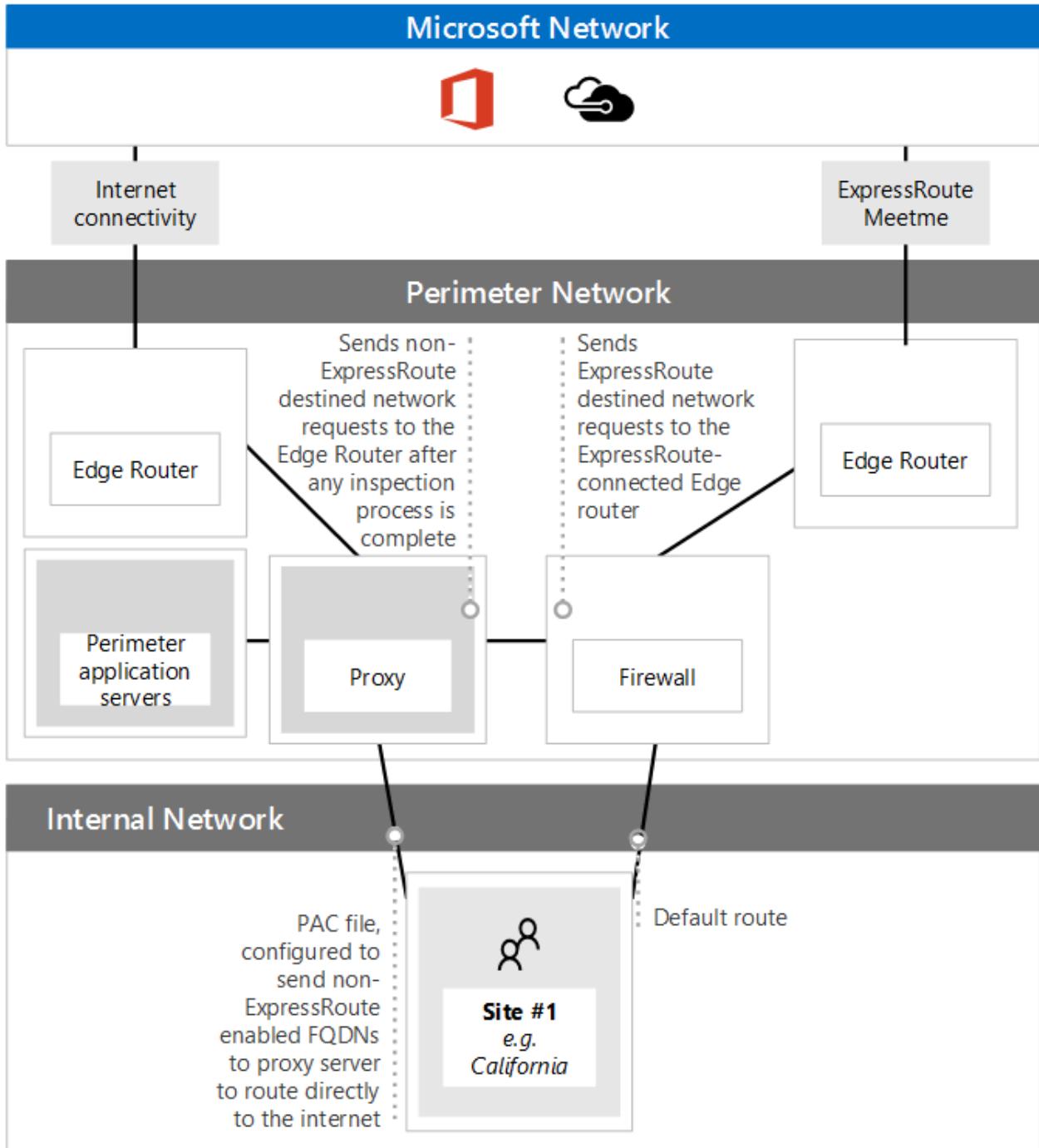
Paper verify that the network design has path symmetry

At this point, you need to verify on paper that your implementation plan offers route symmetry for the different scenarios in which you'll be using Microsoft 365. You'll identify the specific network route that is expected to be taken when a person uses different features of the service. From the on-premises network and WAN routing, to the perimeter devices, to the connectivity path; ExpressRoute or the internet, and on to the connection to the online endpoint.

You'll need to do this for all of the Microsoft 365 network services that were previously identified as services that your organization will adopt.

It helps to do this paper walk-through of routes with a second person. Explain to them where each network hop is expected to get its next route from and ensure that you're familiar with the routing paths. Remember that ExpressRoute will always provide a more scoped route to Microsoft server IP addresses giving it lower route cost than an Internet default route.

Design Client Connectivity Configuration



If you're using a proxy server for internet bound traffic, then you need to adjust any PAC or client configuration files to ensure client computers on your network are correctly configured to send the ExpressRoute traffic you desire to Microsoft 365 without transiting your proxy server, and the remaining traffic, including some Microsoft 365 traffic, is sent to the relevant proxy. Read our guide on [managing Microsoft 365 endpoints](#), for example, PAC files.

ⓘ Note

The endpoints change frequently, as often as weekly. You should only make changes based on the services and features your organization has adopted to reduce the number of changes you'll need to make to stay current. Pay close attention to the **Effective Date** in the RSS feed where the changes are announced

and a record is kept of all past changes, IP addresses that are announced may not be advertised, or removed from advertisement, until the effective date is reached.

Ensuring route symmetry

The Microsoft 365 front-end servers are accessible on both the Internet and ExpressRoute. These servers will prefer to route back to on-premises over ExpressRoute circuits when both are available. Because of this, there's a possibility of route asymmetry if traffic from your network prefers to route over your Internet circuits. Asymmetrical routes are a problem because devices that perform stateful packet inspection can block return traffic that follows a different path than the outbound packets followed.

Regardless of whether you initiate a connection to Microsoft 365 over the Internet or ExpressRoute, the source must be a publicly routable address. With many customers peering directly with Microsoft, having private addresses where duplication is possible between customers isn't feasible.

The following are scenarios where communications from Microsoft 365 to your on-premises network will be initiated. To simplify your network design, we recommend routing the following over the Internet path.

- SMTP services such as mail from an Exchange Online tenant to an on-premises host or SharePoint Mail sent from SharePoint to an on-premises host. SMTP protocol is used more broadly within Microsoft's network than the route prefixes shared over ExpressRoute circuits and advertising on-premises SMTP servers over ExpressRoute will cause failures with these other services.
- ADFS during password validation for signing in.
- [Exchange Server Hybrid deployments](#).
- [SharePoint federated hybrid search](#).
- [SharePoint hybrid BCS](#).
- [Skype for Business hybrid](#) and/or [Skype for Business federation](#).
- [Skype for Business Cloud Connector](#).

For Microsoft to route back to your network for these bi-directional traffic flows, the BGP routes to your on-premises devices must be shared with Microsoft. When you advertise route prefixes to Microsoft over ExpressRoute, you should follow these best practices:

1. Do not advertise the same public IP Address route prefix to the public Internet and over ExpressRoute. It's recommended that the IP BGP Route Prefix advertisements to Microsoft over ExpressRoute are from a range that isn't advertised to the internet at all. If this isn't possible to achieve due to the available IP Address space, then it's essential to ensure you advertise a more specific range over ExpressRoute than any internet circuits.
2. Use separate NAT IP pools per ExpressRoute circuit and separate to that of your internet circuits.
3. Any route advertised to Microsoft will attract network traffic from any server in Microsoft's network, not only those for which routes are advertised to your network over ExpressRoute. Only advertise routes to servers where routing scenarios are defined and well understood by your team. Advertise separate IP Address route prefixes at each of multiple ExpressRoute circuits from your network.

High availability and failover with Azure ExpressRoute

We recommend provisioning at least two active circuits from each egress with ExpressRoute to your ExpressRoute provider. This is the most common place we see failures for customers and you can easily avoid it by provisioning a pair of active/active ExpressRoute circuits. We also recommend at least two active/active Internet circuits because many Microsoft 365 services are only available over the Internet.

Inside the egress point of your network are many other devices and circuits that play a critical role in how people perceive availability. These portions of your connectivity scenarios aren't covered by ExpressRoute or Microsoft 365 SLAs, but they play a critical role in the end-to-end service availability as perceived by people in your organization.

Focus on the people using and operating Microsoft 365, if a failure of any one component would affect peoples' experience using the service, look for ways to limit the total percentage of people affected. If a failover mode is operationally complex, consider the peoples' experience of a long time to recovery and look for operationally simple and automated failover modes.

Outside of your network, Microsoft 365, ExpressRoute, and your ExpressRoute provider all have different levels of availability.

Service Availability

- Microsoft 365 services are covered by well-defined [service level agreements](#), which include uptime and availability metrics for individual services. One reason Microsoft 365 can maintain such high service availability levels is the ability for individual components to seamlessly fail over between the many Microsoft datacenters, using the global Microsoft network. This failover extends from the datacenter and network to the multiple Internet egress points, and enables failover seamlessly from the perspective of the people using the service.
- ExpressRoute [provides a 99.9% availability SLA](#) on individual dedicated circuits between the Microsoft Network Edge and the ExpressRoute provider or partner infrastructure. These service levels are applied at the ExpressRoute circuit level, which consists of [two independent interconnects](#) between the redundant Microsoft equipment and the network provider equipment in each peering location.

Provider Availability

- Microsoft's service level arrangements stop at your ExpressRoute provider or partner. This is also the first place you can make choices that will influence your availability level. You should closely evaluate the architecture, availability, and resiliency characteristics your ExpressRoute provider offers between your network perimeter and your providers connection at each Microsoft peering location. Pay close attention to both the logical and physical aspects of redundancy, peering equipment, carrier provided WAN circuits, and any extra value add services such as NAT services or managed firewalls.

Designing your availability plan

We strongly recommend that you plan and design high availability and resiliency into your end-to-end connectivity scenarios for Microsoft 365. A design should include;

- No single points of failure, including both Internet and ExpressRoute circuits.
- Minimizing the number of people affected and duration of that impact for most anticipated failure modes.
- Optimizing for simple, repeatable, and automatic recovery process from most anticipated failure modes.
- Supporting the full demands of your network traffic and functionality through redundant paths, without substantial degradation.

Your connectivity scenarios should include a network topology that is optimized for multiple independent and active network paths to Microsoft 365. This will yield a better

end-to-end availability than a topology that is optimized only for redundancy at the individual device or equipment level.

Tip

If your users are distributed across multiple continents or geographic regions and each of those locations connects over redundant WAN circuits to a single on-premises location where a single ExpressRoute circuit is located, your users will experience less end-to-end service availability than a network topology design that includes independent ExpressRoute circuits that connect the different regions to the nearest peering location.

We recommend provisioning at least two ExpressRoute circuits with each circuit connecting to with a different geographic peering location. You should provision this active-active pair of circuits for every region where people will use ExpressRoute connectivity for Microsoft 365 services. This allows each region to remain connected during a disaster that affects a major location such as a datacenter or peering location. Configuring them in as active/active allows end user traffic to be distributed across multiple network paths. This reduces the scope of people affected during device or network equipment outages.

We don't recommend using a single ExpressRoute circuit with the Internet as a backup.

Example: Failover and High Availability

Contoso's multi-geographic design has undergone a review of routing, bandwidth, security, and now must go through a high availability review. Contoso thinks about high availability as covering three categories; resiliency, reliability, and redundancy.

Resiliency allows Contoso to recover from failures quickly. Reliability allows Contoso to offer a consistent outcome within the system. Redundancy allows Contoso to move between one or more mirrored instances of infrastructure.

Within each edge configuration, Contoso has redundant Firewalls, Proxies, and IDS. For North America, Contoso has one edge configuration in their Dallas datacenter and another edge configuration in their Virginia datacenter. The redundant equipment at each location offers resiliency to that location.

The network configuration at Contoso is built based on a few key principles:

- Within each geographic region, there are multiple Azure ExpressRoute circuits.

- Each circuit within a region can support all of the network traffic within that region.
- Routing will clearly prefer one or the other path depending on availability, location, and so on.
- Failover between Azure ExpressRoute circuits happens automatically without additional configuration or action required by Contoso.
- Failover between Internet circuits happens automatically without additional configuration or action required by Contoso.

In this configuration, with redundancy at the physical and virtual level, Contoso is able to offer local resiliency, regional resiliency, and global resiliency in a reliable way. Contoso elected this configuration after evaluating a single Azure ExpressRoute circuit per region as well as the possibility of failing over to the internet.

If Contoso was unable to have multiple Azure ExpressRoute circuits per region, routing traffic originating in North America to the Azure ExpressRoute circuit in Asia Pacific would add an unacceptable level of latency and the required DNS forwarder configuration adds complexity.

Using the internet as a backup configuration isn't recommended. This breaks Contoso's reliability principle, resulting in an inconsistent experience using the connection. Additionally, manual configuration would be required to fail over considering the BGP advertisements that have been configured, NAT configuration, DNS configuration, and the proxy configuration. This added failover complexity increases the time to recover and decreases their ability to diagnose and troubleshoot the steps involved.

Still have questions about how to plan for and implement traffic management or Azure ExpressRoute? Read the rest of our [network and performance guidance](#) or the [Azure ExpressRoute FAQ](#).

Applying security controls to Azure ExpressRoute for Microsoft 365 scenarios

Securing Azure ExpressRoute connectivity starts with the same principles as securing Internet connectivity. Many customers choose to deploy network and perimeter controls along the ExpressRoute path connecting their on-premises network to Microsoft 365 and other Microsoft clouds. These controls may include firewalls, application proxies, data leakage prevention, intrusion detection, intrusion prevention systems, and so on. In many cases customers apply different levels of controls to traffic initiated from on-premises going to Microsoft, versus traffic initiated from Microsoft going to customer

on-premises network, versus traffic initiated from on-premises going to a general Internet destination.

Here's a few examples of integrating security with the [ExpressRoute connectivity model](#) you choose to deploy.

[+] [Expand table](#)

ExpressRoute integration option	Network security perimeter model
Colocated at a cloud exchange	Install new or use existing security/perimeter infrastructure in the colocation facility where the ExpressRoute connection is established. Use colocation facility purely for routing/interconnect purposes and back haul connections from colocation facility into the on-premises security/perimeter infrastructure.
Point-to-Point Ethernet	Terminate the Point-to-Point ExpressRoute connection in the existing on-premises security/perimeter infrastructure location. Install new security/perimeter infrastructure specific to the ExpressRoute path and terminate the Point-to-Point connection there.
Any-to-Any IPVPN	Use an existing on-premises security/perimeter infrastructure at all locations that egress into the IPVPN used for ExpressRoute for Microsoft 365 connectivity. Hairpin the IPVPN used for ExpressRoute for Microsoft 365 to specific on-premises locations designated to serve as the security/perimeter.

Some service providers also offer managed security/perimeter functionality as a part of their integration solutions with Azure ExpressRoute.

When considering the topology placement of the network/security perimeter options used for ExpressRoute for Microsoft 365 connections, following are extra considerations

- The depth and type network/security controls may have impact on the performance and scalability of the Microsoft 365 user experience.
- Outbound (on-premises->Microsoft) and inbound (Microsoft->on-premises) [if enabled] flows may have different requirements. These are likely different than Outbound to general Internet destinations.
- Microsoft 365 requirements for ports/protocols and necessary IP subnets are the same, whether traffic is routed through ExpressRoute for Microsoft 365 or through the Internet.
- Topological placement of the customer network/security controls determines the ultimate end to end network between the user and Microsoft 365 service and can

have a substantial impact on network latency and congestion.

- Customers are encouraged to design their security/perimeter topology for use with ExpressRoute for Microsoft 365 in accordance with best practices for redundancy, high availability, and disaster recovery.

Here's an example of Contoso that compares the different Azure ExpressRoute connectivity options with the perimeter security models discussed above.

Example: Securing Azure ExpressRoute

Contoso is considering implementing Azure ExpressRoute and after planning the optimal architecture for ExpressRoute for Microsoft 365 and after using the above guidance to understand bandwidth requirements, they're determining the best method for securing their perimeter.

For Contoso, a multi-national organization with locations in multiple continents, security must span all perimeters. The optimal connectivity option for Contoso is a multi-point connection with multiple peering locations around the globe to service the needs of their employees in each continent. Each continent includes redundant Azure ExpressRoute circuits within the continent and security must span all of these.

Contoso's existing infrastructure is reliable and can handle the extra work, as a result, Contoso is able to use the infrastructure for their Azure ExpressRoute and internet perimeter security. If this weren't the case, Contoso could choose to purchase more equipment to supplement their existing equipment or to handle a different type of connection.

Bandwidth planning for Azure ExpressRoute

Every Microsoft 365 customer has unique bandwidth needs depending on the number of people at each location, how active they are with each Microsoft 365 application, and other factors such as the use of on-premises or hybrid equipment and network security configurations.

Having too little bandwidth will result in congestion, retransmissions of data, and unpredictable delays. Having too much bandwidth will result in unnecessary cost. On an existing network, bandwidth is often referred to in terms of the amount of available headroom on the circuit as a percentage. Having 10% headroom will likely result in congestion and having 80% headroom generally means unnecessary cost. Typical headroom target allocations are 20% to 50%.

To find the right level of bandwidth, the best mechanism is to test your existing network consumption. This is the only way to get a true measure of usage and need as every network configuration and applications are in some ways unique. When measuring, you'll want to pay close attention to the total bandwidth consumption, latency, and TCP congestion to understand your network needs.

Once you have an estimated baseline that includes all network applications, pilot Microsoft 365 with a small group that comprises the different profiles of people in your organization to determine actual usage, and use the two measurements to estimate the amount of bandwidth you'll require for each office location. If there are any latency or TCP congestion issues found in your testing, you may need to move the egress closer to the people using Microsoft 365 or remove intensive network scanning such as SSL decryption/inspection.

All of our recommendations on what type of network processing is recommended applies to both ExpressRoute and Internet circuits. The same is true for the rest of the guidance on our [performance tuning site](#).

Build your deployment and testing procedures

Your implementation plan should include both testing and rollback planning. If your implementation isn't functioning as expected, the plan should be designed to affect the least number of people before problems are discovered. The following are some high-level principles your plan should consider.

1. Stage the network segment and user service onboarding to minimize disruption.
2. Plan for testing routes with traceroute and TCP connect from a separate internet connected host.
3. Preferably, testing of inbound and outbound services should be done on an isolated test network with a test Microsoft 365 tenant.
 - Alternatively, testing can be performed on a production network if the customer isn't yet using Microsoft 365 or is in pilot.
 - Alternatively, testing can be performed during a production outage that is set aside for test and monitoring only.
 - Alternatively, testing can be done by checking routes for each service on each layer 3 router node. This fall back should only be used if no other testing is possible since a lack of physical testing introduces risk.

Build your deployment procedures

Your deployment procedures should roll out to small groups of people in stages to allow for testing before deploying to larger groups of people. The following are several ways to stage the deployment of ExpressRoute.

1. Set up ExpressRoute with Microsoft peering and have the route advertisements forwarded to a single host only for staged testing purposes.
2. Advertise routes to the ExpressRoute network to a single network segment at first and expand route advertisements by network segment or region.
3. If deploying Microsoft 365 for the first time, use the ExpressRoute network deployment as a pilot for a few people.
4. If using proxy servers, you can alternatively configure a test PAC file to direct a few people to ExpressRoute with testing and feedback before adding more.

Your implementation plan should list each of the deployment procedures that must be taken or commands that need to be used to deploy the networking configuration. When the network outage time arrives, all of the changes being made should be from the written deployment plan that was written in advance and peer reviewed. See our guidance on the technical configuration of ExpressRoute.

- Updating your SPF TXT records if you've changed IP addresses for any on-premises servers that will continue to send email.
- Updating any DNS entries for on-premises servers if you've changed IP addresses to accommodate a new NAT configuration.
- Ensure you've subscribed to the RSS feed for Microsoft 365 endpoint notifications to maintain any routing or proxy configurations.

After your ExpressRoute deployment is complete, the procedures in the test plan should be executed. Results for each procedure should be logged. You must include procedures for rolling back to the original production environment in the event the test plan results indicate the implementation was not successful.

Build your test procedures

Your testing procedures should include tests for each outbound and inbound network service for Microsoft 365 both that will be using ExpressRoute and ones that will not. The procedures should include testing from each unique network location including users who aren't on-premises in the corporate LAN.

Some examples of test activities include the following.

1. Ping from your on-premises router to your network operator router.
2. Validate the 500+ Microsoft 365 and CRM Online IP address advertisements are received by your on-premises router.
3. Validate your inbound and outbound NAT is operating between ExpressRoute and the internal network.
4. Validate that routes to your NAT are being advertised from your router.
5. Validate that ExpressRoute has accepted your advertised prefixes.

- Use the following cmdlet to verify peering advertisements:

PowerShell

```
Get-AzureRmExpressRouteCircuitRouteTable -DevicePath Primary -  
ExpressRouteCircuitName TestER -ResourceGroupName RG -PeeringType  
MicrosoftPeering
```

6. Validate your public NAT IP range isn't advertised to Microsoft through any other ExpressRoute or public Internet network circuit unless it's a specific subset of a larger range as in the previous example.
7. ExpressRoute circuits are paired, validate that both BGP sessions are running.
8. Set up a single host on the inside of your NAT and use ping, tracert, and tcpping to test connectivity across the new circuit to the host outlook.office365.com. Alternatively, you could use a tool such as Wireshark or Microsoft Network Monitor 3.4 on a mirrored port to the MSEE to validate you're able to connect to the IP address associated with outlook.office365.com.
9. Test application level functionality for Exchange Online.
 - Test Outlook is able to connect to Exchange Online and send/receive email.
 - Test Outlook is able to use online-mode.
 - Test smartphone connectivity and send/receive capability.
10. Test application level functionality for SharePoint
 - Test OneDrive for Business sync client.
 - Test SharePoint web access.

11. Test application level functionality for Skype for Business calling scenarios:

- Join to conference call as authenticated user [invite initiated by end user].
- Invite user to conference call [invite sent from MCU].
- Join conference as anonymous user using the Skype for Business web application.
- Join call from your wired PC connection, IP phone, and mobile device.
- Call to federated user o Call to PSTN Validation: call is completed, call quality is acceptable, connection time is acceptable.
- Verify presence status for contacts is updated for both members of the tenant and federated users.

Common problems

Asymmetric routing is the most common implementation problem. Here are some common sources to look for:

- Using an open or flat network routing topology without source NAT in place.
- Not using SNAT to route to inbound services through both the internet and ExpressRoute connections.
- Not testing inbound services on ExpressRoute on a test network prior to deploying broadly.

Deploying ExpressRoute connectivity through your network

Stage your deployment to one segment of the network at a time, progressively rolling out the connectivity to different parts of the network with a plan to roll back for each new network segment. If your deployment is aligned with a Microsoft 365 deployment, deploy to your Microsoft 365 pilot users first and extend from there.

First for your test and then for production:

- Run the deployment steps to enable ExpressRoute.
- Test your seeing the network routes are as expected.
- Perform testing on each inbound and outbound service.

- Rollback if you discover any issues.

Set up a test connection to ExpressRoute with a test network segment

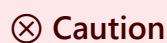
Now that you have the completed plan on paper it's time to test at a small scale. In this test you'll establish a single ExpressRoute connection with Microsoft Peering to a test subnet on your on-premises network. You can configure a [trial Microsoft 365 tenant](#) with connectivity to and from the test subnet and include all outbound and inbound services that you'll be using in production in the test subnet. Set up DNS for the test network segment and establish all inbound and outbound services. Execute your test plan and ensure that you are familiar with the routing for each service and the route propagation.

Execute the deployment and test plans

As you complete the items described above, check off the areas you've completed and ensure you and your team have reviewed them before executing your deployment and testing plans.

- List of outbound and inbound services that are involved in the network change.
- Global network architecture diagram showing both internet egress and ExpressRoute meet-me locations.
- Network routing diagram demonstrating the different network paths used for each service deployed.
- A deployment plan with steps to implement the changes and rollback if needed.
- A test plan for testing each Microsoft 365 and network service.
- Completed paper validation of production routes for inbound and outbound services.
- A completed test across a test network segment including availability testing.

Choose an outage window that is long enough to run through the entire deployment plan and the test plan, has some time available for troubleshooting and time for rolling back if necessary.



Caution

Due to the complex nature of routing over both the internet and ExpressRoute, it is recommended that additional buffer time is added to this window to handle troubleshooting complex routing.

Configure QoS for Skype for Business Online

QoS is necessary to obtain voice and meeting benefits for Skype for Business Online. You can configure QoS after you have ensured that the ExpressRoute network connection doesn't block any of your other Microsoft 365 service access. Configuration for QoS is described in the article [ExpressRoute and QoS in Skype for Business Online](#).

Troubleshooting your implementation

The first place to look is at the steps in this implementation guide, were any missed in your implementation plan? Go back and run further small network testing if possible to replicate the error and debug it there.

Identify which inbound or outbound services failed during testing. Get specifically the IP addresses and subnets for each of the services that failed. Go ahead and walk the network topology diagram on paper and validate the routing. Validate specifically where the ExpressRoute routing is advertised to, Test that routing during the outage if possible with traces.

Run PSPing with a network trace to each customer endpoint and evaluate source and destination IP addresses to validate that they are as expected. Run telnet to any mail host that you expose on port 25 and verify that SNAT is hiding the original source IP address if this is expected.

Keep in mind that while deploying Microsoft 365 with an ExpressRoute connection you'll need to ensure both the network configuration for ExpressRoute is optimally designed and you've also optimized the other components on your network such as client computers. In addition to using this planning guide to troubleshoot the steps you may have missed, we also have written a [Performance troubleshooting plan for Microsoft 365](#).

Here's a short link you can use to come back: <https://aka.ms/implementexpressroute365>

Related Topics

[Assessing Microsoft 365 network connectivity](#)

Azure ExpressRoute for Microsoft 365

[Media Quality and Network Connectivity Performance in Skype for Business Online ↗](#)

[Optimizing your network for Skype for Business Online ↗](#)

[ExpressRoute and QoS in Skype for Business Online ↗](#)

[Call flow using ExpressRoute ↗](#)

[Microsoft 365 performance tuning using baselines and performance history](#)

[Performance troubleshooting plan for Microsoft 365](#)

[Microsoft 365 URLs and IP address ranges ↗](#)

[Microsoft 365 network and performance tuning](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Microsoft 365 endpoints

Article • 02/05/2024

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Endpoints are the set of destination IP addresses, DNS domain names, and URLs for Microsoft 365 traffic on the Internet.

To optimize performance to Microsoft 365 cloud-based services, these endpoints need special handling by your client browsers and the devices in your edge network. These devices include firewalls, TLS Break and Inspect and packet inspection devices, and data loss prevention systems.

See [Managing Microsoft 365 endpoints](#) for the details.

There are currently five different Microsoft 365 clouds. This table takes you to the list of endpoints for each one.

 [Expand table](#)

Cloud	Description
Worldwide endpoints	The endpoints for worldwide Microsoft 365 subscriptions, which include the United States Government Community Cloud (GCC).
U.S. Government DoD endpoints	The endpoints for United States Department of Defense (DoD) subscriptions.
U.S. Government GCC High endpoints	The endpoints for United States Government Community Cloud High (GCC High) subscriptions.
Microsoft 365 operated by 21Vianet endpoints	The endpoints for Microsoft 365 operated by 21Vianet, which is designed to meet the needs for Microsoft 365 in China.

To automate getting the latest list of endpoints for your Microsoft 365 cloud, see the [Microsoft 365 IP Address and URL Web service](#).

For more endpoints, see these articles:

- [Additional endpoints not included in the Web service](#)
- [Network requests in Office 2016 for Mac](#)

If you're a network equipment vendor, join the [Office 365 Networking Partner Program](#).

Enroll in the program to build Microsoft 365 network connectivity principles into your products and solutions.

See also

[Microsoft 365 IP Address and URL Web service](#)

Feedback

Was this page helpful?



Yes



No

[Provide product feedback ↗](#)

Unified cloud.microsoft domain for Microsoft 365 apps

Article • 08/16/2024

Microsoft is unifying user-facing Microsoft 365 apps and services to a single and consistent domain: `cloud.microsoft`.

The growth of Microsoft cloud services led to the expansion of the domain space they occupy, resulting in [hundreds of domains](#). This fragmentation is a challenge for end user navigation, administrative simplicity, and the development of cross-app experiences. To solve this problem and to make it easier for customers, end users and app developers to interface with Microsoft 365 apps and services, Microsoft has designated a special domain - `cloud.microsoft`, to be used by Microsoft SaaS products going forward.

The `.microsoft` top-level domain is exclusive to Microsoft. The new domain doesn't have traditional suffixes such as `.com` or `.net` in the end. This is by design.

`cloud.microsoft` resides under the `.microsoft` top-level domain, for which Microsoft is a registry operator and the sole registrant. This domain allows for extra security, privacy, and protection against spoofing when you interact with apps within that domain. You can trust that any website or app that ends with `cloud.microsoft` is an official Microsoft product or service.

Benefits of a unified domain

Consolidating authenticated user-facing Microsoft 365 experiences to a single domain benefits customer in several ways. For end users, it streamlines the overall experience by reducing sign-ins, redirects, and delays when navigating across apps. For admins, it reduces the complexity of allowlists that are required to connect to Microsoft 365 services and help your organization stay secure and productive. For all our customers – and our developers – this change helps align for better and tighter integration across the Microsoft 365 ecosystem by streamlining development and improving performance of cross-app experiences.

'Dot brand' top-level domains like `.microsoft` enhance security, trustworthiness, and integrity. Microsoft has exclusive rights to the `.microsoft` top-level domain, enabling enhanced security protocols and governance controls to be applied across the entire domain hierarchy, starting from the top level. All experiences on the `.microsoft` domain

are guaranteed to be legitimate and authentic, as Microsoft is the registry operator and sole registrant.

Security considerations

To ensure that customers and users can treat everything under the *.cloud.microsoft domain as fully trusted, the entire domain hierarchy is isolated, purpose built, and dedicated to hosting only secure and compliant Microsoft product experiences. The domain is managed to the highest standards of domain security and reputation, and is kept free of scenarios such as third-party websites, IaaS/PaaS resources (such as file and blob storage), and hosting of active content, code or scripts that may affect the trust and integrity of products and applications residing in the domain.

Requirements for admins

Since 2023, *.cloud.microsoft and other domains related to the domain unification initiative are part of the [Microsoft 365 network guidance on domains and service endpoints](#). Customers who use the Microsoft 365 web service API to automate network settings have been getting the network settings since then. Customers who manually update endpoints should ensure that *.cloud.microsoft and other required domains are included in their allow-list to prevent connectivity and service incidents for their users.

Microsoft product and service URLs

[] Expand table

Service	URL
Microsoft 365 Service Health Status Page	status.cloud.microsoft ↗
Microsoft Admin Center	admin.cloud.microsoft ↗
Microsoft Excel	excel.cloud.microsoft ↗
Microsoft Loop	loop.cloud.microsoft ↗
Microsoft Mesh	mesh.cloud.microsoft ↗
Microsoft Planner	planner.cloud.microsoft ↗
Microsoft PowerPoint	powerpoint.cloud.microsoft ↗
Microsoft Setup	setup.cloud.microsoft ↗

Service	URL
Microsoft Sway	sway.cloud.microsoft ↗
Microsoft Viva Engage	engage.cloud.microsoft ↗
Microsoft Viva Goals	goals.cloud.microsoft ↗
Microsoft Viva Home	viva.cloud.microsoft ↗
Microsoft Viva Insights	insights.cloud.microsoft ↗
Microsoft Viva Learning	learning.cloud.microsoft ↗
Microsoft Viva Pulse	pulse.cloud.microsoft ↗
Microsoft Word	word.cloud.microsoft ↗

The above list provides examples of individual URLs for applications that users can use through the web browser. It does not represent the full set of endpoints required for functionality of these applications and should not be used to granularly control access through network allow-lists and other network settings. To configure network settings, customers should follow Microsoft official network guidance.

See also

- [Introducing cloud.microsoft: a unified domain for Microsoft 365 apps and services](#) ↗
- [Office 365 URLs and IP address ranges](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

Managing Microsoft 365 endpoints

Article • 01/19/2024

Most enterprise organizations that have multiple office locations and a connecting WAN need configuration for Microsoft 365 network connectivity. You can optimize your network by sending all trusted Microsoft 365 network requests directly through your firewall, bypassing all extra packet level inspection or processing. This reduces latency and your perimeter capacity requirements. Identifying Microsoft 365 network traffic is the first step in providing optimal performance for your users. For more information, see [Microsoft 365 Network Connectivity Principles](#).

Microsoft recommends you access the Microsoft 365 network endpoints and ongoing changes to them using the [Microsoft 365 IP Address and URL Web Service](#).

Regardless of how you manage vital Microsoft 365 network traffic, Microsoft 365 requires Internet connectivity. Other network endpoints where connectivity is required are listed at [Additional endpoints not included in the Microsoft 365 IP Address and URL Web service](#).

How you use the Microsoft 365 network endpoints depends on your enterprise organization network architecture. This article outlines several ways that enterprise network architectures can integrate with Microsoft 365 IP addresses and URLs. The easiest way to choose which network requests to trust is to use SD-WAN devices that support automated Microsoft 365 configuration at each of your office locations.

SD-WAN for local branch egress of vital Microsoft 365 network traffic

At each branch office location, you can provide an SD-WAN device that is configured to route traffic for Microsoft 365 Optimize category of endpoints, or Optimize and Allow categories, directly to Microsoft's network. Other network traffic including on-premises datacenter traffic, general Internet web sites traffic, and traffic to Microsoft 365 Default category endpoints is sent to another location where you have a more substantial network perimeter.

Microsoft is working with SD-WAN providers to enable automated configuration. For more information, see [Microsoft 365 Networking Partner Program](#).

Use a PAC file for direct routing of vital Microsoft 365 traffic

Use PAC or WPAD files to manage network requests that are associated with Microsoft 365 but don't have an IP address. Typical network requests that are sent through a proxy or perimeter device increase latency. While TLS Break and Inspect creates the largest latency, other services such as proxy authentication and reputation lookup can cause poor performance and a bad user experience. Additionally, these perimeter network devices need enough capacity to process all of the network connection requests. We recommend bypassing your proxy or inspection devices for direct Microsoft 365 network requests.

[PowerShell Gallery Get-PacFile](#) is a PowerShell script that reads the latest network endpoints from the Microsoft 365 IP Address and URL Web service and creates a sample PAC file. You can modify the script so that it integrates with your existing PAC file management.

ⓘ Note

For more information about the security and performance considerations of direct connectivity to Microsoft 365 endpoints, see [Microsoft 365 Network Connectivity Principles](#).

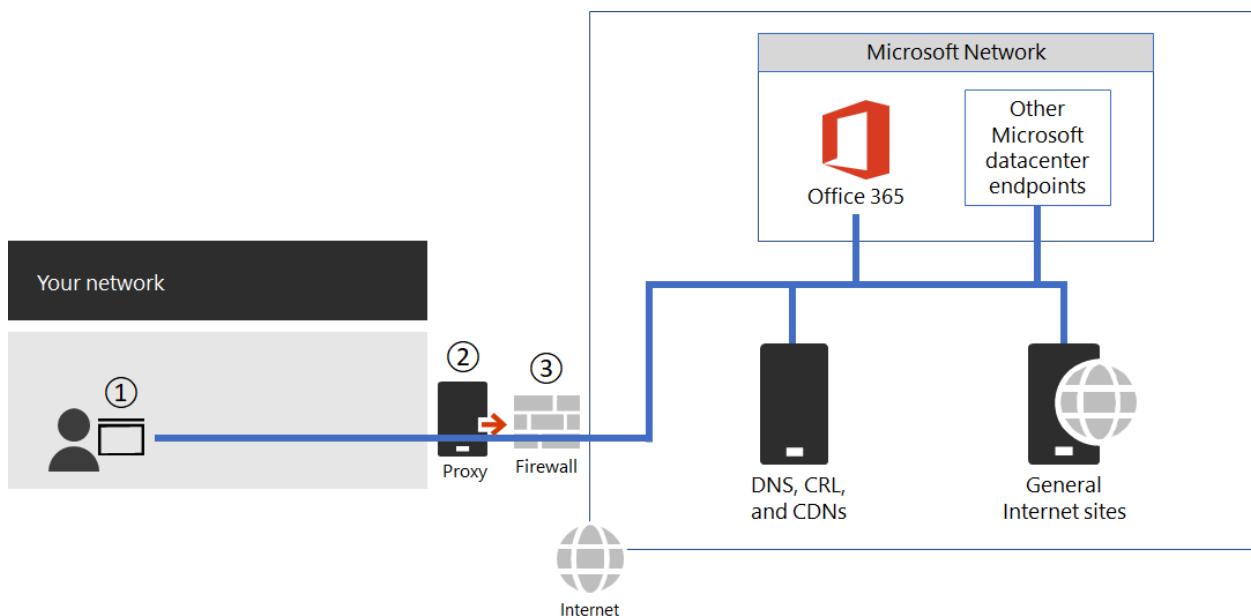


Figure 1 - Simple enterprise network perimeter

The PAC file is deployed to web browsers at point 1 in Figure 1. When using a PAC file for direct egress of vital Microsoft 365 network traffic, you also need to allow connectivity to the IP addresses behind these URLs on your network perimeter firewall.

This is done by fetching the IP addresses for the same Microsoft 365 endpoint categories as specified in the PAC file and creating firewall ACLs based on those addresses. The firewall is point 3 in Figure 1.

Separately if you choose to only do direct routing for the Optimize category endpoints, any required Allow category endpoints that you send to the proxy server needs to be listed in the proxy server to bypass further processing. For example, TLS break and Inspect and Proxy Authentication are incompatible with both the Optimize and Allow category endpoints. The proxy server is point 2 in Figure 1.

The common configuration is to permit without processing all outbound traffic from the proxy server for the destination IP addresses for Microsoft 365 network traffic that hits the proxy server. For information about issues with TLS Break and Inspect, see [Using third-party network devices or solutions on Microsoft 365 traffic](#).

There are two types of PAC files that the Get-PacFile script generates.

[+] Expand table

Type	Description
1	Send Optimize endpoint traffic direct and everything else to the proxy server.
2	Send Optimize and Allow endpoint traffic direct and everything else to the proxy server. This type can also be used to send all supported ExpressRoute for Microsoft 365 traffic to ExpressRoute network segments and everything else to the proxy server.

Here's a simple example of calling the PowerShell script:

PowerShell

```
Get-PacFile -ClientRequestId b10c5ed1-bad1-445f-b386-b919946339a7
```

There are many parameters you can pass to the script:

[+] Expand table

Parameter	Description
ClientRequestId	This is required and is a GUID passed to the web service that represents the client machine making the call.
Instance	The Microsoft 365 service instance, which defaults to Worldwide. This is also passed to the web service.

Parameter	Description
TenantName	Your Microsoft 365 tenant name. Passed to the web service and used as a replaceable parameter in some Microsoft 365 URLs.
Type	The type of the proxy PAC file that you want to generate.

Here's another example of calling the PowerShell script with more parameters:

PowerShell

```
Get-PacFile -Type 2 -Instance Worldwide -TenantName Contoso -ClientRequestId
b10c5ed1-bad1-445f-b386-b919946339a7
```

Proxy server bypass processing of Microsoft 365 network traffic

Where PAC files aren't used for direct outbound traffic, you still want to bypass processing on your network perimeter by configuring your proxy server. Some proxy server vendors have enabled automated configuration of this as described in the [Microsoft 365 Networking Partner Program](#).

If you do this manually, you need to get the Optimize and Allow endpoint category data from the Microsoft 365 IP Address and URL Web Service and configure your proxy server to bypass processing for these. It's important to avoid TLS Break and Inspect and Proxy Authentication for the Optimize and Allow category endpoints.

Change management for Microsoft 365 IP addresses and URLs

In addition to selecting appropriate configuration for your network perimeter, it's critical that you adopt a change management process for Microsoft 365 endpoints. These endpoints change regularly. If you don't manage the changes, you can end up with users blocked or with poor performance after a new IP address or URL is added.

Changes to the Microsoft 365 IP addresses and URLs are usually published near the last day of each month. Sometimes a change is published outside of that schedule due to operational, support, or security requirements.

When a change is published that requires you to act because an IP address or URL was added, you should expect to receive 30 days notice from the time we publish the

change until there's a Microsoft 365 service on that endpoint. This is reflected as the Effective Date. Although we aim for this notification period, it might not always be possible due to operational, support, or security requirements. Changes that don't require immediate action to maintain connectivity, such as removed IP addresses or URLs or less significant changes, don't include advance notification. In these instances, no Effective Date is provided. Regardless of what notification is provided, we list the expected service active date for each change.

Change notification using the Web Service

You can use the Microsoft 365 IP Address and URL Web Service to get change notification. We recommend you call the `/version` web method once an hour to check the version of the endpoints that you're using to connect to Microsoft 365. If this version changes when compared to the version that you have in use, then you should get the latest endpoint data from the `/endpoints` web method and optionally get the differences from the `/changes` web method. It isn't necessary to call the `/endpoints` or `/changes` web methods if there hasn't been any change to the version you found.

For more information, see [Microsoft 365 IP Address and URL Web Service](#).

Change notification using RSS feeds

The Microsoft 365 IP Address and URL Web Service provide an RSS feed that you can subscribe to in Outlook. There are links to the RSS URLs on each of the Microsoft 365 service instance-specific pages for the IP addresses and URLs. For more information, see [Microsoft 365 IP Address and URL Web Service](#).

Change notification and approval review using Power Automate

We understand that you might still require manual processing for network endpoint changes that come through each month. You can use Power Automate to create a flow that notifies you by email and optionally runs an approval process for changes when Microsoft 365 network endpoints have changes. Once review is completed, you can have the flow automatically email the changes to your firewall and proxy server management team.

For information about a Power Automate sample and template, see [Use Power Automate to receive an email for changes to Microsoft 365 IP addresses and URLs](#).

Microsoft 365 network endpoints FAQ

See these frequently asked questions about Microsoft 365 network connectivity.

How do I submit a question?

Select the link at the bottom to indicate if the article was helpful or not and submit any more questions. We monitor the feedback and update the questions here with the most frequently asked.

How do I determine the location of my tenant?

Tenant location is best determined using our [datacenter map](#).

Am I peering appropriately with Microsoft?

Peering locations are described in more detail in [peering with Microsoft](#).

With over 2500 ISP peering relationships globally and 70 points of presence, getting from your network to ours should be seamless. It can't hurt to spend a few minutes making sure your ISP's peering relationship is the most optimal, [here's a few examples](#) of good and not so good peering hand-offs to our network.

I see network requests to IP addresses not on the published list, do I need to provide access to them?

We only provide IP addresses for the Microsoft 365 servers you should route directly to. This isn't a comprehensive list of all IP addresses you'll see network requests for. You'll see network requests to Microsoft and third-party owned, unpublished, IP addresses. These IP addresses are dynamically generated or managed in a way that prevents timely notice when they change. If your firewall can't allow access based on the FQDNs for these network requests, use a PAC or WPAD file to manage the requests.

See an IP associated with Microsoft 365 that you want more information on?

1. Check if the IP address is included in a larger published range using a CIDR calculator, such as these for [IPv4](#) or [IPv6](#). For example, 40.96.0.0/13 includes the IP Address 40.103.0.1 despite 40.96 not matching 40.103.
2. See if a partner owns the IP with a [whois query](#). If it's Microsoft owned, it might be an internal partner. Many partner network endpoints are listed as belonging to the *default* category, for which IP addresses aren't published.

3. The IP address might not be part of Microsoft 365 or a dependency. Microsoft 365 network endpoint publishing doesn't include all of Microsoft network endpoints.
4. Check the certificate. With a browser, connect to the IP address using `HTTPS://<IP_ADDRESS>` and check the domains listed on the certificate to understand what domains are associated with the IP address. If it's a Microsoft-owned IP address and not on the list of Microsoft 365 IP addresses, it's likely the IP address is associated with a Microsoft CDN such as `MSOCDN.NET` or another Microsoft domain without published IP information. If you do find the domain on the certificate is one where we claim to list the IP address, please let us know.

Some Microsoft 365 URLs point to CNAME records instead of A records in the DNS. What do I have to do with the CNAME records?

Client computers need a DNS A or AAAA record that includes one or more IP address(es) to connect to a cloud service. Some URLs included in Microsoft 365 show CNAME records instead of A or AAAA records. These CNAME records are intermediary and there might be several in a chain. They'll always eventually resolve to an A or AAAA record for an IP Address. For example, consider the following series of DNS records, which ultimately resolve to the IP address `IP_1`:

```
Console

serviceA.office.com -> CNAME: serviceA.domainA.com -> CNAME:
serviceA.domainB.com -> A: IP_1
```

These CNAME redirects are a normal part of the DNS and are transparent to the client computer and transparent to proxy servers. They're used for load balancing, content delivery networks, high availability, and service incident mitigation. Microsoft doesn't publish the intermediary CNAME records, they're subject to change at any time, and you shouldn't need to configure them as allowed in your proxy server.

A proxy server validates the initial URL, which in the above example is `serviceA.office.com`, and this URL would be included in Microsoft 365 publishing. The proxy server requests DNS resolution of that URL to an IP Address and receives back `IP_1`. It doesn't validate the intermediary CNAME redirection records.

Hard-coded configurations or using an allowlist based on indirect Microsoft 365 FQDNs aren't recommended and not supported by Microsoft. They are known to cause customer connectivity issues. DNS solutions that block on CNAME redirection, or that otherwise incorrectly resolve Microsoft 365 DNS entries, can be solved via DNS

forwarders with DNS recursion enabled or by using DNS root hints. Many third-party network perimeter products natively integrate recommended Microsoft 365 endpoint to include an allowlist in their configuration using the [Microsoft 365 IP Address and URL Web service](#).

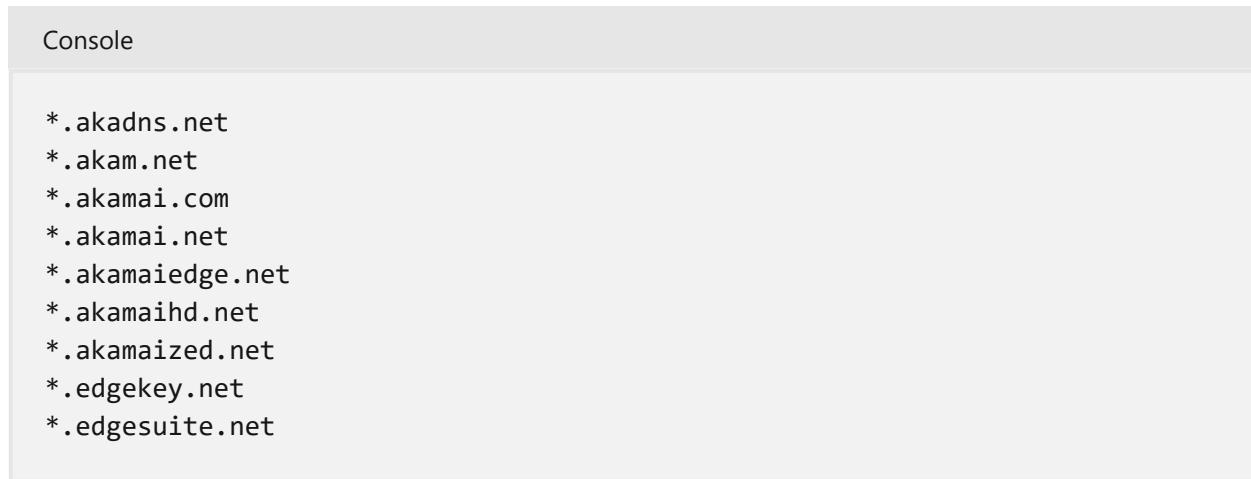
Why do I see names such as nsatc.net or akadns.net in the Microsoft domain names?

Microsoft 365 and other Microsoft services use several third-party services such as Akamai and MarkMonitor to improve your Microsoft 365 experience. To keep giving you the best experience possible, we might change these services in the future. Third-party domains might host content, such as a CDN, or they might host a service, such as a geographical traffic management service. Some of the services currently in use include:

[MarkMonitor](#) is in use when you see requests that include *.nsatc.net. This service provides domain name protection and monitoring to protect against malicious behavior.

[ExactTarget](#) is in use when you see requests to *.exacttarget.com. This service provides email link management and monitoring against malicious behavior.

[Akamai](#) is in use when you see requests that include one of the following FQDNs. This service offers geo-DNS and content delivery network services.



The screenshot shows a 'Console' window with a list of FQDNs. The list includes:
*.akadns.net
*.akam.net
*.akamai.com
*.akamai.net
*.akamaiedge.net
*.akamaihd.net
*.akamaized.net
*.edgekey.net
*.edgesuite.net

I have to have the minimum connectivity possible for Microsoft 365

As Microsoft 365 is a suite of services built to function over the internet, the reliability and availability promises are based on many standard internet services being available. For example, standard internet services such as DNS, CRL, and CDNs must be reachable to use Microsoft 365 just as they must be reachable to use most modern internet services.

The Microsoft 365 suite is broken down into four major service areas representing the three primary workloads and a set of common resources. These service areas may be used to associate traffic flows with a particular application, however given that features often consume endpoints across multiple workloads, these service areas cannot effectively be used to restrict access.

[+] [Expand table](#)

Service Area	Description
Exchange	Exchange Online and Exchange Online Protection
SharePoint	SharePoint Online and OneDrive for Business
Skype for Business Online and Microsoft Teams	Skype for Business and Microsoft Teams
Common	Microsoft 365 Pro Plus, Office in a browser, Microsoft Entra ID, and other common network endpoints

In addition to basic internet services, there are third-party services that are only used to integrate functionality. While these services are needed for integration, they're marked as optional in the Microsoft 365 endpoints article. This means core functionality of the service continues to function if the endpoint isn't accessible. Any network endpoint that is required has the required attribute set to true. Any network endpoint that is optional has the required attribute set to false and the notes attribute detail the missing functionality you should expect if connectivity is blocked.

If you're trying to use Microsoft 365 and are finding third-party services aren't accessible, you want to [ensure all FQDNs marked required or optional in this article are allowed through the proxy and firewall](#).

How do I block access to Microsoft's consumer services?

The tenant restrictions feature now supports blocking the use of all Microsoft consumer applications (MSA apps) such as OneDrive, Hotmail, and Xbox.com. This feature uses a separate header to the login.live.com endpoint. For more information, see [Use tenant restrictions to manage access to SaaS cloud applications](#).

My firewall requires IP Addresses and cannot process URLs. How do I configure it for Microsoft 365?

Microsoft 365 doesn't provide IP addresses of all required network endpoints. Some are provided as URLs only and are categorized as default. URLs in the default category that are required should be allowed through a proxy server. If you don't have a proxy server, look at how you have configured web requests for URLs that users type into the address bar of a web browser; the user doesn't provide an IP address either. The Microsoft 365 default category URLs that don't provide IP addresses should be configured in the same way.

Related articles

[Microsoft 365 IP Address and URL Web service](#)

[Microsoft Azure Datacenter IP Ranges ↗](#)

[Microsoft Public IP Space ↗](#)

[Network infrastructure requirements for Microsoft Intune](#)

[Microsoft 365 URLs and IP address ranges](#)

[Microsoft 365 Network Connectivity Principles](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Microsoft 365 URLs and IP address ranges

Article • 07/31/2024

Microsoft 365 requires connectivity to the Internet. The endpoints below should be reachable for customers using Microsoft 365 plans, including Government Community Cloud (GCC).

[Microsoft 365 Worldwide \(+GCC\)](#) | [Microsoft 365 operated by 21 Vianet](#) | [Microsoft 365 U.S. Government DoD](#) | [Microsoft 365 U.S. Government GCC High](#) |

[+] Expand table

Notes	Download	Use
Last updated: 07/31/2024 -  Change Log subscription	Download: all required and optional destinations in one JSON formatted list.	Use: our proxy PAC files

Start with [Managing Microsoft 365 endpoints](#) to understand our recommendations for managing network connectivity using this data. Endpoints data is updated as needed at the beginning of each month with new IP Addresses and URLs published 30 days in advance of being active. This cadence allows for customers who don't yet have automated updates to complete their processes before new connectivity is required. Endpoints may also be updated during the month if needed to address support escalations, security incidents, or other immediate operational requirements. The data shown on this page below is all generated from the REST-based web services. If you're using a script or a network device to access this data, you should go to the [Web service](#) directly.

Endpoint data below lists requirements for connectivity from a user's machine to Microsoft 365. For detail on IP addresses used for network connections from Microsoft into a customer network, sometimes called hybrid or inbound network connections, see [Additional endpoints](#) for more information.

The endpoints are grouped into four service areas representing the three primary workloads and a set of common resources. The groups may be used to associate traffic flows with a particular application, however given that features often consume endpoints across multiple workloads, these groups can't effectively be used to restrict access.

Data columns shown are:

- **ID:** The ID number of the row, also known as an endpoint set. This ID is the same as is returned by the web service for the endpoint set.
- **Category:** Shows whether the endpoint set is categorized as **Optimize**, **Allow**, or **Default**. This column also lists which endpoint sets are required to have network connectivity. For endpoint sets that aren't required to have network connectivity, we provide notes in this field to indicate what functionality would be missing if the endpoint set is blocked. If you're excluding an entire service area, the endpoint sets listed as required don't require connectivity.

You can read about these categories and guidance for their management in [Optimizing connectivity to Microsoft 365 services](#).

- **ER:** This is **Yes** if the endpoint set is supported over Azure ExpressRoute with Microsoft 365 route prefixes. The BGP community that includes the route prefixes shown aligns with the service area listed. When ER is **No**, this means that ExpressRoute is not supported for this endpoint set.

Some routes may be advertised in more than one BGP community, making it possible for endpoints within a given IP range to traverse the ER circuit, but still be unsupported. In all cases, the value of a given endpoint set's ER column should be respected.

- **Addresses:** Lists the FQDNs or wildcard domain names and IP address ranges for the endpoint set. Note that an IP address range is in CIDR format and may include many individual IP addresses in the specified network.
- **Ports:** Lists the TCP or UDP ports that are combined with listed IP addresses to form the network endpoint. You may notice some duplication in IP address ranges where there are different ports listed.

Note

Microsoft has begun a long-term transition to providing services from the **cloud.microsoft** namespace to simplify the endpoints managed by our customers. If you are following existing guidance for allowing access to required endpoints as listed below, there's no further action required from you.

Exchange Online

[\[+\] Expand table](#)

ID	Category	ER	Addresses	Ports
1	Optimize Required	Yes	outlook.cloud.microsoft, outlook.office.com, outlook.office365.com 13.107.6.152/31, 13.107.18.10/31, 13.107.128.0/22, 23.103.160.0/20, 40.96.0.0/13, 40.104.0.0/15, 52.96.0.0/14, 131.253.33.215/32, 132.245.0.0/16, 150.171.32.0/22, 204.79.197.215/32, 2603:1006::/40, 2603:1016::/36, 2603:1026::/36, 2603:1036::/36, 2603:1046::/36, 2603:1056::/36, 2620:1ec:4::152/128, 2620:1ec:4::153/128, 2620:1ec:c::10/128, 2620:1ec:c::11/128, 2620:1ec:d::10/128, 2620:1ec:d::11/128, 2620:1ec:8f0::/46, 2620:1ec:900::/46, 2620:1ec:a92::152/128, 2620:1ec:a92::153/128	TCP: 443, 80 UDP: 443
2	Allow Optional Notes: POP3, IMAP4, SMTP Client traffic	Yes	outlook.office365.com, smtp.office365.com 13.107.6.152/31, 13.107.18.10/31, 13.107.128.0/22, 23.103.160.0/20, 40.96.0.0/13, 40.104.0.0/15, 52.96.0.0/14, 131.253.33.215/32, 132.245.0.0/16, 150.171.32.0/22, 204.79.197.215/32, 2603:1006::/40, 2603:1016::/36, 2603:1026::/36, 2603:1036::/36, 2603:1046::/36, 2603:1056::/36, 2620:1ec:4::152/128, 2620:1ec:4::153/128, 2620:1ec:c::10/128, 2620:1ec:c::11/128, 2620:1ec:d::10/128, 2620:1ec:d::11/128, 2620:1ec:8f0::/46, 2620:1ec:900::/46, 2620:1ec:a92::152/128, 2620:1ec:a92::153/128	TCP: 587, 993, 995, 143
8	Default Required	No	*.outlook.com, autodiscover.<tenant>.onmicrosoft.com	TCP: 443, 80
9	Allow Required	Yes	*.protection.outlook.com 40.92.0.0/15, 40.107.0.0/16, 52.100.0.0/14, 52.238.78.88/32, 104.47.0.0/17, 2a01:111:f400::/48, 2a01:111:f403::/48	TCP: 443
10	Allow Required	Yes	*.mail.protection.outlook.com, *.mx.microsoft 40.92.0.0/15, 40.107.0.0/16, 52.100.0.0/14, 104.47.0.0/17, 2a01:111:f400::/48, 2a01:111:f403::/48	TCP: 25

SharePoint Online and OneDrive for Business

[\[+\] Expand table](#)

ID	Category	ER	Addresses	Ports
31	Optimize Required	Yes	*.sharepoint.com 13.107.136.0/22, 40.108.128.0/17, 52.104.0.0/14, 104.146.128.0/17, 150.171.40.0/22, 2603:1061:1300::/40, 2620:1ec:8f8::/46, 2620:1ec:908::/46, 2a01:111:f402::/48	TCP: 443, 80
32	Default Optional	No	ssw.live.com, storage.live.com	TCP: 443
	Notes: OneDrive for Business: supportability, telemetry, APIs, and embedded email links			
33	Default Optional	No	*.search.production.apac.trafficmanager.net, *.search.production.emea.trafficmanager.net, *.search.production.us.trafficmanager.net	TCP: 443
	Notes: SharePoint Hybrid Search - Endpoint to SearchContentService where the hybrid crawler feeds documents			
35	Default Required	No	*.wns.windows.com, admin.onedrive.com, officeclient.microsoft.com	TCP: 443, 80
36	Default Required	No	g.live.com, oneclient.sfx.ms	TCP: 443, 80
37	Default Required	No	*.sharepointonline.com, spoprod-a.akamaihd.net	TCP: 443, 80
39	Default Required	No	*.svc.ms	TCP: 443, 80

Microsoft Teams

[+] Expand table

ID	Category	ER	Addresses	Ports
11	Optimize Required	Yes	52.112.0.0/14, 52.122.0.0/15, 2603:1063::/38	UDP: 3478,

ID	Category	ER	Addresses	Ports
				3479, 3480, 3481
12	Allow Required	Yes	*.lync.com, *.teams.microsoft.com, teams.microsoft.com 52.112.0.0/14, 52.122.0.0/15, 52.238.119.141/32, 52.244.160.207/32, 2603:1027::/48, 2603:1037::/48, 2603:1047::/48, 2603:1057::/48, 2603:1063::/38, 2620:1ec:6::/48, 2620:1ec:40::/42	TCP: 443, 80
16	Default Required	No	*.keydelivery.mediaservices.windows.net, *.streaming.mediaservices.windows.net, mlcdn.blob.core.windows.net	TCP: 443
17	Default Required	No	aka.ms	TCP: 443
18	Default Optional Notes: Federation with Skype and public IM connectivity: Contact picture retrieval	No	*.users.storage.live.com	TCP: 443
19	Default Optional Notes: Applies only to those who deploy the Conference Room Systems	No	adl.windows.com	TCP: 443, 80
27	Default Required	No	*.secure.skyapeassets.com, mlcdnprod.azureedge.net	TCP: 443
127	Default Required	No	*.skype.com	TCP: 443, 80
180	Default Required	No	compass-ssl.microsoft.com	TCP: 443

Microsoft 365 Common and Office Online

[\[+\] Expand table](#)

ID	Category	ER	Addresses	Ports
46	Allow Required	Yes	*.officeapps.live.com, *.online.office.com, office.live.com 13.107.6.171/32, 13.107.18.15/32, 13.107.140.6/32, 52.108.0.0/14, 52.244.37.168/32, 2603:1006:1400::/40, 2603:1016:2400::/40, 2603:1026:2400::/40, 2603:1036:2400::/40, 2603:1046:1400::/40, 2603:1056:1400::/40, 2603:1063:2000::/38, 2620:1ec:c::15/128, 2620:1ec:8fc::6/128, 2620:1ec:a92::171/128, 2a01:111:f100:2000::a83e:3019/128, 2a01:111:f100:2002::8975:2d79/128, 2a01:111:f100:2002::8975:2da8/128, 2a01:111:f100:7000::6fdd:6cd5/128, 2a01:111:f100:a004::bfeb:88cf/128	TCP: 443, 80
47	Default Required	No	*.office.net	TCP: 443, 80
49	Default Required	No	*.onenote.com	TCP: 443
50	Default Optional Notes: OneNote notebooks (wildcards)	No	*.microsoft.com	TCP: 443
51	Default Required	No	*cdn.onenote.net	TCP: 443
53	Default Required	No	ajax.aspnetcdn.com, apis.live.net, officeapps.live.com, www.onedrive.com	TCP: 443
56	Allow Required	Yes	*.auth.microsoft.com, *.msftidentity.com, .msidentity.com, account.activedirectory.windowsazure.com, accounts.accesscontrol.windows.net, adminwebservice.microsoftonline.com, api.passwordreset.microsoftonline.com, autologon.microsoftazuresso.com, becws.microsoftonline.com, ccs.login.microsoftonline.com, clientconfig.microsoftonline-p.net, companymanager.microsoftonline.com,	TCP: 443, 80

ID	Category	ER	Addresses	Ports
			device.login.microsoftonline.com, graph.microsoft.com, graph.windows.net, login-us.microsoftonline.com, login.microsoft.com, login.microsoftonline-p.com, login.microsoftonline.com, login.windows.net, logincert.microsoftonline.com, loginex.microsoftonline.com, nexus.microsoftonline-p.com, passwordreset.microsoftonline.com, provisioningapi.microsoftonline.com 20.20.32.0/19, 20.190.128.0/18, 20.231.128.0/19, 40.126.0.0/18, 2603:1006:2000::/48, 2603:1007:200::/48, 2603:1016:1400::/48, 2603:1017::/48, 2603:1026:3000::/48, 2603:1027:1::/48, 2603:1036:3000::/48, 2603:1037:1::/48, 2603:1046:2000::/48, 2603:1047:1::/48, 2603:1056:2000::/48, 2603:1057:2::/48	
59	Default Required	No	*.hip.live.com, *.microsoftonline-p.com, *.microsoftonline.com, *.msauth.net, *.msauthimages.net, *.msecnd.net, *.msftauth.net, *.msftauthimages.net, *.phonefactor.net, enterpriseregistration.windows.net, policykeyservice.dc.ad.msft.net	TCP: 443, 80
64	Allow Required	Yes	*.compliance.microsoft.com, *.protection.office.com, *.security.microsoft.com, compliance.microsoft.com, defender.microsoft.com, protection.office.com, security.microsoft.com 13.107.6.192/32, 13.107.9.192/32, 52.108.0.0/14, 2620:1ec:4::192/128, 2620:1ec:a92::192/128	TCP: 443
66	Default Required	No	*.portal.cloudappsecurity.com	TCP: 443
67	Default Optional	No	*.blob.core.windows.net	TCP: 443
	Notes: Security and Compliance Center eDiscovery export			
68	Default Optional	No	firstpartyapps.oaspapps.com, prod.firstpartyapps.oaspapps.com.akadns.net, telemetryservice.firstpartyapps.oaspapps.com, wus-firstpartyapps.oaspapps.com	TCP: 443
	Notes: Portal and shared: 3rd party office integration. (including CDNs)			

ID	Category	ER	Addresses	Ports
69	Default Required	No	*.aria.microsoft.com, *.events.data.microsoft.com	TCP: 443
70	Default Required	No	*.o365weve.com, amp.azure.net, appsforoffice.microsoft.com, assets.onestore.ms, auth.gfx.ms, c1.microsoft.com, dgps.support.microsoft.com, docs.microsoft.com, msdn.microsoft.com, platform.linkedin.com, prod.msocdn.com, shellprod.msocdn.com, support.microsoft.com, technet.microsoft.com	TCP: 443
71	Default Required	No	*.office365.com	TCP: 443, 80
73	Default Required	No	*.aadrm.com, *.azurerms.com, *.informationprotection.azure.com, ecn.dev.virtualearth.net, informationprotection.hosting.portal.azure.net	TCP: 443
75	Default Optional Notes: Graph.windows.net, Office 365 Management Pack for Operations Manager, SecureScore, Azure AD Device Registration, Forms, StaffHub, Application Insights, captcha services	No	*.sharepointonline.com, dc.services.visualstudio.com, mem gfx.ms, staffhub.ms, staffhubweb.azureedge.net	TCP: 443
78	Default Optional Notes: Some Office 365 features require endpoints within these domains (including CDNs). Many specific FQDNs within these wildcards have been published recently as we work to either remove or better	No	*.microsoft.com, *.msocdn.com, *.onmicrosoft.com	TCP: 443, 80

ID	Category	ER	Addresses	Ports
			explain our guidance relating to these wildcards.	
79	Default Required	No	o15.officeredir.microsoft.com, officepreviewredir.microsoft.com, officeredir.microsoft.com, r.office.microsoft.com	TCP: 443, 80
83	Default Required	No	activation.sls.microsoft.com	TCP: 443
84	Default Required	No	crl.microsoft.com	TCP: 443, 80
86	Default Required	No	office15client.microsoft.com, officeclient.microsoft.com	TCP: 443
89	Default Required	No	go.microsoft.com	TCP: 443, 80
91	Default Required	No	ajax.aspnetcdn.com, cdn.ocd.officeapps.live.com	TCP: 443, 80
92	Default Required	No	officedcdn.microsoft.com, officedcdn.microsoft.com.edgesuite.net, otelrules.azureedge.net	TCP: 443, 80
93	Default Optional Notes: ProPlus: auxiliary URLs	No	*.virtualearth.net, c.bing.net, ocos-office365- s2s.msedge.net, tse1.mm.bing.net, www.bing.com	TCP: 443, 80
95	Default Optional Notes: Outlook for Android and iOS	No	*.acompli.net, *.outlookmobile.com	TCP: 443
96	Default Optional Notes: Outlook for Android and iOS: Authentication	No	login.windows-ppe.net	TCP: 443
97	Default Optional Notes: Outlook for	No	account.live.com, login.live.com	TCP: 443

ID	Category	ER	Addresses	Ports
	Android and iOS: Consumer Outlook.com and OneDrive integration			
105	Default Optional Notes: Outlook for Android and iOS: Outlook Privacy	No	www.acompli.com	TCP: 443
114	Default Optional Notes: Office Mobile URLs	No	*.appex-rf.msn.com, *.appex.bing.com, c.bing.com, c.live.com, d.docs.live.net, docs.live.net, partnerservices.getmicrosoftkey.com, signup.live.com	TCP: 443, 80
116	Default Optional Notes: Office for iPad URLs	No	account.live.com, auth.gfx.ms, login.live.com	TCP: 443, 80
117	Default Optional Notes: Yammer	No	*.yammer.com, *.yammerusercontent.com	TCP: 443
118	Default Optional Notes: Yammer CDN	No	*.assets-yammer.com	TCP: 443
121	Default Optional Notes: Planner: auxiliary URLs	No	www.outlook.com	TCP: 443, 80
122	Default Optional Notes: Sway CDNs	No	eus-www.sway-cdn.com, eus-www.sway-extensions.com, wus-www.sway-cdn.com, wus-www.sway-extensions.com	TCP: 443
124	Default Optional Notes: Sway	No	sway.com, www.sway.com	TCP: 443
125	Default Required	No	*.entrust.net, *.geotrust.com, *.omniroot.com, *.public-trust.com, *.symcb.com, *.symcd.com, *.verisign.com, *.verisign.net, apps.identrust.com, cacerts.digicert.com, cert.int-x3.letsencrypt.org, crl.globalsign.com, crl.globalsign.net, crl.identrust.com, crl3.digicert.com, crl4.digicert.com, isrg.trustid.ocsp.identrust.com,	TCP: 443, 80

ID	Category	ER	Addresses	Ports
			mscrl.microsoft.com, ocsp.digicert.com, ocsp.globalsign.com, ocsp.msocsp.com, ocsp2.globalsign.com, ocspx.digicert.com, secure.globalsign.com, www.digicert.com, www.microsoft.com	
126	Default Optional Notes: Connection to the speech service is required for Office Dictation features. If connectivity is not allowed, Dictation will be disabled.	No	officespeech.platform.bing.com	TCP: 443
147	Default Required	No	*.office.com, www.microsoft365.com	TCP: 443, 80
152	Default Optional Notes: These endpoints enables the Office Scripts functionality in Office clients available through the Automate tab. This feature can also be disabled through the Office 365 Admin portal.	No	*.microsoftusercontent.com	TCP: 443
153	Default Required	No	*.azure-apim.net, *.flow.microsoft.com, *.powerapps.com, *.powerautomate.com	TCP: 443
156	Default Required	No	*.activity.windows.com, activity.windows.com	TCP: 443
158	Default Required	No	*.cortana.ai	TCP: 443
159	Default Required	No	admin.microsoft.com	TCP: 443, 80

ID	Category	ER	Addresses	Ports
160	Default Required	No	cdn.odc.officeapps.live.com, cdn.uci.officeapps.live.com	TCP: 443, 80
184	Default Required	No	*.cloud.microsoft, *.static.microsoft, *.usercontent.microsoft	TCP: 443, 80

Related Topics

[Additional endpoints not included in the Microsoft 365 IP Address and URL Web service](#)

[Managing Microsoft 365 endpoints](#)

[General Microsoft Stream endpoints](#)

[Monitor Microsoft 365 connectivity](#)

[Client connectivity ↗](#)

[Content delivery networks ↗](#)

[Microsoft Azure IP Ranges and Service Tags – Public Cloud ↗](#)

[Microsoft Azure IP Ranges and Service Tags – US Government Cloud ↗](#)

[Microsoft Azure IP Ranges and Service Tags – China Cloud ↗](#)

[Microsoft Public IP Space ↗](#)

[Service Name and Transport Protocol Port Number Registry ↗](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Microsoft 365 U.S. Government DoD endpoints

Article • 07/31/2024

Applies To: Microsoft 365 Admin

Microsoft 365 requires connectivity to the Internet. The endpoints below should be reachable for customers using Microsoft 365 U.S. Government DoD plans only.

Microsoft 365 endpoints: [Worldwide \(including GCC\)](#) | [Microsoft 365 operated by 21 Vianet](#) | [Microsoft 365 U.S. Government DoD](#) | [Microsoft 365 U.S. Government GCC High](#)

[] Expand table

Notes	Download
Last updated: 07/31/2024 -  Change Log subscription ↗	Download: the full list in JSON format ↗

Start with [Managing Microsoft 365 endpoints](#) to understand our recommendations for managing network connectivity using this data. Endpoints data is updated as needed at the beginning of each month with new IP Addresses and URLs published 30 days in advance of being active. This lets customers who don't yet have automated updates to complete their processes before new connectivity is required. Endpoints may also be updated during the month if needed to address support escalations, security incidents, or other immediate operational requirements. The data shown on this page below is all generated from the REST-based web services. If you're using a script or a network device to access this data, you should go to the [Web service](#) directly.

Endpoint data below lists requirements for connectivity from a user's machine to Microsoft 365. It doesn't include network connections from Microsoft into a customer network, sometimes called hybrid or inbound network connections. For more information, see [Additional endpoints not included in the web service](#).

The Microsoft 365 suite is broken down into four major service areas representing the three primary workloads and a set of common resources. These service areas may be used to associate traffic flows with a particular application, however given that features often consume endpoints across multiple workloads, these service areas cannot effectively be used to restrict access.

Data columns shown are:

- **ID**: The ID number of the row, also known as an endpoint set. This ID is the same as is returned by the web service for the endpoint set.
- **Category**: Shows whether the endpoint set is categorized as "Optimize", "Allow", or "Default". You can read about these categories and guidance for management of them at <https://aka.ms/pnc>. This column also lists which endpoint sets are required to have network connectivity. For endpoint sets that aren't required to have network connectivity, we provide notes in this field to indicate what functionality would be missing if the endpoint set is blocked. If you're excluding an entire service area, the endpoint sets listed as required don't require connectivity.
- **ER**: This is **Yes** if the endpoint set is supported over Azure ExpressRoute with Microsoft 365 route prefixes. The BGP community that includes the route prefixes shown aligns with the service area listed. When ER is **No**, this means that ExpressRoute isn't supported for this endpoint set. However, it shouldn't be assumed that no routes are advertised for an endpoint set where ER is **No**. If you plan to use Microsoft Entra Connect, read the [special considerations section](#) to ensure you have the appropriate Microsoft Entra Connect configuration.
- **Addresses**: Lists the FQDNs or wildcard domain names and IP Address ranges for the endpoint set. Note that an IP Address range is in CIDR format and may include many individual IP Addresses in the specified network.
- **Ports**: Lists the TCP or UDP ports that are combined with the Addresses to form the network endpoint. You may notice some duplication in IP Address ranges where there are different ports listed.

Exchange Online

[] Expand table

ID	Category	ER	Addresses	Ports
1	Optimize Required	Yes	outlook-dod.office365.us, webmail.apps.mil 20.35.192.0/20, 40.66.24.0/21, 2001:489a:2200:500::/56, 2001:489a:2200:700::/56	TCP: 443, 80
4	Default Required	Yes	outlook-dod.office365.us, webmail.apps.mil	TCP: 143, 25, 587, 993, 995

ID	Category	ER	Addresses	Ports
5	Default Required	Yes	attachments-dod.office365-net.us, autodiscover-s-dod.office365.us, autodiscover.<tenant>.mail.onmicrosoft.com, autodiscover.<tenant>.mail.onmicrosoft.us, autodiscover.<tenant>.onmicrosoft.com, autodiscover.<tenant>.onmicrosoft.us	TCP: 443, 80
6	Allow Required	Yes	*.protection.apps.mil, *.protection.office365.us 23.103.191.0/24, 23.103.199.0/25, 23.103.204.0/22, 2001:489a:2202::/62, 2001:489a:2202:8::/62, 2001:489a:2202:2000::/63	TCP: 25, 443
34	Default Required	No	admin.exchange.apps.mil	TCP: 443

SharePoint Online and OneDrive for Business

[\[+\] Expand table](#)

ID	Category	ER	Addresses	Ports
9	Optimize Required	Yes	*.dps.mil, *.sharepoint-mil.us 20.34.12.0/22, 2001:489a:2204:902::/63, 2001:489a:2204:c00::/63	TCP: 443, 80
10	Default Required	No	*.wns.windows.com, g.live.com, oneclient.sfx.ms	TCP: 443, 80
19	Allow Required	Yes	*.od.apps.mil, od.apps.mil	TCP: 443, 80
20	Default Required	No	*.svc.ms, az741266.vo.msecnd.net, spoprod-a.akamaihd.net, static.sharepointonline.com	TCP: 443, 80

Microsoft Teams

[\[+\] Expand table](#)

ID	Category	ER	Addresses	Ports
7	Optimize Required	Yes	*.dod.teams.microsoft.us, *.online.dod.skypeforbusiness.us, dod.teams.microsoft.us	TCP: 443 UDP: 3478,

ID	Category	ER	Addresses	Ports
			13.72.128.0/20, 52.127.64.0/21, 104.212.32.0/22, 195.134.240.0/22, 2001:489a:2250::/44	3479, 3480, 3481
21	Default Required	No	dodteamsapuiwebcontent.blob.core.usgovcloudapi.net, msteamsstatics.blob.core.usgovcloudapi.net, statics.teams.microsoft.com	TCP: 443
22	Allow Required	Yes	endpoint1-proddodcecompsvc- dodc.streaming.media.usgovcloudapi.net, endpoint1- proddodeacompsvc-dode.streaming.media.usgovcloudapi.net 52.181.167.113/32, 52.182.52.226/32, 2001:489a:2250::/44	TCP: 443

Microsoft 365 Common and Office Online

[\[+\] Expand table](#)

ID	Category	ER	Addresses	Ports
11	Allow Required	Yes	*.dod.online.office365.us 52.127.80.0/23, 2001:489a:2208:8000::/49	TCP: 443
12	Default Required	No	*.office365.us	TCP: 443, 80
13	Allow Required	Yes	*.auth.microsoft.us, *.gov.us.microsoftonline.com, dod- graph.microsoft.us, graph.microsoftazure.us, login.microsoftonline.us 20.140.232.0/23, 52.126.194.0/23, 2001:489a:3500::/50	TCP: 443
14	Default Required	No	*.msauth.net, *.msauthimages.us, *.msftauth.net, *.msftauthimages.us, clientconfig.microsoftonline-p.net, graph.windows.net, login-us.microsoftonline.com, login.microsoftonline-p.com, login.microsoftonline.com, login.windows.net, loginex.microsoftonline.com, mscrl.microsoft.com, nexus.microsoftonline-p.com, secure.aadcdn.microsoftonline-p.com	TCP: 443
15	Allow Required	Yes	portal.apps.mil, reports.apps.mil, webshell.dodsuite.office365.us, www.ohome.apps.mil 52.127.72.42/32, 52.127.76.42/32, 52.180.251.166/32, 52.181.24.112/32, 52.181.160.113/32, 52.182.24.200/32, 52.182.54.237/32	TCP: 443

ID	Category	ER	Addresses	Ports
16	Allow Required	Yes	*.osi.apps.mil, dod.loki.office365.us 52.127.72.0/21, 2001:489a:2206::/48	TCP: 443
17	Default Required	No	activation.sls.microsoft.com, crl.microsoft.com, go.microsoft.com, insertmedia.bing.office.net, ocsa.officeapps.live.com, ocsredir.officeapps.live.com, ocws.officeapps.live.com, office15client.microsoft.com, officedcdn.microsoft.com, officedcdn.microsoft.com.edgesuite.net, officepreviewredir.microsoft.com, officeredir.microsoft.com, ols.officeapps.live.com, r.office.microsoft.com	TCP: 443, 80
18	Default Required	No	cdn.odc.officeapps.live.com, mrodevicemgr.officeapps.live.com, odc.officeapps.live.com, officeclient.microsoft.com	TCP: 443, 80
24	Default Required	No	lpcres.delve.office.com	TCP: 443
25	Default Required	No	*.cdn.office.net	TCP: 443
26	Allow Required	Yes	*.compliance.apps.mil, *.security.apps.mil, compliance.apps.mil, scc.protection.apps.mil, security.apps.mil 23.103.204.0/22, 52.127.72.0/21	TCP: 443, 80
28	Default Required	No	activity.windows.com, dod.activity.windows.us	TCP: 443
29	Default Required	No	dod-mtis.cortana.ai	TCP: 443
30	Default Required	No	*.aadrm.us, *.informationprotection.azure.us	TCP: 443
31	Default Required	No	pf.events.data.microsoft.com, pf.pipe.aria.microsoft.com	TCP: 443, 80
32	Default Required	No	config.apps.mil	TCP: 443

Notes for this table:

- The Security and Compliance Center (SCC) provides support for Azure ExpressRoute for Microsoft 365. The same applies for many features exposed through the SCC such as Reporting, Auditing, eDiscovery (Premium), Unified DLP,

and Data Governance. Two specific features, PST Import and eDiscovery Export, currently don't support Azure ExpressRoute with only Microsoft 365 route filters due to their dependency on Azure Blob Storage. To consume those features, you need separate connectivity to Azure Blob Storage using any supportable Azure connectivity options, which include Internet connectivity or Azure ExpressRoute with Azure Public route filters. You have to evaluate establishing such connectivity for both of those features. The Microsoft 365 Information Protection team is aware of this limitation and is actively working to bring support for Azure ExpressRoute for Microsoft 365 as limited to Microsoft 365 route filters for both of those features.

- There are additional optional endpoints for Microsoft 365 Apps for enterprise that aren't listed and aren't required for users to launch Microsoft 365 Apps for enterprise applications and edit documents. Optional endpoints are hosted in Microsoft datacenters and don't process, transmit, or store customer data. We recommend that user connections to these endpoints be directed to the default Internet egress perimeter.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Microsoft 365 U.S. Government GCC High endpoints

Article • 07/31/2024

Applies To: Microsoft 365 Admin

Microsoft 365 requires connectivity to the Internet. The endpoints below should be reachable for customers using Microsoft 365 U.S. Government GCC High plans only.

Microsoft 365 endpoints: [Worldwide \(including GCC\)](#) | [Microsoft 365 operated by 21 Vianet](#) | [Microsoft 365 U.S. Government DoD](#) | [Microsoft 365 U.S. Government GCC High](#)

[+] [Expand table](#)

Notes	Download
Last updated: 07/31/2024 -  Change Log subscription ↗	Download: the full list in JSON format ↗

Start with [Managing Microsoft 365 endpoints](#) to understand our recommendations for managing network connectivity using this data. Endpoints data is updated as needed at the beginning of each month with new IP Addresses and URLs published 30 days in advance of being active. This lets customers who don't yet have automated updates to complete their processes before new connectivity is required. Endpoints may also be updated during the month if needed to address support escalations, security incidents, or other immediate operational requirements. The data shown on this page below is all generated from the REST-based web services. If you're using a script or a network device to access this data, you should go to the [Web service](#) directly.

Endpoint data below lists requirements for connectivity from a user's machine to Microsoft 365. It doesn't include network connections from Microsoft into a customer network, sometimes called hybrid or inbound network connections.

The Microsoft 365 suite is broken down into four major service areas representing the three primary workloads and a set of common resources. These service areas may be used to associate traffic flows with a particular application, however given that features often consume endpoints across multiple workloads, these service areas cannot effectively be used to restrict access.

Data columns shown are:

- **ID:** The ID number of the row, also known as an endpoint set. This ID is the same as is returned by the web service for the endpoint set.
- **Category:** Shows whether the endpoint set is categorized as "Optimize", "Allow", or "Default". You can read about these categories and guidance for management of them at <https://aka.ms/pnc>. This column also lists which endpoint sets are required to have network connectivity. For endpoint sets, which aren't required to have network connectivity, we provide notes in this field to indicate what functionality would be missing if the endpoint set is blocked. If you're excluding an entire service area, the endpoint sets listed as required don't require connectivity.
- **ER:** This is **Yes** if the endpoint set is supported over Azure ExpressRoute with Microsoft 365 route prefixes. The BGP community that includes the route prefixes shown aligns with the service area listed. When ER is **No**, this means that ExpressRoute isn't supported for this endpoint set. However, it shouldn't be assumed that no routes are advertised for an endpoint set where ER is **No**. If you plan to use Microsoft Entra Connect, read the [special considerations section](#) to ensure you have the appropriate Microsoft Entra Connect configuration.
- **Addresses:** Lists the FQDNs or wildcard domain names and IP Address ranges for the endpoint set. Note that an IP Address range is in CIDR format and may include many individual IP Addresses in the specified network.
- **Ports:** Lists the TCP or UDP ports that are combined with the Addresses to form the network endpoint. You may notice some duplication in IP Address ranges where there are different ports listed.

Exchange Online

[\[+\] Expand table](#)

ID	Category	ER	Addresses	Ports
1	Optimize Required	Yes	outlook.office365.us 20.35.208.0/20, 20.35.240.0/21, 40.66.16.0/21, 2001:489a:2200:100::/56, 2001:489a:2200:400::/56, 2001:489a:2200:600::/56	TCP: 443, 80
4	Default Required	Yes	attachments.office365-net.us, autodiscover-s.office365.us, autodiscover.<tenant>.mail.onmicrosoft.com, autodiscover. <tenant>.mail.onmicrosoft.us, autodiscover. <tenant>.onmicrosoft.com, autodiscover. <tenant>.onmicrosoft.us	TCP: 443, 80

ID	Category	ER	Addresses	Ports
5	Default Required	Yes	outlook.office365.us	TCP: 143, 25, 587, 993, 995
6	Allow Required	Yes	*.manage.office365.us, *.protection.office365.us, *.scc.office365.us, manage.office365.us, scc.office365.us 23.103.191.0/24, 23.103.199.128/25, 23.103.208.0/22, 52.227.182.149/32, 52.238.74.212/32, 52.244.65.13/32, 2001:489a:2202:4::/62, 2001:489a:2202:c::/62, 2001:489a:2202:2000::/63	TCP: 25, 443

SharePoint Online and OneDrive for Business

[\[+\] Expand table](#)

ID	Category	ER	Addresses	Ports
9	Optimize Required	Yes	*.sharepoint.us 20.34.8.0/22, 2001:489a:2204:800::/63, 2001:489a:2204:900::/63	TCP: 443, 80
10	Default Required	No	*.wns.windows.com, admin.onedrive.us, g.live.com, oneclient.sfx.ms	TCP: 443, 80
20	Default Required	No	*.svc.ms, az741266.vo.msecnd.net, spoprod-a.akamaihd.net, static.sharepointonline.com	TCP: 443, 80

Microsoft Teams

[\[+\] Expand table](#)

ID	Category	ER	Addresses	Ports
7	Optimize Required	Yes	13.72.144.0/20, 52.127.88.0/21, 104.212.44.0/22, 2001:489a:2240::/44	UDP: 3478, 3479, 3480, 3481
21	Default Required	No	msteamsstatics.blob.core.usgovcloudapi.net, statics.teams.microsoft.com, teamsapuiwebcontent.blob.core.usgovcloudapi.net	TCP: 443

ID	Category	ER	Addresses	Ports
31	Allow Required	Yes	*.gov.teams.microsoft.us, gov.teams.microsoft.us 13.72.144.0/20, 52.127.88.0/21, 104.212.44.0/22, 2001:489a:2240::/44	TCP: 443, 80

Microsoft 365 Common and Office Online

[\[+\] Expand table](#)

ID	Category	ER	Addresses	Ports
11	Allow Required	Yes	*.gov.online.office365.us 52.127.37.0/24, 52.127.82.0/23, 2001:489a:2208::/49	TCP: 443
13	Allow Required	Yes	*.auth.microsoft.us, *.gov.us.microsoftonline.com, graph.microsoft.us, graph.microsoftazure.us, login.microsoftonline.us 20.140.232.0/23, 52.126.194.0/23, 2001:489a:3500::/50	TCP: 443
14	Default Required	No	*.msauth.net, *.msauthimages.us, *.msftauth.net, *.msftauthimages.us, clientconfig.microsoftonline-p.net, graph.windows.net, login-us.microsoftonline.com, login.microsoftonline-p.com, login.microsoftonline.com, login.windows.net, loginex.microsoftonline.com, mscr1.microsoft.com, nexus.microsoftonline-p.com, secure.aadcdn.microsoftonline-p.com	TCP: 443
15	Default Required	No	officehome.msocdn.us, prod.msocdn.us	TCP: 443, 80
16	Allow Required	Yes	www.office365.us 52.227.170.242/32	TCP: 443, 80
17	Allow Required	Yes	*.osi.office365.us, gcchigh.loki.office365.us, tasks.office365.us 52.127.240.0/20, 2001:489a:2206::/48	TCP: 443
18	Default Required	No	*.office.delivery.microsoft.com, activation.sls.microsoft.com, crl.microsoft.com, go.microsoft.com, insertmedia.bing.office.net, mrodevicemgr.officeapps.live.com, ocsfa.officeapps.live.com, ocsredir.officeapps.live.com, ocws.officeapps.live.com, office15client.microsoft.com, officecdn.microsoft.com, officecdn.microsoft.com.edgesuite.net,	TCP: 443, 80

ID	Category	ER	Addresses	Ports
			officepreviewredir.microsoft.com, officeredir.microsoft.com, ols.officeapps.live.com, r.office.microsoft.com	
19	Default Required	No	cdn.odc.officeapps.live.com, odc.officeapps.live.com, officeclient.microsoft.com	TCP: 443, 80
23	Default Required	No	*.office365.us	TCP: 443, 80
24	Default Required	No	lpres.delve.office.com	TCP: 443
25	Default Required	No	*.cdn.office.net	TCP: 443
26	Allow Required	Yes	*.compliance.microsoft.us, *.security.microsoft.us, compliance.microsoft.us, scc.office365.us, security.microsoft.us 52.127.240.0/20, 52.227.182.149/32, 52.244.65.13/32, 195.134.252.0/24, 2001:489a:2209::/49	TCP: 443, 80
28	Default Required	No	activity.windows.com, gcc-high.activity.windows.us	TCP: 443
29	Default Required	No	gcch-mtis.cortana.ai	TCP: 443
30	Default Required	No	*.aadrm.us, *.informationprotection.azure.us	TCP: 443
32	Default Required	No	tb.events.data.microsoft.com, tb.pipe.aria.microsoft.com	TCP: 443, 80

Notes for this table:

- The Security and Compliance Center (SCC) provides support for Azure ExpressRoute for Microsoft 365. The same applies for many features exposed through the SCC such as Reporting, Auditing, eDiscovery (Premium), Unified DLP, and Data Governance. Two specific features, PST Import and eDiscovery Export, currently don't support Azure ExpressRoute with only Microsoft 365 route filters due to their dependency on Azure Blob Storage. To consume those features, you need separate connectivity to Azure Blob Storage using any supportable Azure connectivity options, which include Internet connectivity or Azure ExpressRoute with Azure Public route filters. You have to evaluate establishing such connectivity.

for both of those features. The Microsoft 365 Information Protection team is aware of this limitation and is actively working to bring support for Azure ExpressRoute for Microsoft 365 as limited to Microsoft 365 route filters for both of those features.

- There are additional optional endpoints for Microsoft 365 Apps for enterprise that aren't listed and aren't required for users to launch Microsoft 365 Apps for enterprise applications and edit documents. Optional endpoints are hosted in Microsoft data centers and don't process, transmit, or store customer data. We recommend that user connections to these endpoints be directed to the default Internet egress perimeter.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

URLs and IP address ranges for Microsoft 365 operated by 21Vianet

Article • 03/29/2024

Applies To: Microsoft 365 operated by 21Vianet - Small Business Admin, Microsoft 365 operated by 21Vianet - Admin

Summary: The following endpoints (FQDNs, ports, URLs, IPv4, and IPv6 prefixes) apply to Microsoft 365 operated by 21 Vianet and are designed to deliver productivity services to organizations using only these plans.

Microsoft 365 endpoints: [Worldwide \(including GCC\)](#) | [Microsoft 365 operated by 21 Vianet](#) | [Microsoft 365 U.S. Government DoD](#) | [Microsoft 365 U.S. Government GCC High](#) |

Last updated: 03/29/2024 -  [Change Log subscription](#) ↗

Download: all required and optional destinations in one [JSON formatted](#) ↗ list.

Start with [Managing Microsoft 365 endpoints](#) to understand our recommendations for managing network connectivity using this data. Endpoints data is updated as needed at the beginning of each month with new IP Addresses and URLs published 30 days in advance of being active. This allows for customers who don't yet have automated updates to complete their processes before new connectivity is required. Endpoints may also be updated during the month if needed to address support escalations, security incidents, or other immediate operational requirements. The data shown on this page below is all generated from the REST-based web services. If you're using a script or a network device to access this data, you should go to the [Web service](#) directly.

Endpoint data below lists requirements for connectivity from a user's machine to Microsoft 365. It doesn't include network connections from Microsoft into a customer network, sometimes called hybrid or inbound network connections.

The Microsoft 365 suite is broken down into four major service areas representing the three primary workloads and a set of common resources. These service areas may be used to associate traffic flows with a particular application, however given that features often consume endpoints across multiple workloads, these service areas cannot effectively be used to restrict access.

Data columns shown are:

- **ID:** The ID number of the row, also known as an endpoint set. This ID is the same as is returned by the web service for the endpoint set.
- **Category:** Shows whether the endpoint set is categorized as "Optimize", "Allow", or "Default". You can read about these categories and guidance for management of them at <https://aka.ms/pnc>. This column also lists which endpoint sets are required to have network connectivity. For endpoint sets, which aren't required to have network connectivity, we provide notes in this field to indicate what functionality would be missing if the endpoint set is blocked. If you're excluding an entire service area, the endpoint sets listed as required don't require connectivity.
- **ER:** This is **Yes** if the endpoint set is supported over Azure ExpressRoute with Microsoft 365 route prefixes. The BGP community that includes the route prefixes shown aligns with the service area listed. When ER is **No**, this means that ExpressRoute isn't supported for this endpoint set. However, it shouldn't be assumed that no routes are advertised for an endpoint set where ER is **No**.
- **Addresses:** Lists the FQDNs or wildcard domain names and IP Address ranges for the endpoint set. Note that an IP Address range is in CIDR format and may include many individual IP Addresses in the specified network.
- **Ports:** Lists the TCP or UDP ports that are combined with the Addresses to form the network endpoint. You may notice some duplication in IP Address ranges where there are different ports listed.

Exchange Online

 Expand table

ID	Category	ER	Addresses	Ports
1	Optimize Required	No	partner.outlook.cn 40.73.132.0/24, 40.73.164.128/25, 40.73.165.0/26, 42.159.40.0/24, 42.159.44.0/22, 42.159.163.128/25, 42.159.165.0/24, 42.159.172.0/22, 2406:e500:4010::/48, 2406:e500:4030::/53, 2406:e500:4030:800::/54, 2406:e500:4040::/53, 2406:e500:4040:800::/54, 2406:e500:4040:1000::/54, 2406:e500:4040:1400::/54, 2406:e500:4110::/48, 2406:e500:4210::/48, 2406:e500:4310::/48	TCP: 443, 80
2	Allow Required	No	*.protection.partner.outlook.cn 42.159.33.192/27, 42.159.36.0/24, 42.159.161.192/27, 42.159.164.0/24, 139.219.16.0/27, 139.219.17.0/24, 139.219.24.0/22, 139.219.145.0/27, 139.219.146.0/24	TCP: 25, 443, 53, 80

ID	Category	ER	Addresses	Ports
			139.219.156.0/22, 2406:e500:4420::/43, 2406:e500:4440::/43, 2406:e500:c020::/44, 2406:e500:c120::/44	
12	Default Required	No	*.partner.outlook.cn, attachments.office365-net.cn	TCP: 443, 80
20	Allow Required	No	*.partner.outlook.cn 40.73.132.0/24, 40.73.164.128/25, 40.73.165.0/26, 42.159.40.0/24, 42.159.44.0/22, 42.159.163.128/25, 42.159.165.0/24, 42.159.172.0/22, 2406:e500:4010::/48, 2406:e500:4030::/53, 2406:e500:4030:800::/54, 2406:e500:4040::/53, 2406:e500:4040:800::/54, 2406:e500:4040:1000::/54, 2406:e500:4040:1400::/54, 2406:e500:4110::/48, 2406:e500:4210::/48, 2406:e500:4310::/48	TCP: 587, 993, 995

SharePoint Online and OneDrive for Business

[+] Expand table

ID	Category	ER	Addresses	Ports
4	Allow Required	No	*.sharepoint.cn 40.73.129.0/24, 40.73.161.0/24, 42.159.38.0/23, 2406:e500:4600::/39	TCP: 443, 80
21	Default Required	No	*.wns.windows.com	TCP: 443, 80

Skype for Business Online and Microsoft Teams

[+] Expand table

ID	Category	ER	Addresses	Ports
3	Optimize Required	No	42.159.34.32/27, 42.159.34.64/27, 42.159.34.96/28, 42.159.162.32/27, 42.159.162.64/27, 42.159.162.96/28, 159.27.160.0/21, 2406:e500:4a00::/39	UDP: 3479, 3480, 3481, 3478
19	Allow Required	No	*.partner.lync.cn, *.teams.microsoftonline.cn, teams.microsoftonline.cn 40.72.124.128/28, 42.159.34.32/27, 42.159.34.64/27,	TCP: 443, 80

ID	Category	ER	Addresses	Ports
			42.159.34.96/28, 42.159.162.32/27, 42.159.162.64/27, 42.159.162.96/28, 159.27.160.0/21, 2406:e500:4a00::/39	

Microsoft 365 Common and Office Online

[\[+\] Expand table](#)

ID	Category	ER	Addresses	Ports
7	Allow Required	No	*.azure-mobile.cn, *.chinacloud-mobile.cn, *.chinacloudapi.cn, *.chinacloudapp.cn, *.chinacloudsites.cn, *.partner.microsoftonline-m-i.net.cn, *.partner.microsoftonline-m.net.cn, *.partner.microsoftonline-p.net.cn, *.partner.officewebapps.cn, *.windowsazure.cn, portal.partner.microsoftonline.cdnsvc.com, r4.partner.outlook.cn 23.236.126.0/24, 40.73.240.0/24, 40.73.242.0/24, 58.68.168.0/24, 112.25.33.0/24, 123.150.49.0/24, 125.65.247.0/24, 171.107.84.0/24, 180.210.232.0/24, 180.210.234.0/24, 209.177.86.0/24, 209.177.90.0/24, 209.177.94.0/24, 222.161.226.0/24, 2406:e500:4900::/48	TCP: 443, 80
8	Allow Required	No	*.onmschina.cn, *.partner.microsoftonline-i.net.cn, *.partner.microsoftonline.net.cn 101.28.252.0/24, 115.231.150.0/24, 123.235.32.0/24, 171.111.154.0/24, 175.6.10.0/24, 180.210.229.0/24, 211.90.28.0/24	TCP: 443, 80
9	Allow Required	No	*.partner.microsoftonline-p.cn 182.50.87.0/24	TCP: 443, 80
10	Allow Required	No	*.partner.microsoftonline.cn 103.9.8.0/22	TCP: 443, 80
11	Default Required	No	activation.sls.microsoft.com, crl.microsoft.com, odc.officeapps.live.com,	TCP: 443,

ID	Category	ER	Addresses	Ports
			officedcdn.microsoft.com, officeclient.microsoft.com	80
13	Default Required	No	*.msauth.cn, *.msauthimages.cn, *.msftauth.cn, *.msftauthimages.cn, login.microsoftonline.com	TCP: 443, 80
15	Default Required	No	loki.office365.cn	TCP: 443
16	Default Required	No	*.cdn.office.net, shellprod.msocdn.com	TCP: 443
17	Allow Required	No	*.auth.microsoft.cn, login.partner.microsoftonline.cn, microsoftgraph.chinacloudapi.cn 40.72.70.0/23, 52.130.2.32/27, 52.130.3.64/27, 52.130.17.192/27, 52.130.18.32/27, 2406:e500:5500::/48	TCP: 443, 80
18	Default Optional	No	*.aadrm.cn, *.protection.partner.outlook.cn	TCP: 443
	Notes: If using Exchange Online, follow Allow category guidance for *.protection.partner.outlook.cn			
22	Default Required	No	*.partner.office365.cn	TCP: 443, 80
23	Default Required	No	*.microsoftonline.cn	TCP: 443, 80

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Content Delivery Networks (CDNs)

Article • 12/27/2023

This article applies to Microsoft 365 Enterprise.

CDNs help keep Microsoft 365 fast and reliable for end users. Cloud services like Microsoft 365 use CDNs to cache static assets closer to the browsers requesting them to speed up downloads and reduce perceived end user latency. The information in this article will help you learn about Content Delivery Networks (CDNs) and how they're used by Microsoft 365.

What exactly is a CDN?

A CDN is a geographically distributed network consisting of proxy and file servers in datacenters connected by high-speed backbone networks. CDNs are used to reduce latency and load times for a specified set of files and objects in a web site or service. A CDN may have many thousands of endpoints for optimal servicing of incoming requests from any location.

CDNs are commonly used to provide faster downloads of generic content for a web site or service such as JavaScript files, icons and images, and can also provide private access to user content such as files in SharePoint document libraries, streaming media files, and custom code.

CDNs are used by most enterprise cloud services. Cloud services like Microsoft 365 have millions of customers downloading a mix of proprietary content (such as emails) and generic content (such as icons) at one time. It's more efficient to put images everyone uses, like icons, as close to the user's computer as possible. It isn't practical for every cloud service to build CDN datacenters that store this generic content in every metropolitan area, or even in every major Internet hub around the world, so some of these CDNs are shared.

How do CDNs make services work faster?

Downloading common objects like site images and icons over and over again can take up network bandwidth that can be better used for downloading important personal content, like email or documents. Because Microsoft 365 uses an architecture that includes CDNs, the icons, scripts, and other generic content can be downloaded from servers closer to client computers, making the downloads faster. This means faster access to your personal content, which is securely stored in Microsoft 365 datacenters.

CDNs help to improve cloud service performance in several ways:

- CDNs shift part of the network and file download burden away from the cloud service, freeing up cloud service resources for serving user content and other services by reducing the need to serve requests for static assets.
- CDNs are purpose built to provide low-latency file access by implementing high performance networks and file servers, and by leveraging updated network protocols such as [HTTP/2](#) with highly efficient compression and request multiplexing.
- CDN networks use many globally distributed endpoints to make content available as close as possible to users.

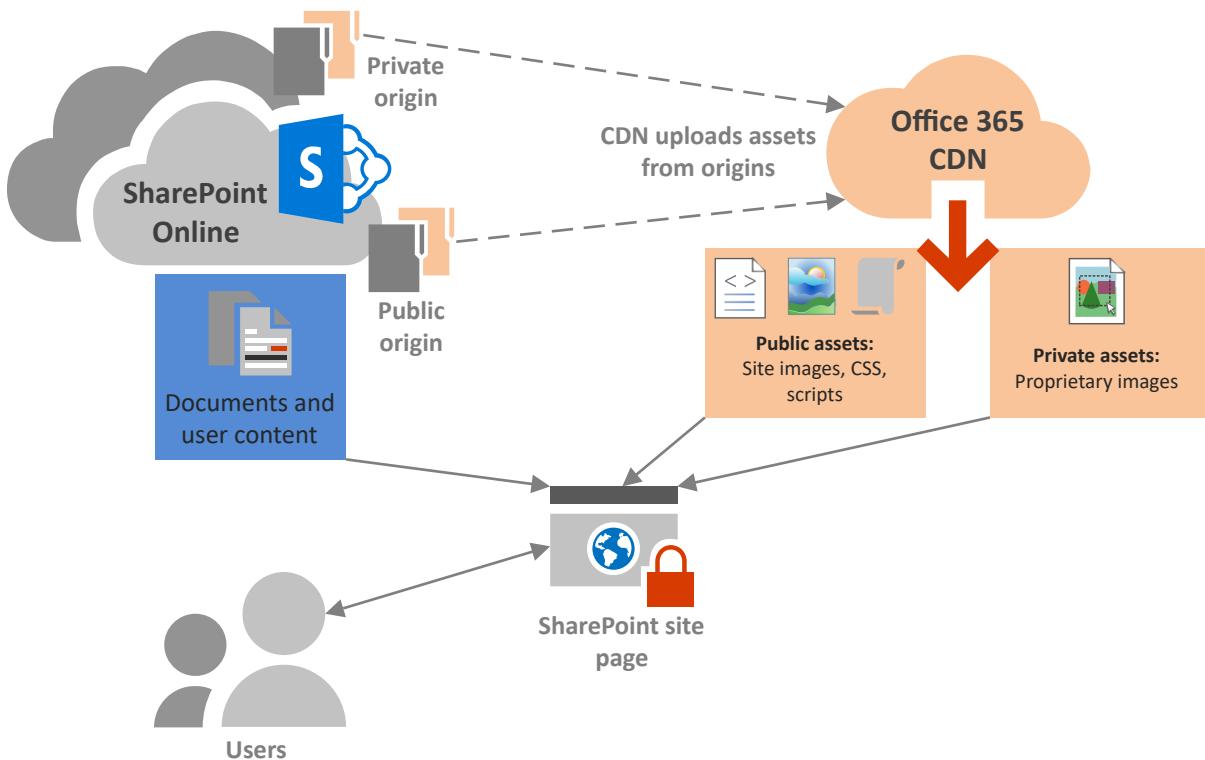
The Microsoft 365 CDN

The built-in Microsoft 365 Content Delivery Network (CDN) allows Microsoft 365 administrators to provide better performance for their organization's SharePoint pages by caching static assets closer to the browsers requesting them, which helps to speed up downloads and reduce latency. The Microsoft 365 CDN uses the [HTTP/2 protocol](#) for improved compression and download speeds.

Note

The Microsoft 365 CDN is only available to tenants in the **Production** (worldwide) cloud. Tenants in the US Government, China and Germany clouds do not currently support the Microsoft 365 CDN.

The Microsoft 365 CDN is composed of multiple CDNs that allow you to host static assets in multiple locations, or *origins*, and serve them from global high-speed networks. Depending on the kind of content you want to host in the Microsoft 365 CDN, you can add **public origins**, **private origins** or both.



Content in **public** origins within the Microsoft 365 CDN is accessible anonymously, and can be accessed by anyone who has URLs to hosted assets. Because access to content in public origins is anonymous, you should only use them to cache non-sensitive generic content such as JavaScript files, scripts, icons and images. The Microsoft 365 CDN is used by default for downloading generic resource assets like the Microsoft 365 client applications from a public origin.

Private origins within the Microsoft 365 CDN provide private access to user content such as SharePoint document libraries, sites and proprietary images. Access to content in private origins is secured with dynamically generated tokens so it can only be accessed by users with permissions to the original document library or storage location. Private origins in the Microsoft 365 CDN can only be used for SharePoint content, and you can only access assets through redirection from your SharePoint tenant.

The Microsoft 365 CDN service is included as part of your SharePoint subscription.

For more information about how to use the Microsoft 365 CDN, see [Use the Microsoft 365 content delivery network with SharePoint](#).

To watch a series of short videos that provide conceptual and HOWTO information about using the Microsoft 365 CDN, visit the [SharePoint Developer Patterns and Practices YouTube channel](#).

Other Microsoft CDNs

Although not a part of the Microsoft 365 CDN, you can use these CDNs in your Microsoft 365 tenant for access to SharePoint development libraries, custom code and other purposes that fall outside the scope of the Microsoft 365 CDN.

Azure CDN

Note

Beginning in Q3 2020, SharePoint will begin caching videos on the Azure CDN to support improved video playback and reliability. Popular videos will be streamed from the CDN endpoint closest to the user. This data will remain within the Microsoft Purview boundary. This is a free service for all tenants and it does not require any customer action to configure.

You can use the **Azure CDN** to deploy your own CDN instance for hosting custom web parts, libraries and other resource assets, which allows you to apply access keys to your CDN storage and exert greater control over your CDN configuration. Use of the Azure CDN isn't free, and requires an Azure subscription.

For more information on how to configure an Azure CDN instance, see [Quickstart: Integrate an Azure storage account with Azure CDN](#).

For an example of how the Azure CDN can be used to host SharePoint web parts, see [Deploy your SharePoint client-side web part to Azure CDN](#).

For information about the Azure CDN PowerShell module, see [Manage Azure CDN with PowerShell](#).

Microsoft Ajax CDN

Microsoft's **Ajax CDN** is a read-only CDN that offers many popular development libraries including jQuery (and all of its other libraries), ASP.NET Ajax, Bootstrap, Knockout.js, and others.

To include these scripts in your project, simply replace any references to these publicly available libraries with references to the CDN address instead of including it in your project itself. For example, use the following code to link to jQuery:

HTML

```
<script src="https://ajax.aspnetcdn.com/ajax/jquery-2.1.1.js"> </script>
```

For more information about how to use the Microsoft Ajax CDN, see [Microsoft Ajax CDN](#).

How does Microsoft 365 use content from a CDN?

Regardless of what CDN you configure for your Microsoft 365 tenant, the basic data retrieval process is the same.

1. Your client (a browser or Office client application) requests data from Microsoft 365.
2. Microsoft 365 either returns the data directly to your client or, if the data is part of a set of content hosted by the CDN, redirects your client to the CDN URL.
 - a. If the data is already cached in a *public* origin, your client downloads the data directly from the nearest CDN location to your client.
 - b. If the data is already cached in a *private* origin, the CDN service checks your Microsoft 365 user account's permissions on the origin. If you have permissions, SharePoint dynamically generates a custom URL composed of the path to the asset in the CDN and two access tokens, and returns the custom URL to your client. Your client then downloads the data directly from the nearest CDN location to your client using the custom URL.
3. If the data isn't cached at the CDN, the CDN node requests the data from Microsoft 365 and then caches the data for time after your client downloads the data.

The CDN figures out the closest datacenter to the user's browser and, using redirection, downloads the requested data from there. CDN redirection is quick, and can save users a lot of download time.

How should I set up my network so that CDNs work best with Microsoft 365?

Minimizing latency between clients on your network and CDN endpoints is the key consideration for ensuring optimal performance. You can use the best practices outlined in [Managing Microsoft 365 endpoints](#) to ensure that your network configuration permits client browsers to access the CDN directly rather than routing CDN traffic through central proxies to avoid introducing unnecessary latency.

You can also read [Microsoft 365 Network Connectivity Principles](#) to understand the concepts behind optimizing Microsoft 365 network performance.

Is there a list of all the CDNs that Microsoft 365 uses?

The CDNs in use by Microsoft 365 are always subject to change and in many cases there are multiple CDN partners configured in the event one is unavailable. The primary CDNs used by Microsoft 365 are:

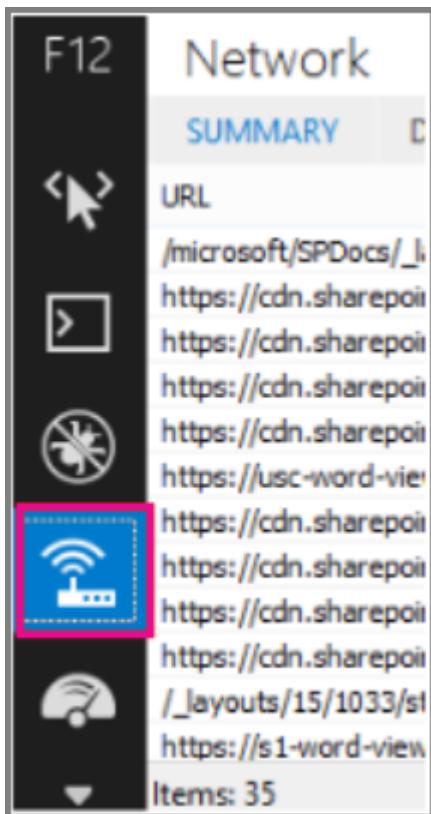
[] [Expand table](#)

CDN	Company	Usage	Link
Microsoft 365 CDN	Microsoft Azure	Generic assets in public origins, SharePoint user content in private origins	Microsoft Azure CDN
Azure CDN	Microsoft	Custom code, SharePoint Framework solutions	Microsoft Azure CDN
Microsoft Ajax CDN (read only)	Microsoft	Common libraries for Ajax, jQuery, ASP.NET, Bootstrap, Knockout.js etc.	Microsoft Ajax CDN

What performance gains does a CDN provide?

There are many factors involved in measuring specific differences in performance between data downloaded directly from Microsoft 365 and data downloaded from a specific CDN, such as your location relative to your tenant and to the nearest CDN endpoint, the number of assets on a page that are served by the CDN, and transient changes in network latency and bandwidth. However, a simple A/B test can help to show the difference in download time for a specific file.

The following screenshots illustrate the difference in download speed between the native file location in Microsoft 365 and the same file hosted on the [Microsoft Ajax Content Delivery Network](#). These screenshots are from the **Network** tab in the Internet Explorer 11 developer tools. These screenshots show the latency on the popular library jQuery. To bring up this screen, in Internet Explorer, press **F12** and select the **Network** tab, which is symbolized with a Wi-Fi icon.



This screenshot shows the library uploaded to the master page gallery on the SharePoint site itself. The time it took to upload the library is 1.51 seconds.

URL	Received	Taken	Initiator
/_catalogs/masterpage/javascript/jquery-2.1.1.min.js	82.98 KB	1.51 s	<script>
https://cdn.sharepointonline.com/12413/_layouts/15/16	18.98 KB	156 ms	<script>
/ScriptResource.axd?d=M1vNi_a6A2vtkOenP45i9-peGfx	100.80 KB	2.04 s	<script>

The second screenshot shows the same file delivered by Microsoft's CDN. This time the latency is around 496 milliseconds. This is a large improvement and shows that a whole second is shaved off the total time to download the object.

URL	Received	Taken
https://ajax.aspnetcdn.com/ajax/jQuery/jquery-2.1.1.min.js	82.74 KB	469 ms
/webResource.axd?d=nMv/y4UrC8wmUsI-GLXGjVJy4RM4H/qCK20lh3D5KbMXzSdwm5KlpDx9vM8MKkztZon...	22.33 KB	0.84 s
/_layouts/15/images/spcommon.png?rev=38	20.56 KB	1.15 s

Is my data safe?

We take great care to protect the data that runs your business. Data stored in the Microsoft 365 CDN is encrypted both in transit and at rest, and access to data in the Microsoft 365 SharePoint CDN is secured by Microsoft 365 user permissions and token authorization. Requests for data in the Microsoft 365 SharePoint CDN must be referred (redirected) from your Microsoft 365 tenant or an authorization token won't be generated.

To ensure that your data remains secure, we recommend that you never store user content or other sensitive data in a public CDN. Because access to data in a public CDN is anonymous, public CDNs should only be used to host generic content such as web script files, icons, images and other non-sensitive assets.

 **Note**

3rd party CDN providers may have privacy and compliance standards that differ from the commitments outlined by the Microsoft 365 Trust Center. Data cached through the CDN service may not conform to the Microsoft Data Processing Terms (DPT), and may be outside of the Microsoft 365 Trust Center compliance boundaries.

For in-depth information about privacy and data protection for Microsoft 365 CDN providers, visit the following:

- Learn more about Microsoft 365 privacy and data protection at the [Microsoft Trust Center ↗](#)
- Learn more about Akamai's privacy and data protection at the [Akamai Privacy Trust Center ↗](#)
- Learn more about Azure privacy and data protection at the [Azure Trust Center ↗](#)

How can I secure my network with all these 3rd party services?

Using an extensive set of partner services allows Microsoft 365 to scale and meet availability requirements and enhance the user experience when using Microsoft 365. The 3rd party services Microsoft 365 leverages include both certificate revocation lists; such as crl.microsoft.com or sa.symcb.com, and CDNs; such as r3.res.outlook.com. Every CDN FQDN generated by Microsoft 365 is a custom FQDN for Microsoft 365. If you're sent to a FQDN at the request of Microsoft 365, you can be assured that the CDN provider controls the FQDN and the underlying content at that location.

For customers that want to segregate requests destined for a Microsoft 365 datacenter from requests that are destined for a 3rd party, we've written up guidance on [Managing Microsoft 365 endpoints ↗](#).

Is there a list of all the FQDNs that leverage CDNs?

The list of FQDNs and how they leverage CDNs change over time. Refer to our published [Microsoft 365 URLs and IP address ranges](#) page to get up to date on the latest FQDNs that leverage CDNs.

You can also use the [Microsoft 365 IP Address and URL Web service](#) to request the current Microsoft 365 URLs and IP address ranges formatted as CSV or JSON.

Can I use my own CDN and cache content on my local network?

We're continually looking for new ways to support our customers' needs and are currently exploring the use of caching proxy solutions and other on-premises CDN solutions.

Although it isn't a part of the Microsoft 365 CDN, you can also use the [Azure CDN](#) for hosting custom web parts, libraries and other resource assets, which allows you to apply access keys to your CDN storage and exert greater control over your CDN configuration. Use of the Azure CDN isn't free, and requires an Azure subscription. For more information on how to configure an Azure CDN instance, see [Quickstart: Integrate an Azure storage account with Azure CDN](#).

I'm using Azure ExpressRoute for Microsoft 365, does that change things?

[Azure ExpressRoute for Microsoft 365](#) provides a dedicated connection to Microsoft 365 infrastructure that is segregated from the public internet. This means that clients will still need to connect over non-ExpressRoute connections to connect to CDNs and other Microsoft infrastructure that isn't explicitly included in the list of services supported by ExpressRoute. For more information about how to route specific traffic such as requests destined for CDNs, see [Implementing ExpressRoute for Microsoft 365](#).

Can I use CDNs with SharePoint Server on-premises?

Using CDNs only makes sense in a SharePoint context and should be avoided with SharePoint Server. This is because all of the advantages around geographic location don't hold true if the server is located on-premises or geographically close anyway. Additionally, if there's a network connection to the servers where it's hosted, then the site may be used without an Internet connection and therefore can't retrieve the CDN

files. Otherwise, you should use a CDN if there's one available and stable for the library and files you need for your site.

See also

[Microsoft 365 Network Connectivity Principles](#)

[Assessing Microsoft 365 network connectivity](#)

[Managing Microsoft 365 endpoints](#)

[Microsoft 365 URLs and IP address ranges](#)

[Use the Microsoft 365 content delivery network with SharePoint](#)

[Microsoft Trust Center ↗](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

IPv6 support in Microsoft 365 services

Article • 03/21/2024

With the growing adoption and support of IPv6 across enterprise networks, service providers, and devices, many customers are wondering if their users can continue to access Microsoft 365 services from IPv6 clients and IPv6 networks. Microsoft 365 services can be successfully used from both IPv6 dual stack and IPv6-only devices (IPv6-only devices require translation technologies such as DNS64 or NAT64). In fact, we have an increasing number of customers, from consumers to large enterprises, who are moving towards greater adoption of IPv6. For most customers, IPv4 won't completely disappear from their digital landscape, so we aren't planning to require IPv6 or to deprioritize IPv4 in any Microsoft 365 features or services.

One of our key priorities with Microsoft 365 is to ensure seamless customer and user experiences over the Internet from any location, from any device. This includes access to Microsoft 365 from customer devices that are using IPv6 in the dual stack configuration as well as transitioning to IPv6-only client deployments. In most cases, when you follow a standard Internet-based model of connecting to Microsoft 365 as described in [Microsoft 365 network connectivity principles](#), [Microsoft 365 URLs and IP address ranges](#), and [Microsoft 365 network planning best practices](#), IPv6 transitions won't be disruptive to your user experience.

Many Microsoft 365 services already provide native IPv6 support today and can be accessed directly from IPv6 dual stack and IPv6-only clients. Microsoft 365 also allows access through conventional IPv6 to IPv4 translation technologies (such as base 64 proxies or DNS64/NAT64) commonly used by customers and network solution providers to connect to IPv4 Internet resources.

As with any SaaS service and the Internet overall, the scope of natively IPv6 enabled Microsoft 365 interfaces, features, and APIs expands continuously and without direct customer action or control. If you're running IPv6 or IPv6-only services on your networks that need access to Microsoft 365 and the Internet, it's recommended that you include dynamic IPv6/IPv4 transitional mechanisms such as DNS64/NAT64 to ensure end-to-end IPv6 connectivity to Microsoft 365 without any further network reconfigurations.

Most of Microsoft 365 services have been or will be enabled with IPv6 capabilities transparently for end users and IT admins. Some Microsoft 365 scenarios (such as anonymous inbound e-mail) do have special requirements and considerations for use in conjunction with IPv6. For more details about scenario specific IPv6 requirements and considerations, contact your Microsoft account team or Microsoft support.

Here's a short link you can use to come back: <https://aka.ms/o365ip6>

See also

[Microsoft 365 Network Connectivity Overview](#)

[Managing Office 365 endpoints](#)

[Office 365 URLs and IP address ranges](#)

[Office 365 IP Address and URL Web service](#)

[Assessing Microsoft 365 network connectivity](#)

[Network planning and performance tuning for Microsoft 365](#)

[Office 365 performance tuning using baselines and performance history](#)

[Performance troubleshooting plan for Office 365](#)

[Content Delivery Networks](#)

[Microsoft 365 connectivity test](#)

[How Microsoft builds its fast and reliable global network](#)

[Office 365 Networking blog](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

NAT support with Office 365

Article • 06/26/2024

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Previously, guidance suggested that the maximum number of Exchange clients you should use per IP address to connect to Office 365 was about 2,000 clients per network port.

Why use NAT?

By using NAT, thousands of people on a corporate network can "share" a few publicly routable IP addresses.

Most corporate networks use private (RFC1918) IP address space. Private address space is allocated by the Internet Assigned Numbers Authority (IANA) and intended solely for networks that do not route directly to and from the global Internet.

To provide Internet access to devices on a private IP address space, organizations use gateway technologies like firewalls and proxies that provide network address translation (NAT) or port address translation (PAT) services. These gateways make traffic from internal devices to the Internet (including Office 365) appear to be coming from one or more publicly routable IP addresses. Each outbound connection from an internal device translates to a different source TCP port on the public IP address.

Why do you need to have so many connections open to Office 365 at the same time?

Outlook may open eight or more connections (in situations where there are add-ins, shared calendars, mailboxes, etc.). Because there are a maximum of 64,000 ports available on a Windows-based NAT device, there can be a maximum of 8,000 users behind an IP address before the ports are exhausted. Note that if customers are using non-Windows OS-based devices for NAT, the total available ports are dependent on what NAT device or software is being used. In this scenario, the maximum number of ports could be less than 64,000. Availability of ports is also affected by other factors such as Windows restricting 4,000 ports for its own use, which reduces the total number of available ports to 60,000. There may be other applications, such as Internet Explorer, that could connect at the same time, requiring additional ports.

Calculating maximum supported devices behind a single public IP address with Office 365

To determine the maximum number of devices behind a single public IP address, you should monitor network traffic to determine peak port consumption per client. Also, a peak factor should be used for the port usage (minimum 4).

Use the following formula to calculate the number of supported devices per IP address:

Maximum supported devices behind a single public IP address = $(64,000 - \text{restricted ports}) / (\text{Peak port consumption} + \text{peak factor})$

For example, if the following were true:

- **Restricted ports:** 4,000 for the operating system
- **Peak port consumption:** 6 per device
- **Peak factor:** 4

Then, the maximum supported devices behind a single public IP address = $(64,000 - 4,000) / (6 + 4) = 6,000$

With the release of Office 365 hosting pack, included in the updates from September 2011 for Microsoft Office Outlook 2007, or November 2011 for Microsoft Outlook 2010, or a later update, the number of connections from Outlook (both Office Outlook 2007 with Service Pack 2 and Outlook 2010) to Exchange can be as few as 2. You'll need to factor in the different operating systems, user behaviors, and so on to determine the minimum and maximum number of ports that your network will require at peak.

If you want to support more devices behind a single public IP address, follow the steps outlined to assess the maximum number of devices that can be supported:

Monitor network traffic to determine peak port consumption per client. You should collect this data:

- From multiple locations
- From multiple devices
- At multiple times

Use the preceding formula to calculate the maximum users per IP address that can be supported in their environment.

There are various methods for distributing client load across additional public IP addresses. Strategies available depend on the capabilities of the corporate gateway solution. The simplest solution is to segment your user address space and statically "assign" a number of IP addresses to each gateway. Another alternative that many gateway devices offer is the ability to use a pool of IP addresses. The benefit of the address pool is that it is much more dynamic and less likely to require adjustment as your user base grows.

See also

[Managing Office 365 endpoints ↗](#)

[Office 365 endpoints FAQ ↗](#)

Feedback

Was this page helpful?



Yes



No

[Provide product feedback ↗](#)

Network requests in Office for Mac

Article • 06/26/2024

Office for Mac applications provide a native app experience on the macOS platform. Each app is designed to work in a variety of scenarios, including states when no network access is available. When a machine is connected to a network, the applications automatically connect to a series of web-based services to provide enhanced functionality. The following information describes which endpoints and URLs the applications try to reach, and the services provided. This information is useful when troubleshooting network configuration issues and setting policies for network proxy servers. The details in this article are intended to complement the [Office 365 URL and address ranges article](#), which includes endpoints for computers running Microsoft Windows. Unless noted, the information in this article also applies to Office 2019 for Mac and Office 2016 for Mac, which are available as a one-time purchase from a retail store or through a volume licensing agreement.

Most of this article is tables detailing network URLs, type, and description of service or feature provided by that endpoint. Each of the Office apps may differ in its service and endpoint usage. The following apps are defined in the tables below:

- W: Word
- P: PowerPoint
- X: Excel
- O: Outlook
- N: OneNote

The URL type is defined as follows:

- ST: Static - The URL is hard-coded into the client application.
- SS: Semi-Static - The URL is encoded as part of a web page or redirector.
- CS: Config Service - The URL is returned as part of the Office Configuration Service.

Office for Mac default configuration

Installation and updates

The following network endpoints are used to download the Office for Mac installation program from the Microsoft Content Delivery Network (CDN).

[\[+\] Expand table](#)

URL	Type	Description
https://go.microsoft.com/fwlink/?linkid=846113	ST	Microsoft 365 Installation Portal forward link service to latest installation packages.
https://officecdn-microsoft-com.akamaized.net/	SS	Location of installation packages on the Content Delivery Network.
https://officecdn.microsoft.com/	SS	Location of installation packages on the Content Delivery Network.
https://officeci-mauservice.azurewebsites.net/	ST	Management Control endpoint for Microsoft AutoUpdate
https://officecdnmac.microsoft.com/		Enhanced content delivery network (CDN) for Microsoft AutoUpdate updates

First app launch

The following network endpoints are contacted on first launch of an Office app. These endpoints provide enhanced Office functionality for users, and the URLs are contacted regardless of license type (including Volume License installations).

[\[+\] Expand table](#)

URL	Apps	Type	Description
https://config.edge.skype.com/	WXPON	ST	'Flighting' Configuration - allows for feature light-up and experimentation.
https://ocos-office365-s2s.msedge.net/	WXPON	ST	'Flighting' Network Configuration Test
https://client-office365-tas.msedge.net/	WXPON	ST	'Flighting' Network Configuration Test
https://officeclient.microsoft.com/	WXPON	ST	Office Configuration Service - Master list of service endpoints.
https://nexusrules.officeapps.live.com/	WXPON	ST	Office Rules Telemetry download - Informs the client about what data and events to upload to the telemetry service.

URL	Apps	Type	Description
https://mobile.pipe.aria.microsoft.com/	N	CS	OneNote Telemetry Service
https://nexus.officeapps.live.com/	WXPON	ST	Office Telemetry Upload Reporting - "Heartbeat" and error events that occur on the client are uploaded to the telemetry service.
https://templateservice.office.com/	WXP	CS	Office Template Service - Provides users with online document templates.
https://omextemplates.content.office.net/	WXP	CS	Office Templates Downloads - Storage of PNG template images.
https://store.office.com/	WXP	CS	Store configuration for Office apps.
https://odc.officeapps.live.com/	WXPN	CS	Office Document Integration Services Catalog (list of services and endpoints) and Home Realm Discovery.
https://cdn.odc.officeapps.live.com/	WXPON	CS	Resources for Home Realm Discovery v2 (15.40 and later)
https://officecdn.microsoft.com/	WXPON	ST	Microsoft AutoUpdate Manifests - checks to see if there are updates available
https://ajax.aspnetcdn.com/	WXPO	SS	Microsoft Ajax JavaScript Library
https://wikipedia.firstpartyapps.oaspapps.com/	W	SS	Wikipedia app for Office configuration and resources.
https://excelbingmap.firstpartyapps.oaspapps.com/	X	SS	Bing Map app for Office configuration and resources.

URL	Apps	Type	Description
https://peoplegraph.firstpartyapps.oaspapps.com/	X	SS	People Graph app for Office configuration and resources.
https://www.onenote.com/	N	ST	What's New content for OneNote.
https://site-cdn.onenote.net/	N	ST	New content for OneNote.
https://site-cdn.onenote.net/	N	SS	What's New images for OneNote.
https://acompli.helpshift.com/	O	ST	In-app Support Service.
https://prod-global-autodetect.acompli.net/	O	ST	Email Account Detection Service.
https://autodiscover-s.outlook.com/	WXPO	ST	Outlook AutoDiscovery
https://outlook.office365.com/	WXPO	ST	Outlook endpoint for Microsoft 365 service.
https://r1.res.office365.com/	O	ST	Icons for Outlook add-ins.

ⓘ Note

The Office Configuration Service acts as an auto-discovery service for all Microsoft Office clients, not just for Mac. The endpoints returned in the response are semi-static in that change is very infrequent, but still possible.

Sign-in

The following network endpoints are contacted when signing in to cloud-based storage. Depending on your account type, different services may be contacted. For example:

- **MSA: Microsoft Account** - typically used for consumer and retail scenarios
- **OrgID: Organization Account** - typically used for commercial scenarios

[\[+\] Expand table](#)

URL	Apps	Type	Description
https://login.windows.net/	WXPON	ST	Windows Authorization Service
https://login.microsoftonline.com/	WXPON	ST	Microsoft 365 Login Service (OrgID)
https://login.live.com/	WXPON	ST	Microsoft Account Login Service (MSA)
https://auth.gfx.ms/	WXPON	CS	Microsoft Account Login Service Helper (MSA)
https://secure.aadcdn.microsoftonline-p.com/	WXPON	SS	Microsoft 365 Login Branding (OrgID)
https://ocws.officeapps.live.com/	WXPN	CS	Document and Places Storage Locator
https://roaming.officeapps.live.com/	WXPN	CS	Most Recently Used (MRU) document service

(!) Note

For subscription-based and retail licenses, signing in both activates the product, and enables access to cloud resources such as OneDrive. For Volume License installations, users are still prompted to sign-in (by default), but that is only required for access to cloud resources, as the product is already activated.

Product activation

The following network endpoints apply to Microsoft 365 Subscription and Retail License activations. Specifically, this does NOT apply to Volume License installations.

[+] [Expand table](#)

URL	Apps	Type	Description
https://ols.officeapps.live.com/	WXPON	CS	Office Licensing Service

What's New content

The following network endpoints apply to Microsoft 365 Subscription only.

[+] [Expand table](#)

URL	Apps	Type	Description
https://contentstorage.osi.office.net/	WXPO	SS	What's New JSON page content.

Researcher

The following network endpoints apply to Microsoft 365 Subscription only.

[\[+\] Expand table](#)

URL	Apps	Type	Description
https://entity.osi.office.net/	W	CS	Researcher Web Service
https://cdn.entity.osi.office.net/	W	CS	Researcher Static Content
https://www.bing.com/	W	CS	Researcher Content Provider

Smart Lookup

The following network endpoints apply to both Microsoft 365 Subscription and Retail/Volume License activations.

[\[+\] Expand table](#)

URL	Apps	Type	Description
https://uci.officeapps.live.com/	WXPN	CS	Insights Web Service
https://ajax.googleapis.com/	WXPN	CS	JQuery Library
https://cdnjs.cloudflare.com/	WXPN	CS	Supporting JavaScript Library
https://www.bing.com/	WXPN	CS	Insights Content Provider
https://tse1.mm.bing.net/	WXPN	CS	Insights Content Provider

PowerPoint Designer

The following network endpoints apply to Microsoft 365 Subscription only.

[\[+\] Expand table](#)

URL	Apps	Type	Description
https://pptsgs.officeapps.live.com/	P	CS	PowerPoint Designer web service

PowerPoint QuickStarter

The following network endpoints apply to Microsoft 365 Subscription only.

[\[+\] Expand table](#)

URL	Apps	Type	Description
https://pptcts.officeapps.live.com/	P	CS	PowerPoint QuickStarter web service

Send a Smile/Frown

The following network endpoints apply to both Microsoft 365 Subscription and Retail/Volume License activations.

[\[+\] Expand table](#)

URL	Apps	Type	Description
https://sas.office.microsoft.com/	WXPON	CS	Send a Smile Service

Contact Support

The following network endpoints apply to both Microsoft 365 Subscription and Retail/Volume License activations.

[\[+\] Expand table](#)

URL	Apps	Type	Description
https://powerlift-frontdesk.acompli.net/	O	CS	Contact Support Service
https://acompli.helpshift.com/	O	CS	In-app Support Service

Save As PDF

The following network endpoints apply to both Microsoft 365 Subscription and Retail/Volume License activations.

[\[+\] Expand table](#)

URL	Apps	Type	Description
https://wordcs.officeapps.live.com/	W	CS	Word document conversion service (PDF)

Office Apps (aka add-ins)

The following network endpoints apply to both Microsoft 365 Subscription and Retail/Volume License activations when Office App add-ins are trusted.

[\[+\] Expand table](#)

URL	Apps	Type	Description
https://store.office.com/	WXPO	CS	Office app store configuration
https://wikipedia.firstpartyapps.oaspapps.com/	W	SS	Wikipedia app resources
https://excelbingmap.firstpartyapps.oaspapps.com/	X	SS	Bing Map app resources
https://peoplegraph.firstpartyapps.oaspapps.com	X	SS	People Graph app resources
https://o15.officeredir.microsoft.com/	WPX	SS	Office Redirection Service
https://appsforoffice.microsoft.com/	WXP	SS	Office JavaScript Libraries
https://telemetry.firstpartyapps.oaspapps.com/	WX	SS	Telemetry and Reporting Service for Office apps
https://ajax.microsoft.com/	W	SS	Microsoft Ajax JavaScript Library
https://ajax.aspnetcdn.com/	X	SS	Microsoft Ajax JavaScript Library
https://c.microsoft.com/	WPXO	SS	Office JavaScript Libraries
https://c1.microsoft.com/	WPXO	SS	Support resources
https://cs.microsoft.com/	WPXO	SS	Support resources
https://c.bing.com/	WPXO	SS	Support resources
https://*.cdn.optimizely.com/	WPXO	SS	JavaScript library
https://errors.client.optimizely.com/	WPX	SS	Error reporting

URL	Apps	Type	Description
https://*-contentstorage.osi.office.net/	WPXO	SS	Font resources
https://nexus.ensighten.com/	WPXO	SS	Telemetry Service
https://browser.pipe.aria.microsoft.com/	WPXO	SS	Telemetry Reporting
https://*.vo.msecnd.net/	WPXO	SS	Microsoft Store Asset Library
https://*.wikipedia.org/	W	SS	Wikipedia page resources
https://upload.wikimedia.org/	W	SS	Wikipedia media resources
https://wikipedia.firstpartyappssandbox.oappseperate.com/	W	SS	Wikipedia sandbox frame
https://*.virtualearth.net/	X	SS	Map templates

Safe Links

The following network endpoint applies to all Office applications for Microsoft 365 Subscription only.

[\[+\] Expand table](#)

URL	Type	Description
https://*.oscs.protection.outlook.com/	CS	Microsoft Safe Link Service

Crash reporting

The following network endpoint applies to all Office applications for both Microsoft 365 Subscription and Retail/Volume License activations. When a process unexpectedly crashes, a report is generated and sent to the Watson service.

[\[+\] Expand table](#)

URL	Type	Description
https://watson.microsoft.com/	ST	Microsoft Error Reporting Service
https://officeci.azurewebsites.net/	ST	Office Collaborative Insights Service

Options for reducing network requests and traffic

The default configuration of Office for Mac provides the best user experience, both in terms of functionality and keeping the machine up to date. In some scenarios, you may wish to prevent applications from contacting network endpoints. This section discusses options for doing so.

Disabling Cloud Sign-In and Office Add-Ins

Volume License customers may have strict policies about saving documents to cloud-based storage. The following per-application preference can be set to disable MSA/OrgID Sign in, and access to Office Add-ins.

- `defaults write com.microsoft.Word UseOnlineContent -integer 0`
- `defaults write com.microsoft.Excel UseOnlineContent -integer 0`
- `defaults write com.microsoft.Powerpoint UseOnlineContent -integer 0`

If users try to access the Sign-In function, they will see an error that a network connection is not present. Because this preference also blocks online product activation, it should only be used for Volume License installations. Specifically, using this preference will prevent Office applications from accessing the following endpoints:

- `https://odc.officeapps.live.com`
- `https://*.firstpartyapps.oaspapps.com`
- All endpoints listed in the 'Sign In' section above.
- All endpoints listed in the 'Smart Lookup' section above.
- All endpoints listed in the 'Product Activation' section above.
- All endpoints listed in the 'Office Apps (aka add-ins)' section above.

To re-establish full functionality for the user, either set the preference to '2' or remove it.

Note

This preference requires Office for Mac build 15.25 [160726] or later.

Telemetry

Office for Mac sends telemetry information back to Microsoft at regular intervals. Data is uploaded to the 'Nexus' endpoint. The telemetry data helps the engineering team assess the health and any unexpected behaviors of each Office app. There are two categories of telemetry:

- **Heartbeat** contains version and license information. This data is sent immediately upon app launch.
- **Usage** contains information about how apps are being used and non-fatal errors. This data is sent every 60 minutes.

Microsoft takes your privacy very seriously. You can read about Microsoft's data collection policy at <https://privacy.microsoft.com>. To prevent applications from sending 'Usage' telemetry, the **SendAllTelemetryEnabled** preference can be adjusted. The preference is per-application, and can be set via macOS Configuration Profiles, or manually from Terminal:

```
defaults write com.microsoft.Word SendAllTelemetryEnabled -bool FALSE
```

```
defaults write com.microsoft.Excel SendAllTelemetryEnabled -bool FALSE
```

```
defaults write com.microsoft.Powerpoint SendAllTelemetryEnabled -bool FALSE
```

```
defaults write com.microsoft.Outlook SendAllTelemetryEnabled -bool FALSE
```

```
defaults write com.microsoft.onenote.mac SendAllTelemetryEnabled -bool FALSE
```

```
defaults write com.microsoft.autoupdate2 SendAllTelemetryEnabled -bool FALSE
```

```
defaults write com.microsoft.Office365ServiceV2 SendAllTelemetryEnabled -bool FALSE
```

Heartbeat telemetry is always sent and cannot be disabled.

Crash reporting

When a fatal application error occurs, the application will unexpectedly terminate and upload a crash report to the 'Watson' service. The crash report consists of a call-stack, which is the list of steps the application was processing leading up to the crash. These steps help the engineering team identify the exact function that failed and why.

In some cases, the contents of a document will cause the application to crash. If the app identifies the document as the cause, it will ask the user if it's okay to also send the document along with the call-stack. Users can make an informed choice to this question. IT administrators may have strict requirements about the transmission of documents and make the decision on behalf of the user to never send documents. The following preference can be set to prevent documents from being sent, and to suppress the prompt to the user:

```
defaults write com.microsoft.errorreporting IsAttachFilesEnabled -bool FALSE
```

Note

If **SendAllTelemetryEnabled** is set to **FALSE**, all crash reporting for that process is disabled. To enable crash reporting without sending usage telemetry, the following preference can be set: `defaults write com.microsoft.errorreporting IsMerpEnabled -bool TRUE`

Updates

Microsoft releases Office for Mac updates at regular intervals (typically once a month). We strongly encourage users and IT administrators to keep machines up to date to ensure the latest security fixes are installed. In cases where IT administrators want to closely control and manage machine updates, the following preference can be set to prevent the AutoUpdate process from automatically detecting and offering product updates:

```
defaults write com.microsoft.autoupdate2 HowToCheck -string 'Manual'
```

Blocking Requests with a Firewall/Proxy

If your organization blocks requests to URLs via a firewall or proxy server be sure to configure the URLs listed in this document as either allowed, or block listed with a 40X response (e.g. 403 or 404). A 40X response will allow the Office applications to gracefully accept the inability to access the resource, and will provide a faster user experience, than simply dropping the connection, which in turn will cause the client to retry.

If your proxy server requires authentication, a 407 response will be returned to the client. For the best experience, ensure that you're using Office for Mac builds 15.27 or later, as they include specific fixes for working with NTLM and Kerberos servers.

See also

[Office 365 URLs and IP address ranges](#)

Feedback

Was this page helpful?



Yes



No

[Provide product feedback ↗](#)

Network planning and performance tuning for Microsoft 365

Article • 08/28/2024

Before you deploy for the first time or migrate to Microsoft 365, you can use the information in these articles to estimate the bandwidth you need and then to test and verify that you have enough bandwidth to deploy or migrate to Microsoft 365. For an overview, see: [Network and migration planning for Microsoft 365](#).

[+] Expand table

Category	Description	Category	Description
Network planning 	<p>Want fast connections and pages that load quickly? Read Getting the best connectivity and performance in Microsoft 365. Read Microsoft 365 Network Connectivity Overview to understand concepts.</p>	Measuring your network 	<p>Read Microsoft 365 performance tuning using baselines and performance history and Performance troubleshooting plan for Microsoft 365. Use these tools to evaluate your existing network.</p>
Best practices 	<p>Best practices for network planning and improving migration performance for Microsoft 365. Want to get started helping your users right away? See Best practices for using Office 365 on a slow network. Microsoft 365 Network Connectivity Principles will help you understand the most recent guidance for securely optimizing Microsoft 365 network connectivity.</p>	Reference 	<p>Want the details, like a list of IP addresses and ports? See the Network planning reference for Microsoft 365.</p>
	<p>For the steps to optimize your network for Microsoft 365 and other Microsoft cloud platforms and services, see the Microsoft Cloud Networking for Enterprise Architects poster.</p>		

Performance tuning and troubleshooting resources for Microsoft 365

Once you have Microsoft 365 deployed, you can optimize your performance by using the articles in this section. If you experience performance degradation you can also use these articles to troubleshoot issues.

For information about using network address translation with Office 365, see [NAT support with Office 365](#). Also, take a look at the [top 10 tips for optimizing and troubleshooting your Office 365 network connectivity](#).

Tune Exchange Online performance: Use these articles to fine tune Exchange Online performance.

Prepare your organization's network for Microsoft Teams: Use these articles to optimize your network for Teams.

Tune Skype for Business Online performance: Use these articles to fine tune Skype for Business Online performance.

Tune SharePoint performance: Use these articles to fine tune SharePoint performance.

Tune Project Online performance ↗: Use this article to fine tune Project Online performance.

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Monitor Microsoft 365 connectivity

Article • 05/06/2024

Once you've deployed Microsoft 365, you can maintain Microsoft 365 connectivity using some of the tools and techniques below. You should understand the official [Service Health and Continuity](#) guidelines as well as our [Best practices for using Microsoft 365 on a slow network](#). You'll also want to grab the [Microsoft 365 admin app](#) and bookmark our [Microsoft 365 for business - Admin Help](#).

Monitoring Microsoft 365 Connectivity

[+] [Expand table](#)

Type of monitoring	Description
Getting notified of new Microsoft 365 endpoints	If you're Managing Microsoft 365 endpoints , you'll want to receive notifications when we publish new endpoints, you can subscribe to our RSS feed using your favorite RSS reader. Here's how to subscribe via Outlook or you can have the RSS feed updates emailed to you .
Use System Center to Monitor Microsoft 365	If you're using Microsoft System Center, you can download the Microsoft System Center Operations Manager Management Pack for Microsoft 365 to begin monitoring Microsoft 365 today. For more detailed guidance, see the management pack operations guide.
Monitoring the health of Azure ExpressRoute	If you're connecting to Microsoft 365 using Azure ExpressRoute for Microsoft 365, you'll want to ensure that you're using both the Microsoft 365 Service Health Dashboard as well as the Azure Reducing troubleshooting time with Azure Resource health
Using Microsoft Entra Connect Health with AD FS	If you're using AD FS for single sign-on with Microsoft 365, you'll want to begin using Microsoft Entra Connect Health to monitor your AD FS infrastructure .
Programmatically monitor Microsoft 365	Refer to our guidance on the Microsoft 365 Management API .

Here's a short link you can use to come back: <https://aka.ms/monitorconnectivity365>

Related articles

[Configure Microsoft 365 Enterprise services and applications](#)

[Get your organization ready for Microsoft 365 Enterprise](#)

[Network planning and performance tuning for Microsoft 365](#)

[Microsoft 365 integration with on-premises environments](#)

[Managing Microsoft 365 endpoints](#)

Feedback

Was this page helpful?

 Yes

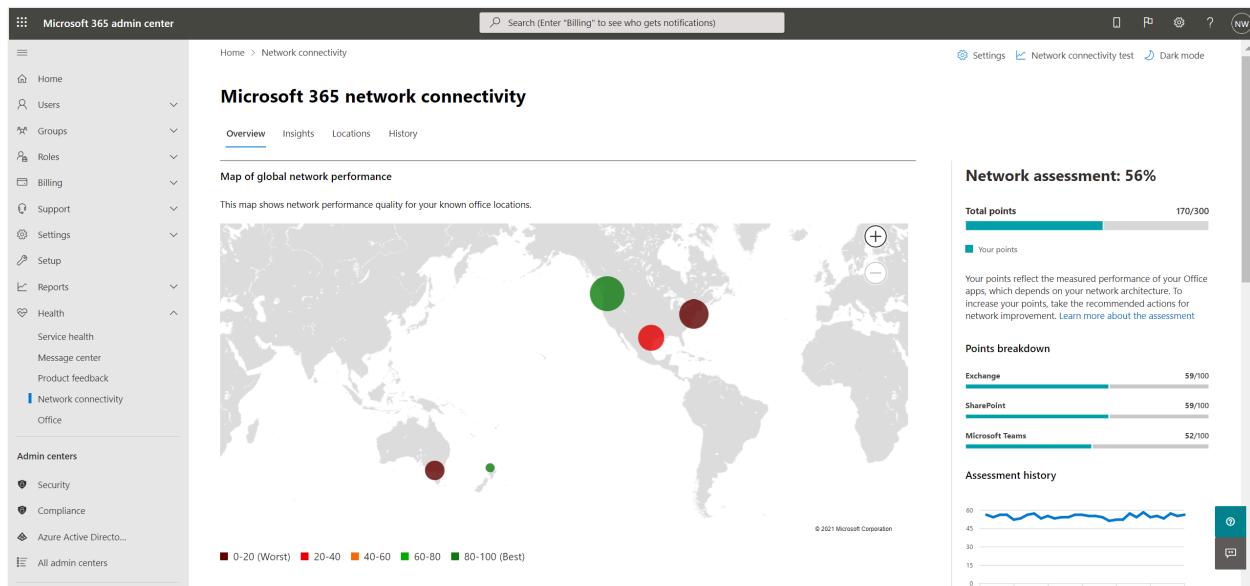
 No

[Provide product feedback ↗](#)

Network connectivity in the Microsoft 365 Admin Center

Article • 04/05/2024

The Microsoft 365 Admin Center now includes aggregated network connectivity metrics collected from your Microsoft 365 tenant and available to view only by administrative users in your tenant.



Network assessments and network insights are displayed in the Microsoft 365 Admin Center under **Health | Network connectivity**.



⚠ Note

Network connectivity in the Admin Center supports tenants in WW Commercial but not GCC Moderate, GCC High, DoD or China.

When you first navigate to the network performance page, you have to configure your locations in order to see the map of global network performance, a network assessment

scoped to the entire tenant, percentage of your users working remotely vs onsite, and a list of current issues to take action on and/or to research further. From the overview pane, you can drill down to view specific network performance metrics and issues by location. For more information, see [Network performance overview in the Microsoft 365 Admin Center](#).

To access the network connectivity page, you must be an administrator for the organization within Microsoft 365. The Report Reader administrative role will have read access to this information. To configure locations and other elements of network connectivity an administrator must have the Service Support Administrator role.

Prerequisites for network connectivity assessments to appear

To get started, turn on your location opt-in setting to automatically collect data from devices using Windows Location Services, go to your Locations list to add or upload location data, or run the Microsoft 365 network connectivity test from your office locations. These three options for office location information are detailed below. While network connectivity can be evaluated across the organization, any network design improvements need to be done for specific office locations. Network connectivity information is provided for each office location once those locations can be determined. There are three options for getting network assessments from your office locations:

1. Enable Windows Location Services

For this option, you must have at least two computers running at each office location that support the prerequisites. OneDrive for Windows version must be up-to-date and installed on each computer. Network tests are only run no more than once a day at a random time. Network measurements will be added to other Office 365 client applications soon.

Windows Location Service must be consented on the machines. You can test this by running the **Maps** app and locating yourself. It can be enabled on a single machine with **Settings | Privacy | Location** where the setting *Allow apps to access your location* must be enabled. Windows Location Services consent can be deployed to PCs using MDM or Group Policy with the setting *LetAppsAccessLocation*.

You don't need to add locations in the Admin Center with this method as they're automatically identified at the city resolution. Multiple office locations within the same city won't be shown when using Windows Location Services. Location information is rounded to the nearest 300 meters by 300 meters so that more precise location

information isn't accessed. Use of Windows Location Services for network measurements is off by default for customers. You must enable it in the Network Connectivity Settings Location flyout.

Locations

Choose to improve location detection and classification of remote and onsite connections to your network.

Location detection

To discover more office locations on your network, include location information in the Office app network data you're already sending to Microsoft. This sends information about the location without identifying any individual user or device. After turning on the setting, it can take up to 10 days before locations are discovered.

- Include location information in network data**

Users might see a "location in-use" notification on their device. [Learn more about location services](#)

The machines should have Wi-Fi networking rather than an ethernet cable. Machines with an ethernet cable don't have accurate location information.

Measurement samples and office locations should start to appear 24 hours after these prerequisites have been met. Office locations discovered from Windows Location Services are aggregated per City and are retained in your view for 90 days after samples are no longer received. If you choose to switch to office locations added by the Administrator with LAN subnet information, you can disable Windows Location Services and hide all of the discovered locations. They'll be removed after the 90 day period.

2. Add locations and provide LAN subnet information

For this option, neither Windows Location Services nor Wi-Fi is required. Your OneDrive for Windows version must be up-to-date and installed on at least one computer at the location and you must know your LAN subnet information for each of your offices. This option allows multiple office locations per city and you can name your office locations. You can also upload them from other sources.

Make sure that you also add locations in the **locations page** or import those from a CSV file. The locations added must include your office LAN subnet information. In the dialog for adding or editing a location, you can specify a number of LAN subnets and a number of public egress IP subnets. The LAN subnets are required and one of them must match the LAN subnet attribute on a received network assessment for results to show up. We now support matching of all subnets under a given network when you add

locations using LAN subnets. The main advantage with this is, you no longer need to define exact matches for LAN subnets when you add locations. For example, you added a location using /20 as the LAN subnet definition, in the network assessment we received a LAN subnet attribute containing /24 which is part of the supernet you defined using /20 and there's no other specific match for the /24 subnet, we'll map this network assessment to the location you added using the /20 LAN subnet definition.

Usually, LAN subnets are private IP address ranges as defined in RFC1918 such that the use of public IP addresses as the LAN subnets is likely to be incorrect. The dialog shows suggestions of LAN subnets that have been seen in recent network assessment tests for your organization so that you can choose.

If you add public egress IP addresses, these are used as a secondary differentiator and are intended for when you have multiple sites using the same LAN subnet IP address ranges. To make sure your test results show up, you should start by leaving the public egress IP address ranges blank. If they're included, then a test result must match both one of the LAN subnet IP address ranges and one of the public egress IP address ranges.

This option allows you to have multiple offices defined within a city.

All test measurements from client machines include the LAN subnet information, which is correlated with the office location details that you've entered. Measurement samples and office locations should start to appear 24 hours after these prerequisites have been met.

3. Manually gather test reports with the Microsoft 365 network connectivity test tool

For this option, you need to identify a person at each location. Ask them to browse to [Microsoft 365 network connectivity test](#) on a Windows machine on which they have administrative permissions. On the web site, they need to sign in to their Office 365 account for the same organization that you want to see the results. Then they should click **Run test**. During the test, there's a downloaded Connectivity test EXE. They need to open and execute that. Once the tests are completed, the test result is uploaded to the Admin Center.

Test reports are linked to a location if it was added with LAN subnet information, otherwise they're shown at the discovered City location only.

Measurement samples and office locations should start to appear 2-3 minutes after a test report is completed. For more information, see [Microsoft 365 network connectivity](#)

test.

Note

Currently, When adding your office locations to Microsoft 365 network connectivity in the Microsoft 365 admin center, you can provide only IPv4 addresses for your LAN subnets. Egress IP addresses must use IPv4.

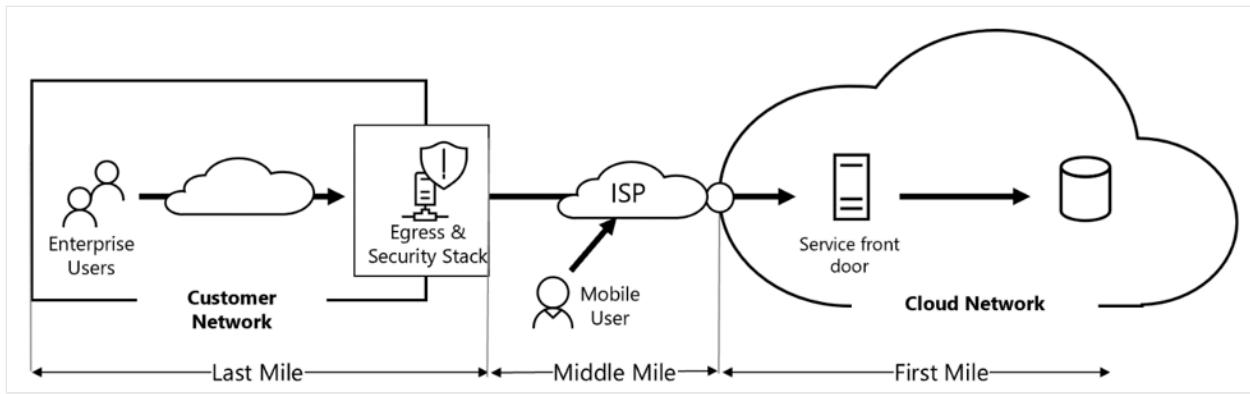
How do I use this information?

Network insights, their related performance recommendations and network assessments are intended to help in designing network perimeters for your office locations. Each insight provides details about the performance characteristics for a specific common networking issue for each geographic location where users are accessing your tenant. **Performance recommendations** for each network insight offer specific network architecture design changes you can make to improve user experience related to Microsoft 365 network connectivity. The network assessment shows how network connectivity impacts user experience, allowing for comparison of different user location network connections.

Network assessments distill an aggregate of many network performance metrics into a snapshot of your enterprise network health, represented by a points value from 0 - 100. Network assessments are scoped to both the entire tenant and for each geographic location from which users connect to your tenant, providing Microsoft 365 administrators with an easy way to instantly grasp a gestalt of the enterprise's network health and quickly drill down into a detailed report for any global office location.

Complex enterprises with multiple office locations and nontrivial network perimeter architectures can benefit from this information either during their initial onboarding to Microsoft 365 or to remediate network performance issues discovered with usage growth. This is usually not necessary for small businesses using Microsoft 365, or any enterprises who already have simple and direct network connectivity. Enterprises with over 500 users and multiple office locations are expected to benefit the most.

Enterprise network connectivity challenges



Many enterprises have network perimeter configurations, which have grown over time and are primarily designed to accommodate employee Internet web site access where most web sites aren't known in advance and are untrusted. The prevailing and necessary focus is avoiding malware and phishing attacks from these unknown web sites. This network configuration strategy, while helpful for security purposes, can lead to degradation of Microsoft 365 user performance and user experience.

How we can solve these challenges

Enterprises can improve general user experience and secure their environment by following [Office 365 connectivity principles](#) and by using the Microsoft 365 Admin Center network connectivity feature. In most cases, following these general principles will have a significant positive impact on end-user latency, service reliability, and overall performance of Microsoft 365.

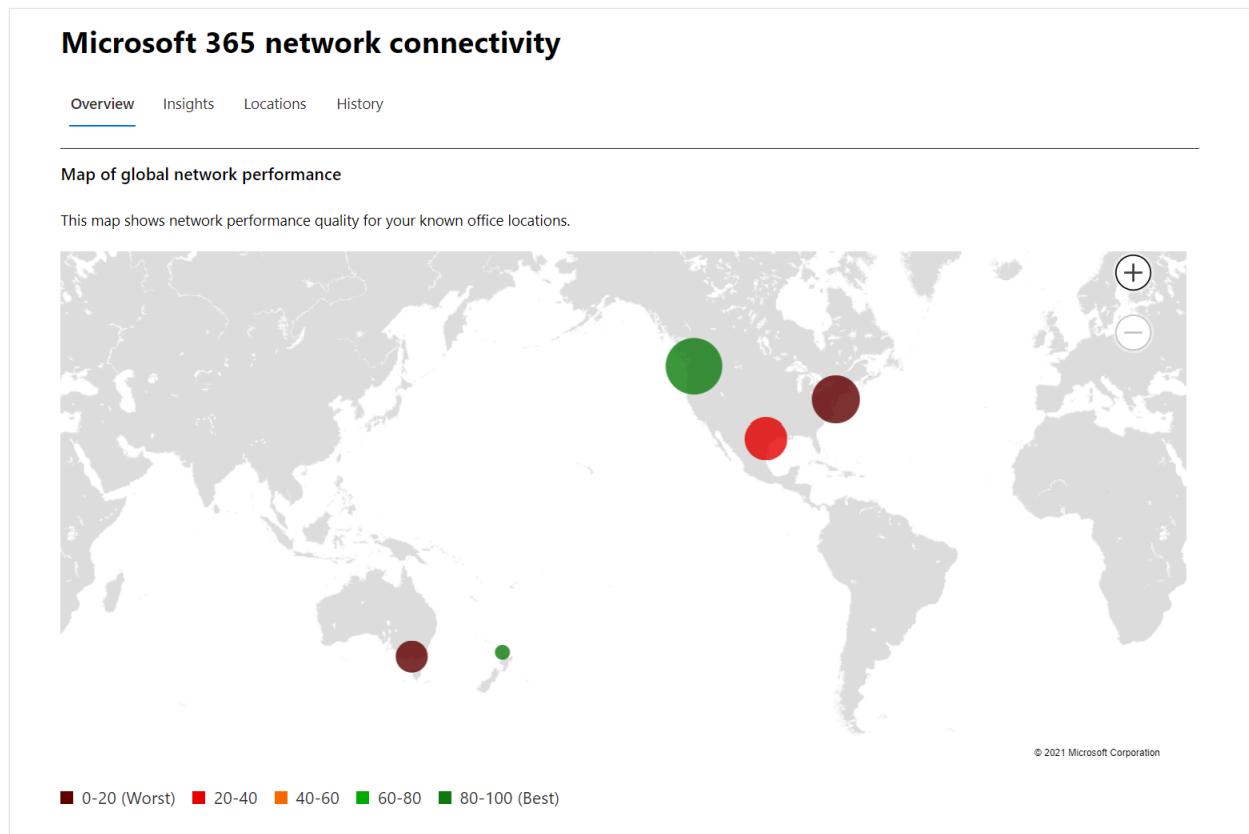
Microsoft is sometimes asked to investigate network performance issues with Microsoft 365 for large enterprise customers, and these frequently have a root cause related to the customer's network perimeter infrastructure. When a common root cause of a customer network perimeter issue is found, we seek to identify simple test measurements. A test with a measurement threshold that identifies a specific problem is valuable because we can test the same measurement at any location, tell whether this root cause is present there and share it as a network insight with the administrator.

Some network insights will merely indicate a problem that needs further investigation. A network insight where we have enough tests to show a specific remediation action to correct the root cause is listed as a **recommended action**. These recommendations, based on live metrics that reveal values that fall outside a predetermined threshold, are much more valuable than general best practice advice since they're specific to your environment and will show the actual improvement once the recommended changes have been made.

Network connectivity overview in the Microsoft 365 Admin Center

Microsoft has existing network measurements from several Office desktop and web clients, which support the operation of Microsoft 365. These measurements are now being used to provide network architecture design insights and a network assessment, which are shown in the **Network connectivity** page in the Microsoft 365 Admin Center.

By default, approximate location information associated with the network measurements identifies the city where client devices are located. The network assessment at each location is shown with color and the relative number of users at each location is represented by the size of the circle.



The overview page also shows the network assessment for the customer as a weighted average across all office locations.

Network assessment: 56%

Total points

170/300



Your points

Your points reflect the measured performance of your Office apps, which depends on your network architecture. To increase your points, take the recommended actions for network improvement. [Learn more about the assessment](#)

Points breakdown

Exchange

59/100



SharePoint

59/100



Microsoft Teams

52/100



Assessment history



Your assessment

You can view a table view of the locations where they can be filtered, sorted, and edited in the **Locations** tab. Locations with specific recommendations might also include an estimated potential latency improvement. This is calculated by taking the median latency of your organization users at the location and subtracting the median latency for all organizations in the same city.

Location type	City or location	Samples collected	Assessment	Insights	Potential improvement	Sharing and user-submitted reports
Office	Auckland, New Zealand	6.3%	94			None submitted
Office	Charleston	0.0%	0			None submitted
Office	Haizhou District, Jiangsu, China	0.0%	0			View
Office	Melbourne, Australia	10.6%	17	Egress, and 7 more	Potential 100 ms improvement	None submitted
Office	Philadelphia, PA, United States	16.9%	18	Egress, and 6 more	Potential 280 ms improvement	None submitted
Office	Redmond, WA, United States	21.1%	97			None submitted
Office	San Antonio, TX, United States	12.7%	35	Area comparison, Egress, and 3 more	Potential 50 ms improvement	None submitted
Office	Seattle, WA, United States	6.3%	83	Area comparison, SSL, Proxy	Potential 30 ms improvement	None submitted

Remote worker assessment and user connection metrics

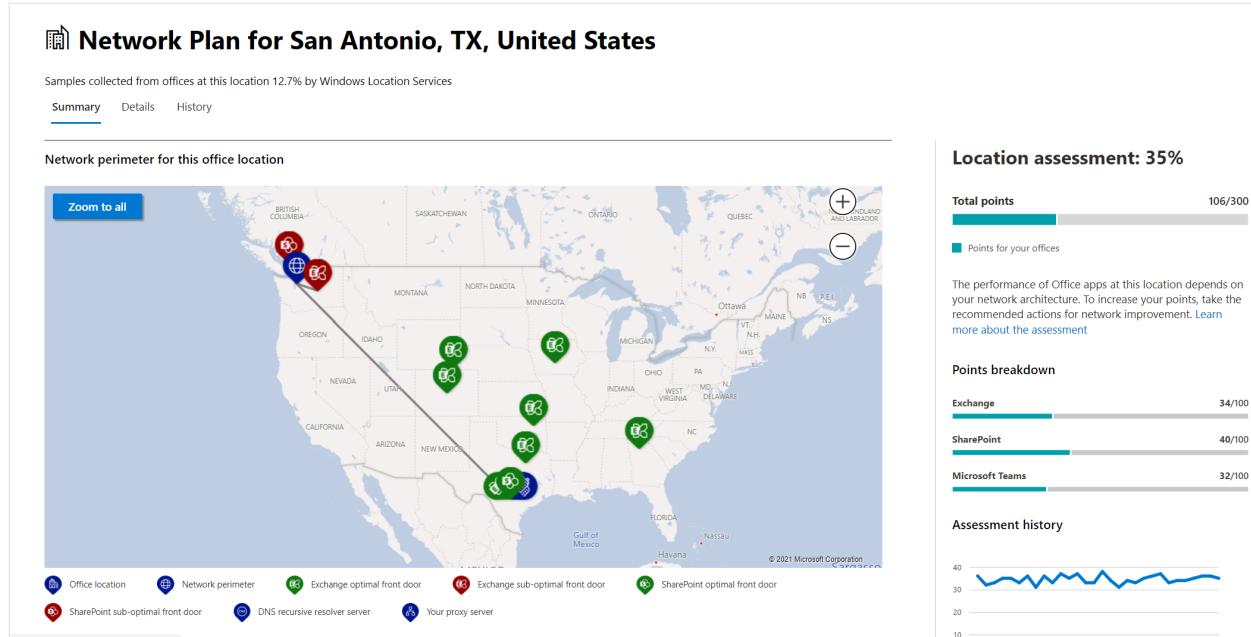
We classify network traffic logs as remote or onsite users and show their percentages in the user connection metrics section of the overview pane. For cities where you have remote users, you'll find the location specific remote network assessment score when you open that location's page. The locations list will have both office locations and remote worker cities, which can be filtered and sorted. We provide the remote worker assessment score, with points breakdown for Exchange, SharePoint, and Teams.

Home user networking insights are aggregated and reported at a city level and limited to cities with a minimum of five remote employees. We aren't identifying individual employees working from home.

Locations are auto classified as onsite or remote, however, you have the option to enter all your onsite egress IP addresses manually to ensure a 100% classification. If you decide to go this route, you'll have to check the **Enter all onsite egress IP addresses manually** checkbox in the Locations Settings flyout after adding all your egress IP addresses. When this is done, all network traffic logs from egress IP addresses you've marked as onsite will always be classified as offices and every other egress IP address will be classified as remote.

Specific office location network performance summary and insights

Selecting an office location opens a location-specific summary page showing details of the network egress that has been identified from measurements for that office location.



A map of the perimeter network for your organization users at the location is shown with some or all of these elements:

- **Office location** - The office location for the page you're looking at
- **Network perimeter** - The location of the source IP Address for connections from the office location. This depends on the accuracy of geo-IP location databases
- **Exchange optimal service front door** - One of the recommended Exchange service front doors that users in this office location should connect to
- **Exchange sub-optimal front door** - An Exchange service front door that users are connected to, but isn't recommended
- **SharePoint optimal service front door** - One of the recommended SharePoint service front doors that users in this office location should connect to
- **SharePoint sub-optimal service front door** - A SharePoint service front door that users are connected to, but isn't recommended
- **DNS recursive resolver server** - The location from a geo IP database of the detected DNS recursive resolver used for Exchange Online (if available)
- **Your proxy server** - The location from a geo IP database of the detected proxy server (if available)

The office location summary page additionally shows the location's network assessment, network assessment history, a comparison of this location's assessment to other

customers in the same city, and a list of specific insights and recommendations that you can undertake to improve network performance and reliability.

Comparisons between customers in the same city are based on the expectation that all customers have equal access to network service providers, telecommunications infrastructure, and nearby Microsoft network points of presence.

Location names can be customized when adding a new location or editing an existing location in the location flyout. This provides you with the flexibility to customize your location names at any time. Also, when adding LAN subnets directly in the location flyout, we show a drop-down list of soft-matched LAN subnets that you can select from. Circuit names for specific office egress IP addresses can be added and edited as well.

The details tab on the office location page shows the specific measurement results that were used to come up with any insights, recommendations, and the network assessment. This is provided so that network engineers can validate the recommendations and factor in any constraints or specifics in their environment. You'll also find the estimated number of users for collected samples at that office locations as well as the remote workers in that city.

Network Plan for Melbourne, Australia

Samples collected from offices at this location 10.6% by Windows Location Services

Summary Details History

Below are the results of your network services for this location. Sampled result information is updated every 24 hours.

Test	Collected samples	Remote workers
Location info (5)		
Network egress location (the location where your network connects to your ISP)	Woodinville, WA, US	Various
Distance from the network egress location	8193 miles (13185 km)	
Percentage of people in this area who have a better network connection to Microsoft 365	83% have a better network connection	27% have a better network connection
Estimated number of users ⓘ	1500-2000	Less than 10
Egress IP address ranges		
Exchange Online (3)		
Exchange service front door location	Quincy, WA, US	Various
Latency	160 ms. Potential 130 ms improvement	37 ms
Best Exchange service front door(s) for this location	New South Wales, Australia Victoria, Australia	New South Wales, Australia Victoria, Australia
SharePoint Online (4)		
SharePoint service front door location	Vancouver, BC, Canada	Various
Latency	160 ms	38 ms

Sharing network assessment data with Microsoft

By default, the network assessments for your organization and the network insights are shared with Microsoft employees. This doesn't include any personal data from your staff but only the specific network assessment metrics and network insights shown in the

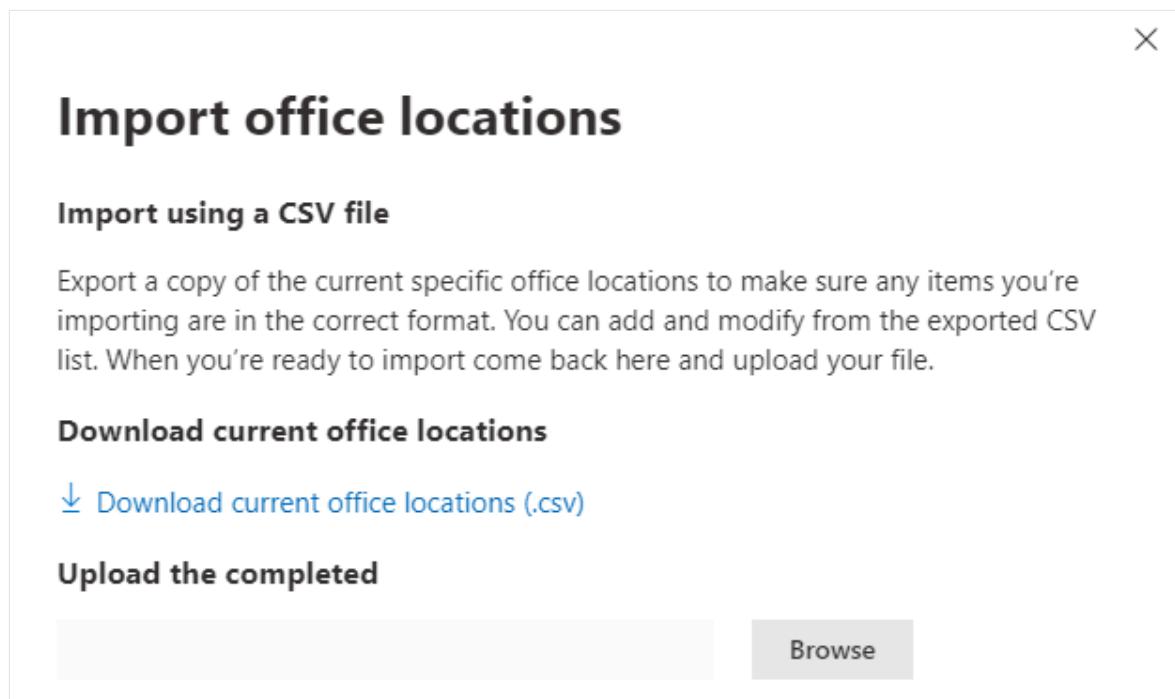
admin center for your office locations. It also doesn't include your office location names or street addresses so you would need to tell them the city and support ID of the office you want to discuss. If this is turned off, the Microsoft engineers that you're discussing your network connectivity with can't view any of this information. Enabling this setting only shares future data starting the day after you enable it.

CSV Import for LAN subnet office locations

For LAN subnet office identification, you need to add each location in advance. Instead of adding individual office locations in the **Locations** tab you can import them from a CSV file. You might be able to obtain this data from other places you have stored it such as the Call Quality Dashboard or Active Directory Sites and Services.

In the CSV file, a discovered city location shows in the userEntered column as blank, and a manually added office location shows as 1.

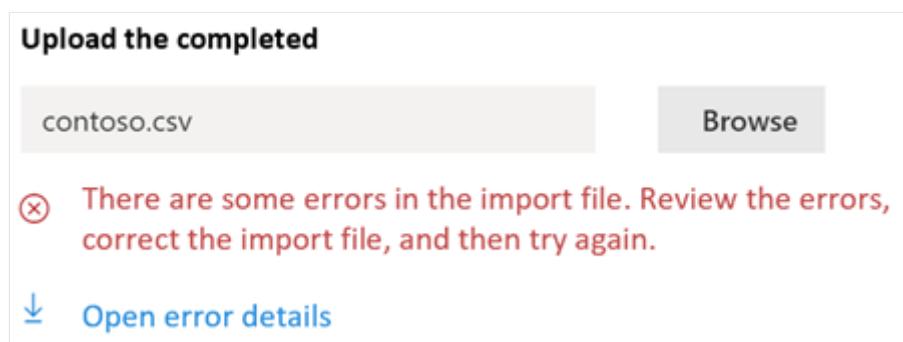
1. In the main *Connectivity to Microsoft 365* window, click the **Locations** tab.
2. Click the **Import** button just above the locations list. The **Import office locations** flyout will appear.



3. Click the **Download current office locations (.csv)** link to export the current locations list to a CSV file, and save it to your local hard disk. This will provide you with a correctly formatted CSV with column headings to which you can add locations. You can leave the existing exported locations as they are; they won't be duplicated when you import the updated CSV. If you wish to change the address of

an existing location, it's updated when you import the CSV. You can't change the address of a discovered city.

4. Open the CSV and add your locations by filling out the following fields on a new line for each location you want to add. Leave all other fields blank; values you enter in other fields will be ignored.
 - a. **userEntered** (required): Must be 1 for a new LAN Subnet office location being added
 - b. **Name** (required): The name of the office location
 - c. **Address** (required): The physical address of the office
 - d. **Latitude** (optional): Populated from Bing maps lookup of the address if blank
 - e. **Longitude** (optional): Populated from Bing maps lookup of the address if blank
 - f. **Egress IP Address ranges 1-5** (optional): For each range, enter the circuit name followed by a space separated list of valid IPv4 CIDR addresses. These values are used to differentiate multiple office locations where you use the same LAN subnet IP Addresses. Egress IP Address ranges all must be /24 network size and the /24 isn't included in the input.
 - g. **LanIps** (required): List the LAN subnet ranges in use at this office location. LAN subnet IDs need to have a CIDR network size included where the network size can be between /8 and /29. Multiple LAN subnet ranges can be separated by a comma or a semicolon.
5. When you have added your office locations and saved the file, click the **Browse** button next to the **Upload the completed** field and select the saved CSV file.
6. The file will be automatically validated. If there are validation errors, you'll see the error message: *There are some errors in the import file. Review the errors, correct the import file, and then try again.* Click the link **Open error details** for a list of specific field validation errors.



7. If there are no errors in the file, you'll see the message: *The report is ready. Found x locations to add and x locations to update.* Click the **Import** button to upload the CSV.

Upload the completed

contoso.csv

Browse

✓ This import is ready.

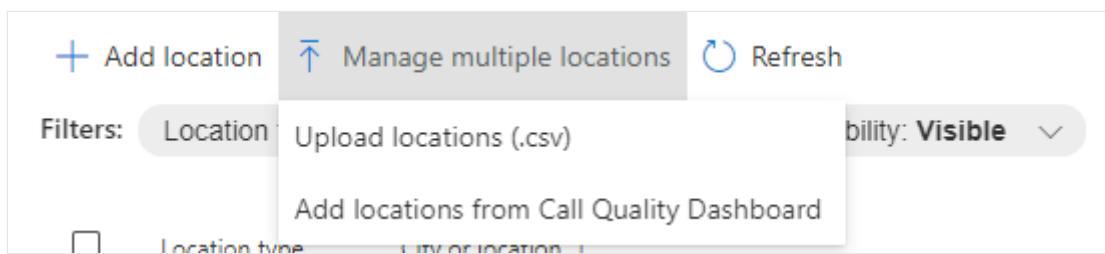
Found 1 locations to add and 1 locations to update.

CQD TSV Import for LAN subnet office locations

If you've uploaded building data to your Call Quality Dashboard, you can add those locations here to start assessing their network connectivity. This won't affect your existing locations.

Go to [Tenant Data Upload](#) in Call Quality Dashboard. If you've uploaded your building data, you'll see an option to download it to a .tsv file. Download the .tsv file from Call Quality Dashboard, then upload it in the CQD flyout following the steps below. If you want to create the .tsv file manually, please align the schema with that in Upload building data file, or try the CSV Import for LAN subnet office locations instead.

1. In the main Connectivity to Microsoft 365 window, click the **Locations** tab.
2. Click the **Manage multiple locations** button just above the locations list.



3. Click the **Add locations from Call Quality Dashboard**, the **Add locations from Call Quality Dashboard** flyout will appear.



Add locations from Call Quality Dashboard

If you've uploaded building data to your Call Quality Dashboard, you can add those locations here to start assessing their network connectivity. This won't affect your existing locations.

[Go to Tenant Data Upload](#) in Call Quality Dashboard. If you've uploaded your building data, you'll see an option to download it to a .tsv file. Download the .tsv file from Call Quality Dashboard, then upload it here.

Locations from Call Quality Dashboard were added on: 11/11/2021

Uploading your Call Quality Dashboard file again might overwrite existing locations.

Select a .tsv file to upload

Browse

4. Click the **Browse** button next to the **Select a .tsv file to upload** field and select the saved TSV file. Make sure the value in the file is tab separated.
5. The file will be automatically validated and parsed to the list of office locations. If there are validation errors, the **We couldn't upload your file** flyout appears to list the errors.



We couldn't upload your file

We detected errors in test1.tsv. Open the file in Excel or a similar app to fix each row affected by an error. When you're done, save the file and try uploading it again.

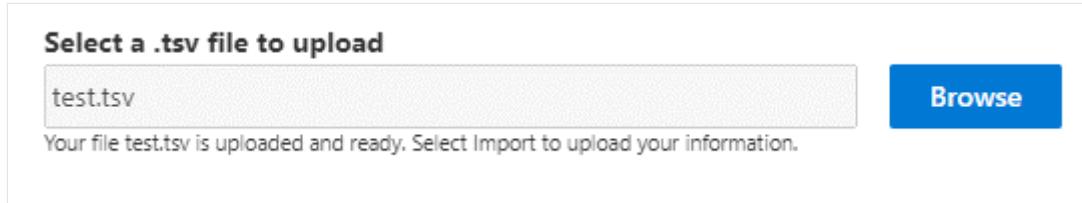
Try uploading again

Some locations have invalid network IP subnets.

Some network IP addresses you entered are in conflict with other network IPs in the same building.

Some location are missing an address or the addresses aren't valid.

6. If there are no errors in the file, you'll see the message: *Your file test.tsv is uploaded and ready. Select Import to upload your information.*



7. Click **Upload** button at the bottom of the panel to upload the office locations.

Understanding test sampling

FAQ

What role is needed to access Network Connectivity in Microsoft 365 Admin Center?

You'll need the Network Administrator role.

What is a Microsoft 365 service front door?

The Microsoft 365 service front door is an entry point on Microsoft's global network where Office clients and services terminate their network connection. For an optimal network connection to Microsoft 365, it's recommended that your network connection is terminated into the closest Microsoft 365 front door.

 **Note**

Microsoft 365 service front door has no direct relationship to the Azure Front Door Service product available in the Azure marketplace.

What is an optimal Microsoft 365 service front door?

An optimal Microsoft 365 service front door is one that is closest to your network egress, generally in your city or metro area. Use the [Microsoft 365 connectivity test tool](#) to determine the location of your in-use Microsoft 365 service front door and optimal service front door. If the tool determines your in-use front door is optimal, you're optimally connecting to Microsoft's global network.

What is an internet egress location?

The internet egress location is the location where your network traffic exits your enterprise network and connects to the Internet. This is also identified as the location where you have a Network Address Translation (NAT) device and usually where you connect with an Internet Service Provider (ISP). If you see a long distance between your location and your internet egress location, this might indicate a significant WAN backhaul.

What license is needed for this capability?

You require a license that provides access to the Microsoft 365 admin center.

Related articles

[Microsoft 365 network insights](#)

[Microsoft 365 network assessment](#)

[Microsoft 365 connectivity test tool](#)

[Microsoft 365 Network Connectivity Location Services](#)

Feedback

Was this page helpful?

 Yes

 No

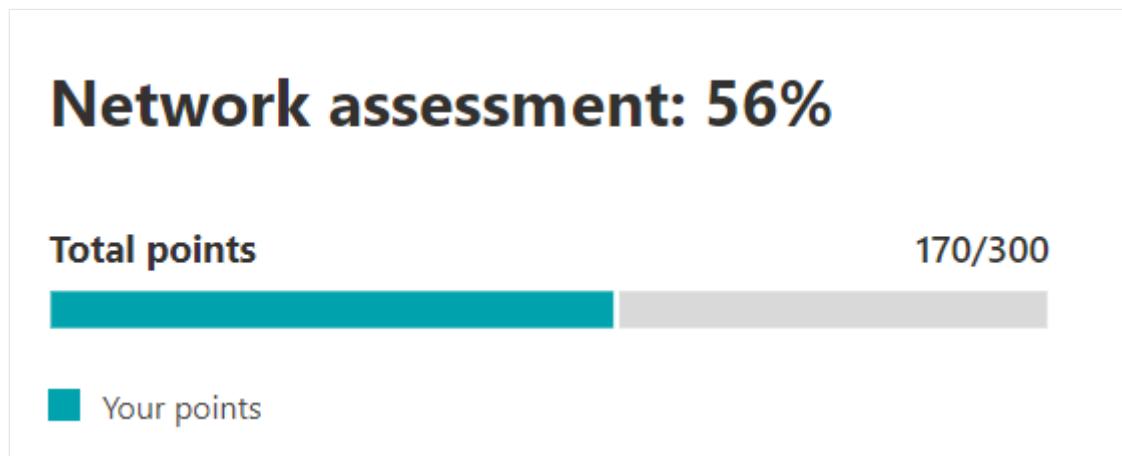
[Provide product feedback ↗](#)

Microsoft 365 network assessment

Article • 04/05/2024

In the Microsoft 365 Admin Center's network connectivity, **network assessments** distill an aggregate of many network performance metrics into a snapshot of your enterprise network perimeter health. A network assessment tells you how much the customer responsible network design is impacting Office 365 user experience. Network assessments are scoped to both the entire tenant and to each geographic location from which users connect to your tenant. The assessments provide Microsoft 365 administrators with an easy way to instantly get a sense of the enterprise's network health and quickly drill down into a detailed report for any global office location.

The network assessment points value is from 0 to 100 and is an average of TCP latency, download speed, and UDP connection quality metrics. These metrics are compiled once a day. Performance metrics for Microsoft-owned networks are excluded from these measurements to ensure that assessment results are unambiguous and specific to the corporate network.



A very low network assessment value suggests that Microsoft 365 clients will have significant problems connecting to the tenant or maintaining a responsive user experience. A high value indicates a properly configured network with few ongoing performance issues. A value of 80% represents a healthy baseline, above which you shouldn't expect to receive regular user complaints about Microsoft 365 connectivity or responsiveness due to network performance. As iterative network connectivity improvements are made, this value increases along with user experience.

[+] Expand table

Network assessment	Expected user experience
100	Best

Network assessment	Expected user experience
80	Meets recommendations
60	Acceptable
40	Users might experience issues
20	Users might complain
0	Network problems a common topic of discussion

Network assessment panel

Each network assessment, whether scoped to the tenant or to a specific office location, shows a panel with details about the assessment. This panel shows a bar chart of the assessment both as a percentage and as the total points for each component workload including only workloads where measurement data was received. For an office location network assessment, we also show a comparison to the percent of Microsoft 365 customers in each of five quintiles that reported data in the same city as your office location.

Network assessment: 56%

Total points

170/300



Your points

Your points reflect the measured performance of your Office apps, which depends on your network architecture. To increase your points, take the recommended actions for network improvement. [Learn more about the assessment](#)

Points breakdown

Exchange

59/100



SharePoint

59/100



Microsoft Teams

52/100



Assessment history



Your assessment

The **Assessment breakdown** in the panel shows the assessment for each of the component workloads.

The **Assessment history** shows the past 30 days of the assessment and the benchmark. You can also report on the metrics history for any office location for up to two years using the history tab. The history tab allows you to select your attributes to report on. By choosing a report time frame, you can highlight the impact of a network update project and see the improvement to your network assessment.

Tenant network assessments and office location network assessments

A network assessment measures the design of the network perimeter of an office location to Microsoft's network. Improvements to the network perimeter are best done at each office location.

We show a network assessment value for the whole Microsoft 365 tenant on the network performance overview page. This value is a weighted average of the network assessments for all office locations. There's also a specific network assessment value for each detected office location on that location's summary page.

Exchange Online

For Exchange Online, the TCP latency from the client machine to the Exchange service front door is measured. This latency can be impacted by the distance the network travels over the customers LAN and WAN. It can also be impacted by network intermediary devices or services, which delay the connectivity or cause packets to be resent. And it's impacted by how far away the nearest Exchange service front door is. The median (also known as the 50th percentile or P50 measure) is taken for all measurements over the previous three days.

The Exchange Online assessment is made using the following table. Any TCP latency number between the thresholds are assigned points linearly within the band.

[+] [Expand table](#)

TCP Latency	Points
10 ms or less	100
25 ms	80

TCP Latency	Points
100 ms	60
200 ms	40
300 ms	20
350 ms or more	0

SharePoint

For SharePoint the download speed available for a user to access a document from SharePoint or OneDrive is measured. This can be impacted by the bandwidth available on network circuits between the client machine and Microsoft's network. It's also often impacted by network congestion that exists in bottlenecks in complex network devices or in poor coverage Wi-Fi areas. The download speed is measured in megabytes per second, which is approximately one tenth of a circuit's rated megabits per second. The MegaByte per second unit is helpful because you can directly see what size file can be downloaded in 1 second. The 25th percentile (also known as the P25 measure) is taken for all measurements over the previous three days. This 25th percentile helps reduce the impact of varying congestion over time.

The SharePoint assessment is made using the following table. Any download speed number between the thresholds are assigned points linearly within the band.

[\[+\] Expand table](#)

Download speed	Points
20 MBps or more	100
14 MBps	80
8 MBps	60
4 MBps	40
2 MBps	20
0 MBps	0

Microsoft Teams

For Microsoft Teams the Network quality is measured as UDP latency, UDP jitter, and UDP packet loss. UDP is used for call and conferencing audio and video media connectivity for Microsoft Teams. This can be impacted by the same factors as for latency and download speed in addition to connectivity gaps in a network's UDP support since UDP is configured separately to the more common TCP protocol. The median (also known as the 50th percentile or P50 measure) is taken for all measurements over the previous three days.

We calculate a mean opinion score from these UDP measurements for a scale from one to five. Then we map that to the 0-100 points scale for the Microsoft Teams network assessment. Overall good is over 87.5 points and overall bad is below 50 points.

Understanding test sampling

Network test sampling doesn't include user or device identities and hence the size of offices and number of users in them is estimated. We use the number of test results from Exchange tests and the number of tests from SharePoint tests to do this. If no samples are received for the office location, then summary assessment information is still shown for up to 60 days but detailed information isn't shown, including the estimated number of users.

Related articles

[Network connectivity in the Microsoft 365 Admin Center](#)

[Microsoft 365 network performance insights](#)

[Microsoft 365 network connectivity test tool](#)

[Microsoft 365 Network Connectivity Location Services](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Microsoft 365 Network Insights

Article • 04/05/2024

Network insights are performance metrics collected from your Microsoft 365 tenant, and available to view only by administrative users in your tenant. Insights are displayed in the Microsoft 365 Admin Center at <https://portal.microsoft.com/adminportal/home#/networkperformance>.

Insights are intended to help in designing network perimeters for your office locations. Each insight provides live details about the performance characteristics for a specific common issue for each geographic location where users are accessing your tenant.

These are network insights that might be shown for each office location:

- Backhauled network egress
- Network intermediary device
- Better performance detected for customers near you
- Use of a nonoptimal Exchange Online service front door
- Use of a nonoptimal SharePoint service front door
- Low download speed from SharePoint front door
- China user optimal network egress

These are tenant-level network insights that might be shown for the tenant:

- Exchange sampled connections affected by connectivity issues
- SharePoint sampled connections affected by connectivity issues

These insights also appear in the productivity score pages.

Backhauled network egress

This insight displays if the network insights service detects that the distance from a given user location to the network egress is greater than 500 miles (800 kilometers). This might indicate that Microsoft 365 traffic is being backhauled to a common Internet edge device or proxy.

This insight is abbreviated as "Egress" in some summary views.

Backhauled network egress

The distance from this office to the network egress location is greater than 500 miles (800 kilometers). We recommend connecting to a closer network egress point. [Read our specific recommendations for improving your network connectivity](#)

Office location:  [Melbourne, Australia](#)

Samples collected from offices at this location 10.6% by Windows Location Services

Egress location: Woodinville, WA, US

Distance from the network egress: 8193 miles (13190 km)

End: Insight is still present

What does this mean?

This identifies that the distance between the office location and the network egress is more than 500 miles (800 kilometers). The office location is identified by an obfuscated client machine location and the network egress location is identified by using reverse IP Address to location databases. The office location might be inaccurate if Windows Location Services is disabled on machines. The network egress location might be inaccurate if the reverse IP address database information is inaccurate.

Details for this insight include:

- Office location
- Estimated percentage of total tenant user at the location
- Current network egress location
- Relevance of the egress location
- Distance between the location and the current egress point
- The date the condition was first detected
- The date the condition was resolved

What should I do?

We recommend network egress as close as possible to the office location. Microsoft 365 traffic should route optimally to Microsoft's global network and to the nearest Microsoft 365 service front door. Having close network egress to users office locations also allows for improved performance as Microsoft expands both network points of presence and Microsoft 365 service front doors in the future.

For more information about how to resolve this issue, see [Egress network connections locally in Microsoft 365 Network Connectivity Principles](#).

Network intermediary device

This insight displays if we detected devices between your users and Microsoft's network. We recommend that latency-sensitive Microsoft 365 network traffic bypass such devices. This recommendation is additionally described in [Microsoft 365 Network Connectivity Principles](#).

One network intermediary insight we show is SSL break and inspection when network intermediary devices intercept and decrypt critical Microsoft 365 network endpoints for Exchange, SharePoint, and Teams.

What does this mean?

Network intermediary devices such as proxy servers, VPNs, and data loss prevention devices can affect performance and stability of Microsoft 365 clients where traffic is intermediated.

What should I do?

Configure the network intermediary device that was detected to bypass processing for Microsoft 365 network traffic.

Better performance detected for customers near you

This insight displays if the network insights service detects that a significant number of customers in your metro area have better performance than users at this office location.

This insight is abbreviated as "Peers" in some summary views.

Other people in this area have better network connectivity to Microsoft 365

At least 10% of people in this area have better network connectivity to Microsoft 365, which means that your network connectivity can be improved. More testing is needed to recommend specific improvements. [Read our specific recommendations for improving your network connectivity](#)

Office location:  **Philadelphia, PA, US**

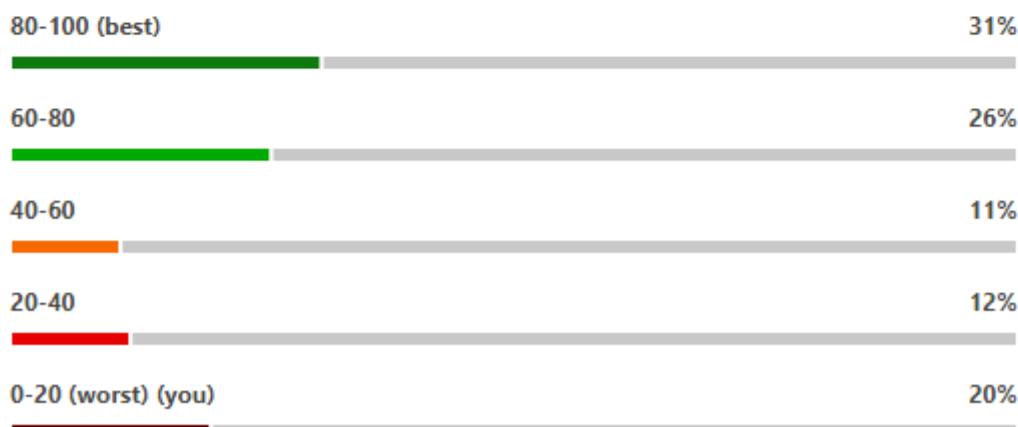
Samples collected from offices at this location 16.9% by Windows Location Services

Customers with better performance: 80%

End: Insight is still present

Your network performance for this location is worse than 80% of nearby customers

This chart compares your network performance for this location to all Office 365 customers in the same metropolitan area. Network performance is rated on a scale of 0 and 100, where 100 is best.



What does this mean?

This insight examines the aggregate performance of Microsoft 365 customers in the same city as this office location. This insight displays if the average latency of your users is 10% greater than the average latency of neighboring tenants.

What should I do?

There could be many reasons for this condition, including latency in your corporate network or ISP, bottlenecks, or architecture design issues. Examine the latency between each hop in the route between your office network and the current Microsoft 365 front door. For more information, see [Microsoft 365 Network Connectivity Principles](#).

Use of a nonoptimal Exchange Online service front door

This insight displays if the network insights service detects that users in a specific location aren't connecting to an optimal Exchange Online service front door.

This insight is abbreviated as "Routing" in some summary views.

Not connected to the best Exchange service front door location

We recommend connecting to an Exchange service front door that is closer to this office location. More testing is needed to know why you aren't connected to the closest service front door. [Read our specific recommendations for improving your network connectivity](#)

Office location:  [San Antonio, TX, US](#)

Samples collected from offices at this location 12.7% by Windows Location Services

Exchange service front door location: Quincy, WA, US

Median latency: 50 ms

Best Exchange service front door(s) for this location:

Alpharetta

Cheyenne, WY, US

Colorado Springs, CO, US

Dallas, TX, US

Des Moines, IA, US

San Antonio, TX, US

Tulsa, OK, US

End: Insight is still present

What does this mean?

We list Exchange Online service front doors that are suitable for use from the office location city. If the current test shows use of an Exchange Online service front door not

on this list, then we make this recommendation.

What should I do?

Network backhaul might cause use of a nonoptimal Exchange Online service front door, in which case we recommend local and direct network egress. If you have implemented a remote DNS Recursive Resolver server, we recommend aligning the server configuration with the network egress.

Use of a nonoptimal SharePoint service front door

This insight displays if the network insights service detects that users in a specific location aren't connecting to the closest SharePoint service front door.

This insight is abbreviated as "Afd" in some summary views.

Not connected to the best SharePoint service front door location

We recommend connecting to a SharePoint service front door that is closer to this office location. More testing is needed to know why you aren't connected to the closest service front door. [Read our specific recommendations for improving your network connectivity](#)

Office location:  [Melbourne, Australia](#)

Samples collected from offices at this location 10.6% by Windows Location Services

SharePoint service front door location: Vancouver, BC, Canada

Median latency: 160 ms

Download speed: 5 MBps

Best SharePoint service front door(s) for this location:

Melbourne, Australia

End: Insight is still present

What does this mean?

We identify the SharePoint service front door that the test client is connecting to, and then we compare the office location city to the expected SharePoint service front door

for that city. If the test client service front door and the expected service front door match, we recommend connecting to a SharePoint service front door closer to the office location.

What should I do?

Network backhaul before the corporate network egress could cause nonoptimal SharePoint service front door use. If so, try local and direct network egress. Nonoptimal SharePoint service front door use could also be caused by a remote DNS Recursive Resolver server, in which case we recommend aligning the DNS Recursive Resolver server with the network egress.

Low download speed from SharePoint front door

This insight displays if the network insights service detects that bandwidth between the specific office location and SharePoint is less than 1 MBps.

This insight is abbreviated as "Throughput" in some summary views.

What does this mean?

The download speed that a user can get from SharePoint and OneDrive service front doors is measured in megabytes per second (MBps). If this value is less than 1 MBps, then we provide this insight.

What should I do?

To improve download speeds, your organization might need to increase bandwidth. Alternatively, network congestion might exist between computers at the office location and the SharePoint service front door. This condition restricts the download speed available to users even if sufficient bandwidth is available.

China user optimal network egress

This insight displays if your organization has users in China connecting to your Microsoft 365 tenant in other geographic locations.

What does this mean?

If your organization has private WAN connectivity, we recommend configuring a network WAN circuit from your office locations in China that have network egress to the Internet in any of the following locations:

- Hong Kong Special Administrative Region
- Japan
- Taiwan
- South Korea
- Singapore
- Malaysia

Internet egress farther away from users than these locations reduces performance, and egress in China might cause high latency and connectivity issues due to cross-border congestion.

What should I do?

For more information about how to mitigate performance issues related to this insight, see [Microsoft 365 global tenant performance optimization for China users](#).

Exchange sampled connections affected by connectivity issues

This insight shows when 50% or more of the sampled connections are affected. The impact is defined by the Exchange assessment being below 60% for each sample.

What does this mean?

This insight indicates that most of your users likely experience issues with Outlook connecting to Exchange Online. The percentage of samples represents the percentage of users below 60 points.

What should I do?

Enable office location network connectivity visibility if you haven't already done so. Identify which offices are affected by poor network connectivity and find ways to improve the network perimeter at each that connects the users to Microsoft's network.

SharePoint sampled connections affected by connectivity issues

This insight shows when 50% or more of the sampled connections are affected. The impact is defined by the SharePoint assessment being below 40% for each sample.

What does this mean?

This insight indicates that most of your users are likely experiencing issues with SharePoint and OneDrive. The percentage of samples represents the percentage of users who show below 40 points.

What should I do?

Enable office location network connectivity visibility if you haven't already done so. Identify which offices are affected by poor network connectivity and find ways to improve the network perimeter at each that connects the users to Microsoft's network.

Related articles

[Network connectivity in the Microsoft 365 Admin Center](#)

[Microsoft 365 network assessment](#)

[Microsoft 365 network connectivity test tool](#)

[Microsoft 365 Network Connectivity Location Services](#)

Feedback

Was this page helpful?

 Yes

 No

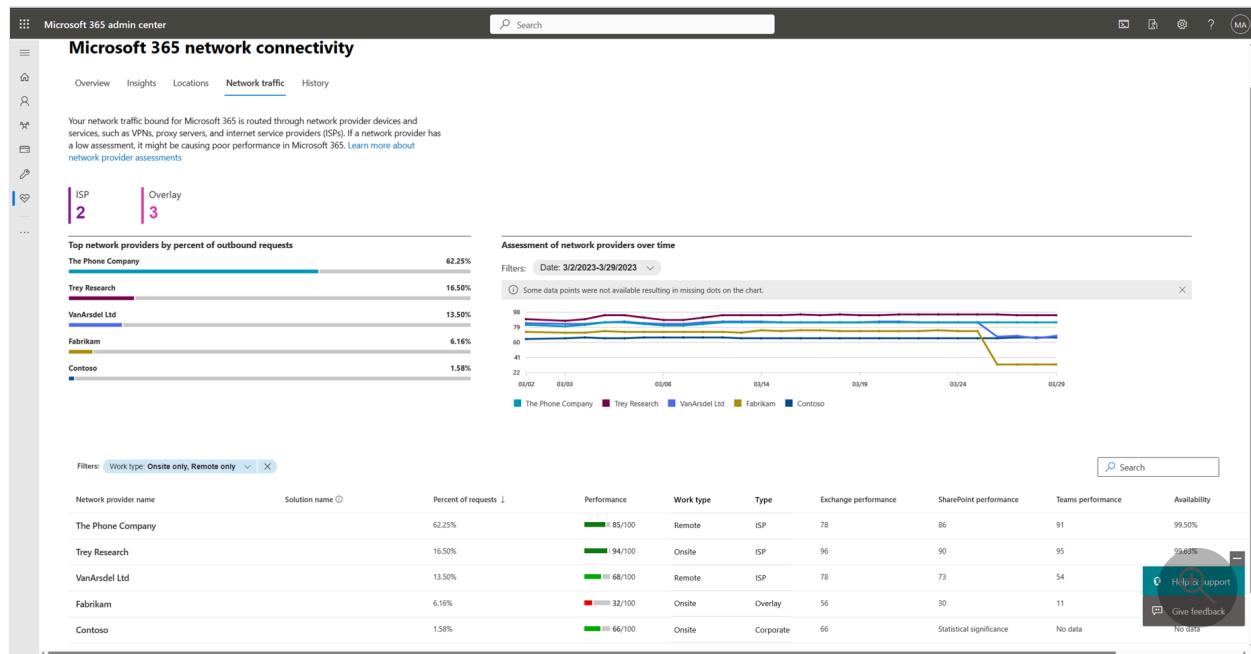
[Provide product feedback ↗](#)

Network provider connectivity attribution in the Microsoft 365 Admin Center

Article • 04/05/2024

The network provider table

In the Microsoft 365 Admin Center you can view network providers in use by your users and we apportion network connectivity performance and availability experienced by your users to each. To access these reports in the Microsoft 365 Admin Center, select the **Health | Network connectivity** menu.



When you navigate to the Network traffic tab, you'll see information about connectivity solutions from network providers that have been detected between Office 365 users and Microsoft's network.

Network providers are identified as either of the following:

- **ISP** – Internet Service Provider that provides data transmission media such as terrestrial ISP, cellular ISP, or satellite ISP
- **Overlay** – An additional detected network provider providing other services such as VPN, Cloud Proxy, SD-WAN, and SASE
- **Corporate** – The customer owns detection attributes for network providers

The top five network providers by network requests from your users are shown on the left. On the right is a historical chart showing the performance assessment of each of the top five network providers over time. You can adjust the time range back as far as two years though the default is one month.

In the lower part of the page shows a table of all significant detected network providers. It can show these attributes for each network provider:

- **Network provider name** – The network provider name from public contributions
- **Solution name** – Listed if a network provider has multiple network solutions which are measured separately
- **Percent of requests** – The percentage of requests for the specific provider for all your users
- **Performance** – The network assessment performance out of 100 attributed to this network provider
- **Work type** – Shows either remote, onsite, or remote and onsite
- **Type** – Shows either ISP, Overlay, or Corporate
- **Exchange Performance** – Exchange network assessment out of 100
- **SharePoint Performance** – SharePoint network assessment out of 100
- **Teams Performance** – Teams network assessment out of 100
- **SharePoint Throughput** – SharePoint throughput aggregate with error margin in Megabytes per second
- **Exchange Latency** – Exchange TCP latency aggregate with error margin in milliseconds
- **Teams packet loss** – Teams UDP Packet loss in percent aggregate with error margin
- **Teams jitter** – Teams UDP Jitter with error margin in milliseconds
- **Teams latency** – Teams UDL latency with error margin in milliseconds
- **Availability** – The network availability as a percentage attributed to this network provider
- **Exchange Availability** – Exchange specific availability
- **SharePoint Availability** – SharePoint specific availability
- **Teams Availability** – Teams specific availability

You can filter the table of network providers by connections from onsite corporate office locations or remote worker locations such as homes, cafés, hotels.

If you click the network provider name a flyout will appear showing details about that network provider.

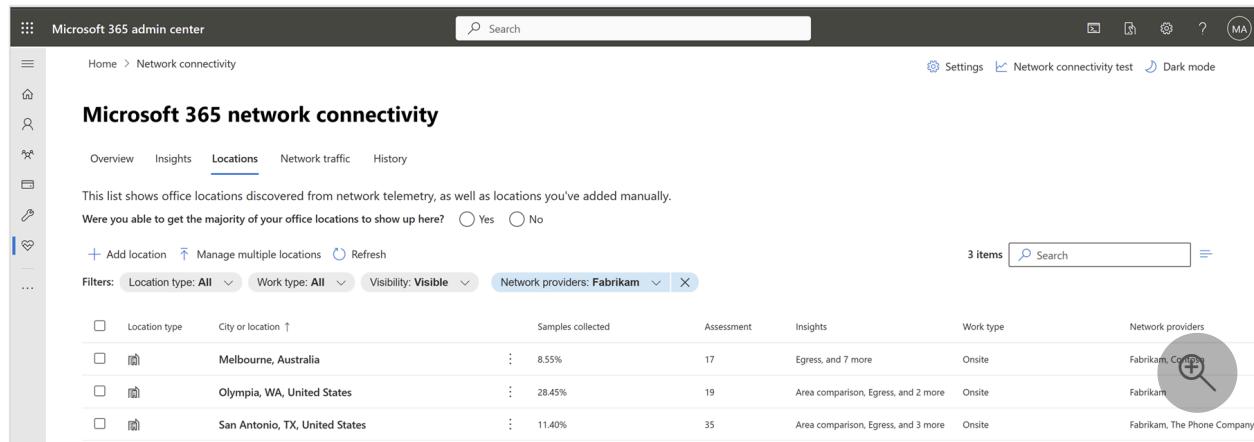
The flyout shows more information about a particular network provider. If this network provider is in the Microsoft 365 network partner program, then a **Setup info** section will

be shown with a link to configuration instructions that the network provider shares for optimal connectivity to Microsoft 365.

The flyout also has a Location section which contains a link to open the **Network connectivity | Location** table filtered for this network provider. If the network provider selected has an identified network insight causing poor Microsoft 365 user experience, then the flyout text will provide recommendations for improvement.

Network providers by location

The table of locations can be filtered by specific network providers. The table will be filtered to only show locations where the specified network provider is detected. If multiple network providers are selected in the filter, then locations where any of them were detected are shown.



	Samples collected	Assessment	Insights	Work type	Network providers
Melbourne, Australia	8.55%	17	Egress, and 7 more	Onsite	Fabrikam, Contoso
Olympia, WA, United States	28.45%	19	Area comparison, Egress, and 2 more	Onsite	Fabrikam
San Antonio, TX, United States	11.40%	35	Area comparison, Egress, and 3 more	Onsite	Fabrikam, The Phone Company

A network providers column is included in the table where network providers are shown as fit. The network providers are all shown in the details tab.

Top Providers for a location (Network Provider Index or NPI chart)

The NPI chart shows the network providers with the highest performance for Office 365 applications for customers who are in the same country/region and state as your office. We show availability and performance data related to these providers. This chart also has a target baseline that shows the best performance observed in the same country/region and state.

Top providers for this location

June 2023

This index, published monthly, lists network providers with the highest Microsoft 365 network performance score in Auckland, New Zealand. Assessments measure Microsoft 365 availability and performance attributed to each network provider.

Target baseline for Auckland, New Zealand ⓘ

Availability	Performance
99.993%	80/100

Name	Availability ⓘ	Performance ⓘ
The Phone Company	99.999%	 75/100
Trey Research	99.555%	 50/100
VanArdsel Ltd	99.755%	 73/100
Fabrikam	99.999%	 75/100
Contoso	98.000%	 9/100

Note: NPI chart is currently available only for United States of America. The chart will be expanded soon to all locations globally.

Providers used at this location

Below the NPI Chart is a list of network providers detected for your users at this specific office location. The Table of network providers for this location has the following fields:

Providers used at this location				
Network provider name	Solution name ⓘ	Percent of requests ↓	Availability	Performance
The Phone Company		83.89%	99.40%	 85/100
Fabrikam		12.79%	97.74%	 32/100

- Network provider name
- Solution name
- Percent of requests
- Availability
- Performance

Related articles

[Network connectivity in the Microsoft 365 admin center](#)

[Network provider program data calculations](#)

[Microsoft 365 network assessment](#)

[Microsoft 365 network connectivity test tool](#)

Feedback

Was this page helpful?



Yes



No

[Provide product feedback ↗](#)

Microsoft 365 network provider assessments.

Article • 04/05/2024

Microsoft measures network performance and availability between client applications on user machines and Microsoft's network.

Network performance

Read about the network performance assessment calculation method at [Microsoft 365 network assessment](#).

Network availability

The reliability of Microsoft 365 services as experienced by the client is shown by the network availability metric. It's measured as the length of time that Exchange and SharePoint are working, and for Microsoft Teams as a proportion of calls that connected successfully both expressed as a percentage.

Exchange and SharePoint Network availability

Exchange and Sharepoint availability are the proportion of minutes without any major user errors out of the total user minutes. This is how it's calculated:

$$1 - \frac{\text{Impacted user minutes}}{\text{total user minutes}}$$

We receive notification of unsuccessful connections after network connectivity is restored.

Teams Network availability

By using telemetry data from the actual calls, Microsoft Teams availability is computed as a percentage of calls that failed compared to total calls. This is how it's calculated:

$$1 - \frac{\text{failed calls}}{\text{total calls}}$$

Detecting network providers

Network providers are detected from network attributes in Office 365 network telemetry. Network attributes that may be used for detection include:

- Public IP Address ownership
- Public ASN ownership
- VPN network interface details
- SSL Certificate ownership

Specific network attributes for a network provider solution are either obtained from public sources, from Microsoft network telemetry, or contributed to Microsoft by the network provider.

When a network provider solution is detected on network telemetry the Office 365 measured performance and availability from that connection is attributed to the network provider and aggregated. This isn't intended to represent the network provider but rather represents Office 365 performance and availability experienced by users as attributed to detected network providers.

Calculation of standard error of sampling

What if you don't see the exact same measurement as our aggregation? Our aggregation of network telemetry is sample based and this sample represents the complete possible population of network connections that may be made. We calculate the standard error of sampling and present it along with results. If this error is greater than 20% or there are fewer than 24 samples, then we don't show the result, but instead show an error marker in the data field.

The formula used for the standard error is:

$$\text{Standard error} = z * c \frac{\sigma}{\sqrt{n}}$$

Where:

- z is the statistical coefficient and for 95% confidence interval the value is 1.96
- c is the error coefficient for the percentile and for the 50th percentile it's 1.09
- σ is the standard deviation of the aggregation
- n is the number of samples

Data aggregation slicing

For customer specific reporting the aggregations are sliced by the customer and by detected network provider and by work location type. They're also sliced by office location for drill-down capability. For the NPI Chart views including Target Baseline metrics are aggregations sliced by network provider and by country/region and state. The NPI Chart data is aggregated from all Office 365 customers.

For network providers the aggregations are sliced by network provider, by geography (including country/region, state, and city), and by /24 public network.

Data aggregation statistical evaluations

There are some markers we show where data can't be reported.

- **Statistical significance** – As described above we don't show data where the standard error of sampling is greater than 20%.
- **No data** – This is displayed if for some reason this data element had no samples.
- **Privacy requirement** – This is displayed for the network provider view if there were fewer than five customers in any aggregation result or if there were fewer than 24 samples in the aggregation. We don't provide customer performance data directly to network providers for customer privacy reasons.
- **Dominating customer** – Even where there are five or more customers, there might be cases where a customer can be guessed due to the specific network provider having a large customer in a geographic area. To avoid this, we compare the population including the largest customer with the same population excluding the largest customer. Using a Cohen's D calculation, we discard results where the population difference is greater than 0.5. This means that where the largest customer has a medium to large Cohen's D effect on the aggregation result the result is blocked. A network provider simply needs to expand their geographic area where they have more customers to see results.

The markers **Privacy requirement** and **Dominating customer** aren't shown in customer reports. In addition, we remove outliers from the sample source where outliers are defined as:

$$\text{Outlier cutoff} = \text{mean} + 3 * \text{standard deviation}$$

Network providers will additionally not be shown in a tenant or location view if that network provider accounts for fewer than 0.01% of users represented in that view.

Network Provider Index Chart

The NPI Chart shows the network providers with the highest performance for Office 365 applications for customers who are in the same country/region and state as your office. We show availability and performance data related to these providers. This chart also has a target baseline that shows the best performance observed in the same country/region and state.

Note: NPI Chart is currently available only for United States of America. The chart will be expanded soon to all locations globally.

Related articles

[Network connectivity in the Microsoft 365 Admin Center](#)

[Network provider reporting](#)

[Microsoft 365 network assessment](#)

[Microsoft 365 network connectivity test tool](#)

[Microsoft 365 Network Connectivity Location Services](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Network provider details in the Microsoft 365 Admin Center

Article • 04/05/2024

We try to detect network provider device interference between your tenant users and Microsoft 365 services. Here are the types of device interference we can detect.

Percentage refers to the percentage of media streams for Teams, and percentage of connections for Exchange and SharePoint.

SSL break and inspect test

This test detects a private or unknown certificate presented by a network device to your tenant users for data path connections to Microsoft 365 services, a private certificate is typically used when the network device intends to perform break and inspect operation at the SSL or TLS layer for those connections. We may not be able to show you the detected certificate issuer names due to privacy reasons.

Service	Percentage	Certificate names
Exchange	  14.29%	UnknownSSL
SharePoint	  5%	UnknownSSL

Incorrect destination IP address detected

This indicates that the destination endpoint representing Microsoft 365 endpoints have incorrect or unfamiliar IP addresses assigned to them. Typically, this means there's an intermediate network device acting as a proxy and we'll show you the incorrect or unfamiliar IP address detected.

Service	Percentage	IP addresses
Exchange	<div><div style="width: 100%;">■ ■ ■</div></div> 100%	137.40.12.80
SharePoint	<div><div style="width: 100%;">■ ■ ■</div></div> 100%	137.40.12.80

VPN or tunneling detected

This indicates that the network taken to connect to Microsoft 365 endpoints involves a VPN or traffic tunneling. A VPN or traffic tunneling might cause backhaul of network traffic and lead to network performance issues that impacts user experience.

Service	Percentage	VPN interface names
Exchange	 100%	Fabrikam
SharePoint	 100%	Fabrikam

No device interference detected

This is aligned with our connectivity principles and indicates that there was no device interference detected between your tenant users and Microsoft 365 services.

Related articles

[Network connectivity in the Microsoft 365 admin center](#)

[Network provider program data calculations](#)

[Microsoft 365 network assessment](#)

[Microsoft 365 network connectivity test tool](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Microsoft 365 network connectivity test tool

Article • 04/05/2024

The Microsoft 365 network connectivity test tool is located at <https://connectivity.office.com>. It's an adjunct tool to the network assessment and network insights available in the Microsoft 365 admin center under the **Health | Connectivity** menu.

ⓘ Note

This document mentions the URL (<https://connectivity.office.com>) for the Global version of this tool. For other versions, please refer to the table below for the corresponding URLs.

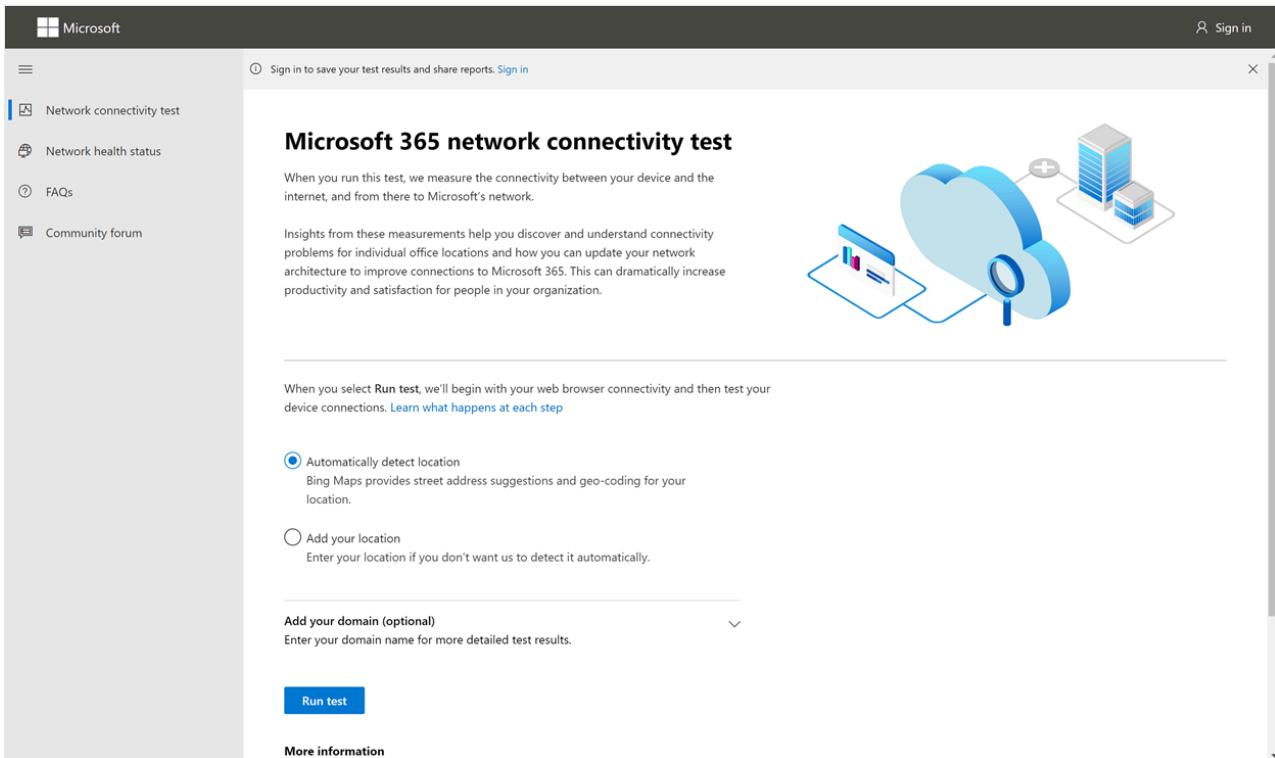
[] Expand table

Feature	Global service https://connectivity.office.com	US Government (GCC) https://connectivity.office.com	China operated by 21Vianet https://connectivity.sovcloud.cn
Anonymous test	✓	✓	✓
Print report	✓	✓	✓
Login	✓	✗	✓
Save report	✓	✗	✓
View report	✓	✗	✓
Share report in tenant	✓	✗	✓
Share report to public	✓	✗	✓
Network health status	✓	✓	✓
Multi-languages support: English, Chinese Simplified, Chinese Traditional, Japanese	✓	✓	✓
Testing from the command line	✓	✗	✓

Feature	Global service https://connectivity.office.com	US Government (GCC) https://connectivity.office.com	China operated by 21Vianet https://connectivity.sovcloud.cn
FAQ	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Community forum	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

ⓘ Important

It's important to sign in to your Microsoft 365 tenant as all test reports are shared with your administrator and uploaded to the tenant while you are signed in.



Network insights in the Microsoft 365 Admin Center are based on regular in-product measurements for your Microsoft 365 tenant, aggregated each day. In comparison, network insights from the Microsoft 365 network connectivity test are run locally in the tool.

In-product testing is limited, and running tests local to the user collects more data resulting in deeper insights. Network insights in the Microsoft 365 Admin Center show that there's a networking problem at a specific office location. The Microsoft 365 connectivity test can help to identify the root cause of that problem and provide a targeted performance improvement action.

We recommend that these insights be used together where networking quality status can be assessed for each office location in the Microsoft 365 Admin Center. More specifics can be found after deployment of testing based on the Microsoft 365 connectivity test.

What happens at each test step

Office location identification

When you select the *Run test* button, we show the running test page and identify the office location. You can type in your location by city, state, and country/region or choose to have it detected for you. If you detect the office location, the tool requests the latitude and longitude from the web browser and limits the accuracy to 300 meters by 300 meters before use. It's not necessary to identify the location more accurately than the building to measure network performance.

JavaScript tests

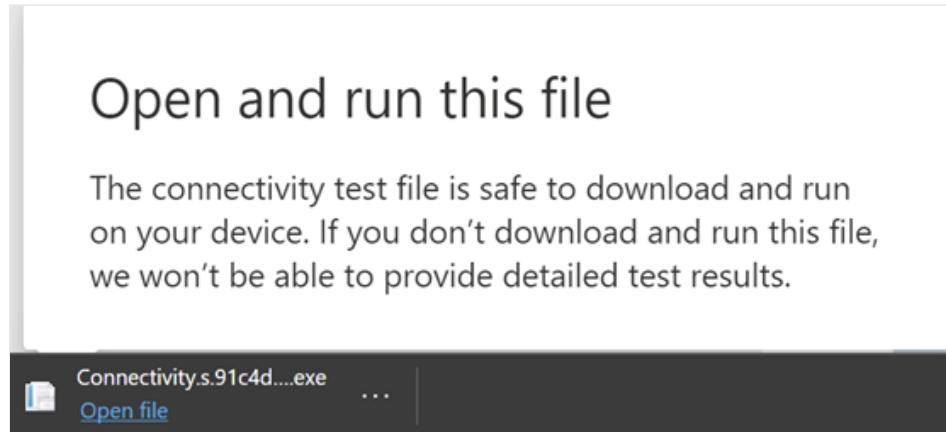
After office location identification, we run a TCP latency test in JavaScript and we request data from the service about in-use and recommended Microsoft 365 service front door servers. When these tests are completed, we show them on the map and in the details tab where they can be viewed before the next step.

Download the advanced tests client application

Next, we start the download of the advanced tests client application. We rely on the user to launch the client application and they must also have .NET 6.0 Runtime installed.

There are two parts to the Microsoft 365 network connectivity test: the web site <https://connectivity.office.com> and a downloadable Windows client application that runs advanced network connectivity tests. Most of the tests require the application to be run. It populates results back into the web page as it runs.

You'll be prompted to download the advanced client test application from the web site after the web browser tests have completed. Open and run the file when prompted.



Start the advanced tests client application

Once the client application starts, the web page updates to show this result. Test data starts to be received to the web page. The page updates each time new-data is received and you can review the data as it arrives.

Advanced tests completed and test report upload

When the tests are completed, the web page and the advanced tests client will both show that. If the user is signed in, the test report is uploaded to the customer's tenant.

Sharing your test report

The test report requires authentication to your Microsoft 365 account. Your administrator selects how you can share your test report. The default settings allow for sharing of your reports with other user within your organization and the ReportID link isn't available. Reports will expire by default after 90 days.

Sharing your report with your administrator

If you're signed in when a test report occurs, the report is shared with your administrator.

Sharing with your Microsoft account team, support or other personnel

Test reports (excluding any personal identification) are shared with Microsoft employees. This sharing is enabled by default and can be disabled by your administrator in the **Health | Network Connectivity** page in the Microsoft 365 Admin Center.

Sharing with other users who sign in to the same Microsoft 365 tenant

You can choose users to share your report with. Being able to choose is enabled by default, but it can be disabled by your administrator.

The screenshot shows the Microsoft 365 Admin Center interface. On the left, there's a sidebar with options like 'Network connectivity test', 'Reports', 'Network health status', 'FAQs', and 'Community forum'. The main area displays 'Network connectivity test results for you'. It includes sections for 'Summary' (which is currently selected), 'Details', 'Your location information', and a list of test results. A 'Share results' button is at the bottom right of this section. A modal window titled 'Share these results' is open on the right. It has a search bar with 'PA' typed in, a note about selecting people or groups, and a 'Sharing history' table with one entry for 'Admin name' and 'Type'.

Sharing with anyone using a ReportID link

You can share your test report with anyone by providing access to a ReportID link. This link generates a URL that you can send to someone so that they can bring up the test report without signing in. This sharing is disabled by default and must be enabled by your administrator.

Network connectivity test results for your location

Summary Details

Here are the detailed connectivity test results for your location. [Learn about the tests we run](#)

Your location information

Test	Result
Your location	Redmond, WA, United States found by the web browser
Network egress location	Redmond, WA, United States
<input checked="" type="checkbox"/> Your distance from the Microsoft 365 network	0 miles (1 kilometers)
<input checked="" type="checkbox"/> Customers in your metropolitan area with better performance	Not a significant number of other customers have better network connectivity.
Time to make a DNS request on your network	192.168.15.2 (18 ms) 1.1.1.1 (21 ms) ::
<input checked="" type="checkbox"/> Your distance from and/or time to connect to a DNS recursive resolver	108.162.244.89 (22 ms)
<input checked="" type="checkbox"/> If you use a proxy server, distance from your location and time to connect	A proxy server was not identified in your connection
<input checked="" type="checkbox"/> Virtual private network (VPN) you use to connect to your organization	VPN detected: MSFTVPN
<input checked="" type="checkbox"/> VPN Split Tunnel	Exchange Online Optimize is split out Sharepoint Online Optimize is selective tunneled

Network Connectivity Test Results

The results are shown in the **Summary** and **Details** tabs. The summary tab shows a map of the detected network perimeter and a comparison of the network assessment to other Microsoft 365 customers nearby. It also allows for sharing of the test report. Here's what the summary results view looks like:

Network connectivity test results for your location

Summary Details

Map of your network connections

No one in nearby locations have better network connectivity to Microsoft 365 than your location.

This chart shows the network connection quality for Microsoft 365 customers in your area.

Quality Range	Percentage
80-100 (best) (you)	50%
60-80	38%
40-60	6%
20-40	1%
0-20 (worst)	1%

Legend:

- Your location
- Your network's connection to your ISP
- Recommended Exchange front door
- Your current Exchange front door
- DNS recursive resolver server
- Your proxy server

Here's an example of the details tab output. On the details tab, we show a green circle check mark if the result was compared favorably. We show a red triangle exclamation point if the result exceeded a threshold indicating a network insight. The following sections describe each of the details tab results rows and explain the thresholds used for network insights.

Your location information

Test	Result
Your location	Redmond, WA, United States found by the web browser
Network egress location (the location where your network connects to your ISP)	Redmond, WA, United States
✓ Your distance from the network egress location	0 miles (1 kilometers)
✓ Customers in your metropolitan area with better performance	Not a significant number of other customers have better network connectivity.
Time to make a DNS request on your network	:: 192.168.15.2 (19 ms) 1.1.1.1 (22 ms)
✓ Your distance from and/or time to connect to a DNS recursive resolver	108.162.244.89 (21 ms)
✓ If you use a proxy server, distance from your location and time to connect	A proxy server was not identified in your connection
✓ Virtual private network (VPN) you use to connect to your organization	VPN detected: MSFTVPN
✓ VPN Split Tunnel	Exchange Online Optimize is split out Sharepoint Online Optimize is selective tunneled Microsoft Teams Optimize is split out

Exchange Online

Test	Result
✓ Exchange service front door location	Quincy, WA, United States (21 ms). Potential 13 ms improvement
Best Exchange service front door(s) for your location	Cheyenne, WY, United States Quincy, WA, United States Santa Clara, CA, United States
Service front door recorded in the client DNS	outlook.office365.com -> EAT-efz.ms-acdc.office.com [40.97.85.18]

SharePoint Online

Test	Result
The service front door location	Quincy, WA, United States (21 ms)
✓ Download speed	3.43 MBps
✓ Buffer bloat	+66 ms

Microsoft Teams

Test	Result
✓ Media connectivity (audio, video, and application sharing)	No errors
✓ Packet loss	0.08% (target < 1% during 15 s)
✓ Latency	45 ms (target < 100 ms)
✓ Jitter	23 ms (target < 30 ms)

Connectivity

All connectivity tests passed

Your location information

This section shows test results related to your location.

Your location

The user location is detected from the users web browser. It can also be typed in at the user's choice. It's used to identify network distances to specific parts of the enterprise network perimeter. Only the city from this location detection and the distance to other network points are saved in the report.

The user office location is shown on the map view.

Network egress location (the location where your network connects to your ISP)

We identify the network egress IP address on the server side. Location databases are used to look up the approximate location for the network egress. These databases typically have an accuracy of about 90% of IP addresses. If the location looked up from the network egress IP address isn't accurate, this inaccuracy would lead to a false result. To validate if this error is occurring for a specific IP address, you can use publicly accessible network IP address location web sites to compare against your actual location.

Your distance from the network egress location

We determine the distance from that location to the office location. This distance is shown as a network insight if the distance is greater than **500 miles** (800 kilometers) since that is likely to increase the TCP latency by more than 25 ms and might affect user experience.

The map shows the network egress location in relation to the user office location indicating the network backhaul inside of the enterprise WAN.

Implement local and direct network egress from user office locations to the Internet for optimal Microsoft 365 network connectivity. Improvements to local and direct egress are the best way to address this network insight.

Proxy server information

We identify whether proxy server(s) are configured on the local machine to pass Microsoft 365 network traffic in the **Optimize** category. We identify the distance from the user office location to the proxy servers.

The distance is tested first by ICMP ping. If that fails, we test with TCP ping and finally we look up the proxy server IP address in an IP address location database. We show a network insight if the proxy server is further than **500 miles** (800 kilometers) away from the user office location.

Virtual private network (VPN) you use to connect to your organization

This test detects if you're using a VPN to connect to Microsoft 365. A passing result shows if you have no VPN, or if you have a VPN with recommended split tunnel configuration for Microsoft 365.

VPN Split Tunnel

Each Optimize category route for Exchange Online, SharePoint Online, and Microsoft Teams is tested to see if it's tunneled on the VPN. A split out workload avoids the VPN entirely. A tunneled workload is sent over the VPN. A selective tunneled workload has some routes sent over the VPN and some split out. A passing result shows if all workloads are split out or selective tunneled.

Customers in your metropolitan area with better performance

Network latency between the user office location and the Exchange Online service is compared to other Microsoft 365 customers in the same metro area. A network insight is shown if 10% or more of customers in the same metro area have better performance. This means their users have better performance in the Microsoft 365 user interface.

This network insight is generated on the basis that all users in a city have access to the same telecommunications infrastructure and the same proximity to Internet circuits and Microsoft's network.

Time to make a DNS request on your network

This shows the DNS server configured on the client machine that ran the tests. It might be a DNS Recursive Resolver server however this is uncommon. It's more likely to be a DNS forwarder server, which caches DNS results and forwards any uncached DNS requests to another DNS server.

This is provided for information only and doesn't contribute to any network insight.

Your distance from and/or time to connect to a DNS recursive resolver

The in-use DNS Recursive Resolver is identified by making a specific DNS request and then asking the DNS Name Server for the IP Address that it received the same request from. This IP Address is the DNS Recursive Resolver and it's looked up in IP Address location databases to find the location. The distance from the user office location to the DNS Recursive Resolver server location is then calculated. This is shown as a network insight if the distance is greater than **500 miles** (800 kilometers).

The location looked up from the network egress IP Address might not be accurate and this inaccuracy would lead to a false result from this test. To validate if this error is occurring for a specific IP Address, you can use publicly accessible network IP Address location web sites.

This network insight affects the selection of the Exchange Online service front door. To address this insight local and direct network egress should be a prerequisite and then DNS Recursive Resolver should be located close to that network egress.

Exchange Online

This section shows test results related to Exchange Online.

Exchange service front door location

The in-use Exchange service front door is identified in the same way that Outlook does this and we measure the network TCP latency from the user location to it. The TCP latency is shown and the in-use Exchange service front door is compared to the list of best service front doors for the current location. This is shown as a network insight if one of the best Exchange service front doors isn't in use.

Not using one of the best Exchange service front doors could be caused by network backhaul before the corporate network egress in which case we recommend local and direct network egress. It could also be caused by use of a remote DNS recursive resolver server in which case we recommend aligning the DNS recursive resolver server with the network egress.

We calculate a potential improvement in TCP latency (ms) to the Exchange service front door. This is done by looking at the tested user office location network latency and subtracting the network latency from the current location to the closets Exchange service front door. The difference represents the potential opportunity for improvement.

Best Exchange service front door(s) for your location

This lists the best Exchange service front door locations by city for your location.

Service front door recorded in the client DNS

This shows the DNS name and IP Address of the Exchange service front door server that you were directed to. It's provided for information only and there's no associated network insight.

SharePoint

This section shows test results related to SharePoint and OneDrive.

The service front door location

The in-use SharePoint service front door is identified in the same way that the OneDrive client does. We measure the network TCP latency from the user office location to it.

Download speed

We measure the download speed for a 15-Mb file from the SharePoint service front door. The result is shown in megabytes per second to indicate what size file in megabytes can be downloaded from SharePoint or OneDrive in **one second**. The number should be similar to one tenth of the minimum circuit bandwidth in megabits per second. For example if you have a 100mbps internet connection, you may expect 10 megabytes per second (10 MBps).

Buffer bloat

During the 15-Mb download, we measure the TCP latency to the SharePoint service front door. This is the latency under load and it's compared to the latency when not under load. The increase in latency when

under load is often attributable to consumer network device buffers being loaded (or bloated). A network insight is shown for any bloat of 100 ms or more.

Service front door recorded in the client DNS

This shows the DNS name and IP Address of the SharePoint service front door server that you were directed to. It's provided for information only and there's no associated network insight.

Microsoft Teams

This section shows test results related to Microsoft Teams.

Media connectivity (audio, video, and application sharing)

This tests for UDP connectivity to the Microsoft Teams service front door. If this is blocked, then Microsoft Teams might still work using TCP, but audio and video will be impaired. Read more about these UDP network measurements, which also apply to Microsoft Teams at [Media Quality and Network Connectivity Performance in Skype for Business Online](#).

Packet loss

Shows the UDP packet loss measured in a 10-second test audio call from the client to the Microsoft Teams service front door. This should be lower than **1.00%** for a pass.

Latency

Shows the measured UDP latency, which should be lower than **100ms**.

Jitter

Shows the measured UDP jitter, which should be lower than **30ms**.

Connectivity

We test for HTTP connectivity from the user office location to all of the required Microsoft 365 network endpoints. These are published at <https://aka.ms/o365ip>. A network insight is shown for any required network endpoints, which can't be connected to.

Connectivity might be blocked by a proxy server, a firewall, or another network security device on the enterprise network perimeter. Connectivity to TCP port 80 is tested with an HTTP request and connectivity to TCP port 443 is tested with an HTTPS request. If there's no response the FQDN is marked as a failure. If there's an HTTP response code 407 the FQDN is marked as a failure. If there's an HTTP response code 403, then we check the Server attribute of the response and if it appears to be a proxy server we mark this as a failure. You can simulate the tests we perform with the Windows command-line tool curl.exe.

We test the TLS/SSL certificate at each required Microsoft 365 network endpoint that is in the optimize or allow category as defined at <https://aka.ms/o365ip>. If any tests don't find a Microsoft TLS/SSL certificate,

then the encrypted network connected must have been intercepted by an intermediary network device. A network insight is shown on any intercepted encrypted network endpoints.

Where an TLS/SSL certificate is found that isn't provided by Microsoft, we show the FQDN for the test and the in-use TLS/SSL certificate owner. This TLS/SSL certificate owner might be a proxy server vendor, or it might be an enterprise self-signed certificate.

Network path

This section shows the results of an ICMP traceroute to the Exchange Online service front door, the SharePoint service front door, and the Microsoft Teams service front door. It's provided for information only and there's no associated network insight. There are three traceroutes provided. A traceroute to *outlook.office365.com*, a traceroute to the customers SharePoint front end or to *microsoft.sharepoint.com* if one wasn't provided, and a traceroute to *world.tr.teams.microsoft.com*.

! Note

In reports generated in different versions, the addresses you see above may also vary slightly.

Connectivity reports

When you're signed in you can review previous reports that you have run. You can also share them or delete them from the list.

The screenshot shows a Microsoft web interface titled "Connectivity reports". On the left, a sidebar menu includes "Network connectivity test", "Reports" (which is selected), "Network health status", "FAQs", and "Community forum". The main content area is titled "Connectivity reports" and displays a table of five items. The columns are "Date and time", "User", "Location", and "Report link". The data is as follows:

Date and time	User	Location	Report link
9/10/2020, 6:01:40 PM	Paul Rendle	Redmond, WA, United States	View report
9/9/2020, 7:55:08 AM	Paul Rendle	Redmond, WA, United States	View report
9/9/2020, 7:51:34 AM	Paul Rendle	Redmond, WA, United States	View report
9/2/2020, 4:23:24 PM	Paul Rendle	Redmond, WA, United States	View report

Network health status

This shows any significant health issues with Microsoft's global network, which might affect Microsoft 365 customers.

The screenshot shows the Microsoft 365 network health status page. On the left, there's a sidebar with links: Network connectivity test, Reports, Network health status (which is selected), FAQs, and Community forum. The main content area has a title 'Microsoft 365 network health status' and a note: 'There might be delays in the updates to this page. We are updating it manually while we build a more automated solution.' Below this, a paragraph explains that significant issues within Microsoft's global network or with internet connectivity between customers and Microsoft's network will be posted here. It also recommends using Service health in the Microsoft 365 admin center for more detailed information. A table titled '3 items' shows columns for Location, Health, Status, and Details, with a message 'No current issues.' at the bottom. To the right, there are 'Recommended resources' sections for VPN split tunneling, Connectivity principles, and Network services for remote work.

Testing from the Command Line

We provide a command line executable that can be used by your remote deployment, execution tools and run the same tests as are available in the Microsoft 365 network connectivity test tool web site.

The command line test tool can be downloaded here: [Command Line Tool ↗](#)

You can run it by double clicking the executable in Windows File Explorer, or you can start it from a command prompt, or you can schedule it with task scheduler.

The first time you launch the executable you'll be prompted to accept the end user license agreement (EULA) before testing is performed. If you have already read and accepted the EULA, you can create an empty file called Microsoft-365-Network-Connectivity-Test-EULA-accepted.txt in the current working directory for the executable process when it's launched. To accept the EULA, you can type 'y' and press enter in the command line window when prompted.

The executable accepts the following command line parameters:

- -h to show a link to this help documentation
- -testlist <test> Specifies tests to run. By default only basic tests are run. Valid test names include: all, dnsConnectivityPerf, dnsResolverIdentification, bufferBloat, traceroute, proxy, vpn, skype, connectivity, networkInterface
- -filepath <filedir> Directory path of test result files. Allowed value is absolute or relative path of an accessible directory
- -city <city> For the city, state, and country/region fields the specified value will be used if provided. If not provided then Windows Location Services (WLS) will be queried. If WLS fails the location will be detected from the machines network egress
- -state <state>
- -country <country>
- -proxy <account> <password> Proxy account name and password can be provided if you require a proxy to access the Internet

Results

Output of results is written to a JSON file in a folder called TestResults, which is created in the current working directory of the process unless it already exists. The filename format for the output is connectivity_test_result_YYYY-MM-DD-HH-MM-SS.json. The results are in JSON nodes that match the output shown on the web page for the Microsoft 365 network connectivity test tool web site. A new result file is created each time you run it and the standalone executable doesn't upload results to your Microsoft tenant for viewing in the Admin Center Network Connectivity pages. Front door codes, longitudes, and latitudes aren't included in the result file.

Launching from Windows File Explorer

You can double select on the executable to start the testing and a command prompt window will appear.

Launching from the Command Prompt

In a CMD.EXE command prompt window, you can type the path and name of the executable to run it. The filename is MicrosoftConnectivityTest.exe.

Launching from Windows Task Scheduler

In Windows Task Scheduler, you can add a task to launch the standalone test executable. You should specify the current working directory of the task to be where you have created the EULA accepted file since the executable blocks until the EULA is accepted. You can't interactively accept the EULA if the process is started in the background with no console.

More details on the standalone executable

The commandline tool uses Windows Location Services to find the users City State Country/region information for determining some distances. If Windows Location Services is disabled in the control panel, then user location based assessments are blank. In Windows Settings, "Location services" must be on and "Let desktop apps access your location" must also be on.

The commandline tool attempts to install the .NET Framework if it isn't already installed. It also downloads the main testing executable from the Microsoft 365 network connectivity test tool and launch that.

Test using the Microsoft Support and Recovery Assistant

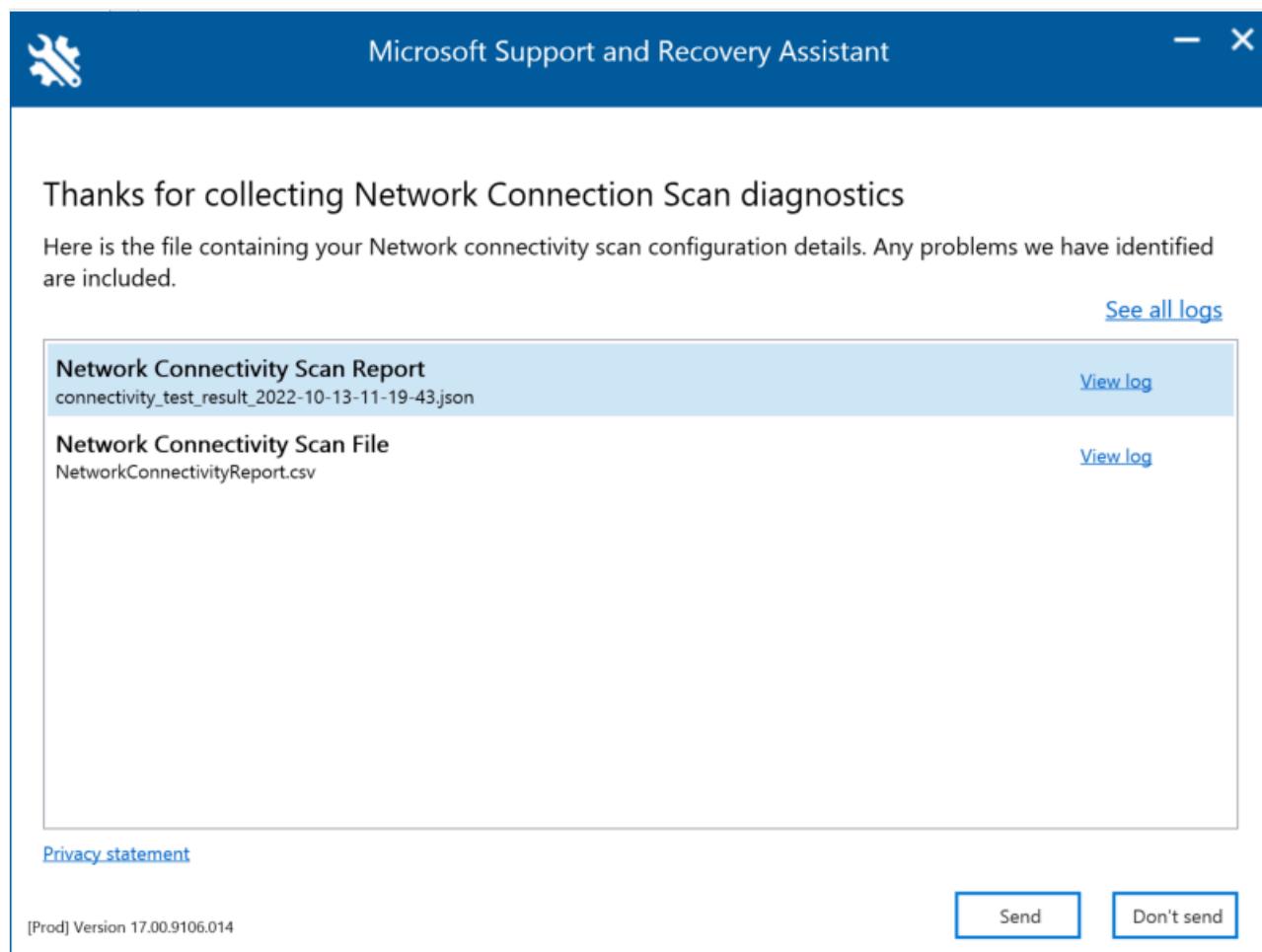
[Microsoft Support and Recovery Assistant](#) (Assistant) automates all the steps required to execute the command-line version of the Microsoft 365 network connectivity test tool on a user's machine and creates a report similar to the one created by the web version of the connectivity test tool. Note, the Assistant runs the command line version of Microsoft 365 network connectivity test tool to produce the same JSON result file, but the JSON file is converted into .CSV file format.

You can [download and run the Assistant here](#).

Viewing Test Results

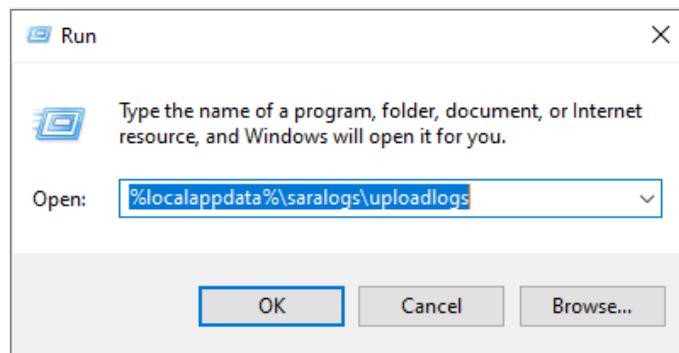
Reports can be accessed in the following ways:

The reports are available on the below screen once the Assistant has finished scanning the user's machine. To access these reports, simply select on the "View log" option to view them.

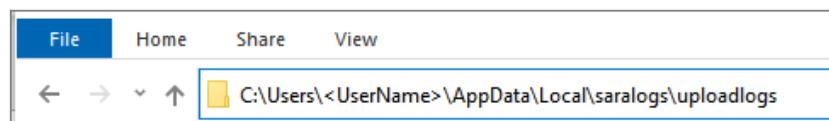


Connectivity test results and Telemetry data are collected and uploaded to the **uploadlogs** folder. To access this folder, use one of the following methods:

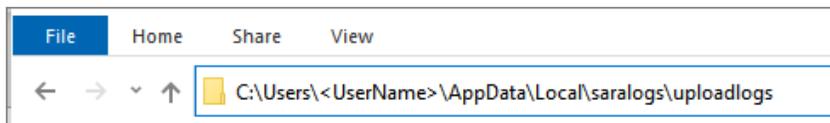
- Open Run (Windows logo key + R), and run the %localappdata%\saralogs\uploadlogs command as follows:



- In File Explorer, type C:\Users<UserName>\AppData\Local\saralogs\uploadlogs and press **Enter** as follows:



Note: <UserName> is the user's Windows profile name. To view the information about the test results and telemetry, double-click and open the files.



Types of result files

Microsoft Support and Recovery Assistant creates two files:

1. Network Connectivity Report (CSV) This report runs the raw JSON file against a rule engine to make sure defined thresholds are being met and if they aren't met a "warning" or "error" is displayed in the output column of the CSV file. You can view the NetworkConnectivityReport.csv file to be informed about any detected issues or defects. See [What happens at each test step](#) for details on each test and the thresholds for warnings.
2. Network Connectivity Scan Report (JSON) This file provides the raw output test results from the command-line version of the Microsoft 365 network connectivity test tool (MicrosoftConnectivityTest.exe).

FAQ

Here are answers to some of our frequently asked questions.

What is required to run the advanced test client?

The advanced test client requires .NET 6.0 Runtime. If you run the advanced test client without that installed you'll be directed to [the .NET 6.0 installer page](#). Be sure to install from the Run desktop apps column for Windows. Administrator permissions on the machine are required to install .NET 6.0 Runtime.

The advanced test client uses SignalR to communicate to the web page. For this, you must ensure that TCP port 443 connectivity to **connectivity.service.signalr.net** is open. This URL isn't published in the <https://aka.ms/o365ip> because that connectivity isn't required for a Microsoft 365 client application user. If you're using an HTTP proxy for connection to FQDN connectivity.office.com and encounter the error **SignalR proxy configuration is different than origin.**, ensure connection to FQDN connectivity.service.signalr.net is allowed through the proxy. If a PAC file is being used to push proxy configuration settings, ensure the PAC file will return the same proxy settings for FQDN's connectivity.office.com and connectivity.service.signalr.net.

What is Microsoft 365 service front door?

The Microsoft 365 service front door is an entry point on Microsoft's global network where Office clients and services terminate their network connection. For an optimal network connection to Microsoft 365, It's recommended that your network connection is terminated into the closest Microsoft 365 front door in your city or metro.

Note

Microsoft 365 service front door has no direct relationship to the **Azure Front Door Service** product available in the Azure marketplace.

What is the best Microsoft 365 service front door?

A best Microsoft 365 service front door (formerly known as an optimal service front door) is one that is closest to your network egress, generally in your city or metro area. Use the Microsoft 365 network performance tool to determine location of your in-use Microsoft 365 service front door and the best service front door(s). If the tool determines your in-use front door is one of the best ones, then you should expect great connectivity into Microsoft's global network.

What is an internet egress location?

The internet egress Location is the location where your network traffic exits your enterprise network and connects to the Internet. This is also identified as the location where you have a Network Address Translation (NAT) device and usually where you connect with an Internet Service Provider (ISP). If you see a long distance between your location and your internet egress location, then this might identify a significant WAN backhaul.

Related articles

[Network connectivity in the Microsoft 365 Admin Center](#)

[Microsoft 365 network performance insights](#)

[Microsoft 365 network assessment](#)

[Microsoft 365 Network Connectivity Location Services](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Microsoft 365 Network Provider Program

Article • 06/26/2024

Network connectivity has a direct impact on your users' ability to work quickly, collaborate effectively, and streamline business processes with Microsoft 365. For customers in any stage of their digital transformation, network design is a critical aspect that should be proactively addressed before issues negatively impact user experience.

As customers adopt Microsoft 365 for business productivity, Microsoft has observed a common trend that network performance and the resulting end-user collaboration experience is directly influenced by network solutions in the path between the user and Microsoft 365. To help partners design optimal network solutions and help customers make informed decisions regarding such solutions, we built the Microsoft 365 Network Provider Program.

The Microsoft 365 Network Provider Program deepens our collaboration with network partners and identifies key products and solutions that follow Microsoft 365 networking requirements, recommendations, and best practices. The goal of the Microsoft 365 Network Provider program is to facilitate customer ability to improve their Microsoft 365 experience through easy discovery of validated partner solutions that consistently demonstrate alignment to key principles for optimal Microsoft 365 connectivity in customer deployments.

To modernize enterprise networks for great connectivity to Microsoft 365, customers often rely on network solution providers, on-premises or cloud-based security services, and system integrators to plan, design, and implement network connectivity for cloud services. Customers often ask Microsoft whether their network architecture and solutions work with Microsoft 365 and whether they align with Microsoft's [Network Connectivity Principles for Microsoft 365](#).

The Microsoft 365 Network Provider Program demonstrates Microsoft's commitment to help our customers get the best Microsoft 365 experience. The Microsoft 365 team works with many network industry partners to help ensure that key principles for optimal connectivity are natively built into their network product and solutions.

The Microsoft 365 Network Provider program is in preview for a limited number of network providers. If you are interested in participating in the preview to give early feedback on the program, please register your interest by [filling out the form](#) ↗.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Tenant roadmap for Microsoft 365

Article • 02/12/2024

Your Microsoft 365 tenant is the set of services assigned to your organization. Typically, this tenant is associated with one or more of your public DNS domain names and acts as a central and isolated container for different subscriptions and the licenses within them that you assign to user accounts. For more information, see [Subscriptions, licenses, accounts, and tenants for Microsoft's cloud offerings](#).

When you create a Microsoft 365 tenant, you assign it to a specific geographical location. You can also have a tenant with multiple geographical locations and move your tenant from one location to another.

To get your tenant ready for user, groups, licenses, and cloud apps, it's critical to carefully plan and execute your tenant configuration.

Set up your Microsoft 365 tenant

Before you begin planning your network for Microsoft 365 network connectivity, it's important to understand the connectivity principles for securely managing Microsoft 365 traffic and getting the best possible performance. Ensure that your networking is optimized for access to Microsoft 365 for both on-premises and remote workers by [understanding and planning for Microsoft 365 network optimization](#).

Your next big tasks are planning for and then configuring your Microsoft 365 tenant for DNS domain names, common services, and for that identity infrastructure that supports secure user sign-in.

Plan

To plan for your tenant implementation:

- Understand subscriptions, licenses, and Microsoft Entra tenants
- Understand how to use third-party SSL certificates
- Understand the ways a Microsoft 365 tenant is integrated with Microsoft Entra services
- Plan for client app support
- Determine how to use hybrid modern authentication
- Plan for Office 2007 and Office 2010 upgrades
- Understand tenant isolation

Deploy

To deploy your tenant:

- Add the [DNS domains](#) for your organization.
- Use the [setup guides in the Microsoft 365 admin center](#).
- Build out your [identity infrastructure](#).

Move a tenant's geographic locations

Microsoft continues to open new datacenter geographic locations (geos) for Microsoft 365 services. These new datacenter geos add capacity and compute resources to support customer demand and usage growth. Additionally, the new datacenter geos offer in-geo data residency for core customer data.

For more information, see [Moving core data to new Microsoft 365 datacenter geos](#).

Deploy Microsoft 365 Multi-Geo

With Microsoft 365 Multi-Geo, your organization can expand its Microsoft 365 presence to multiple geographic regions and/or countries within your existing tenant.

For more information, see [Microsoft 365 Multi-Geo](#).

Manage multiple Microsoft 365 tenants

Although having a single tenant for your organization is ideal, you may be one of many organizations that have multiple tenants. Reasons can include mergers and acquisitions, you want administrative isolation, or you have a decentralized IT.

If you have multiple Microsoft 365 tenants, see these articles for more information about:

- [Inter-tenant collaboration](#)
- [Cross-tenant mailbox migration](#)
- [Tenant-to-tenant migrations](#)

Next step

Start your tenant planning with [Subscriptions, licenses, accounts, and tenants](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Subscriptions, licenses, accounts, and tenants for Microsoft's cloud offerings

Article • 07/22/2024

Microsoft provides a hierarchy of organizations, subscriptions, licenses, and user accounts for consistent use of identities and billing across its cloud offerings:

- Microsoft 365 and Microsoft Office 365
- Microsoft Azure
- Microsoft Dynamics 365

Elements of the hierarchy

Here are the elements of the hierarchy:

Organization

An organization represents a business entity that is using Microsoft cloud offerings, typically identified by one or more public Domain Name System (DNS) domain names, such as contoso.com. The organization is a container for subscriptions.

Subscriptions

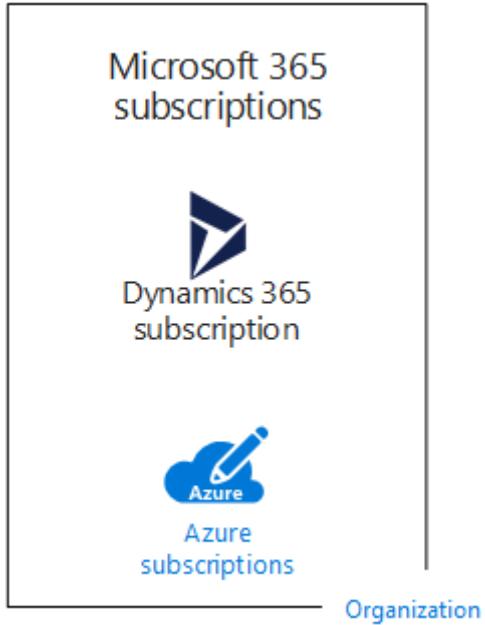
A subscription is an agreement with Microsoft to use one or more Microsoft cloud platforms or services, for which charges accrue based on either a per-user license fee or on cloud-based resource consumption.

- Microsoft's Software as a Service (SaaS)-based cloud offerings (Microsoft 365 and Dynamics 365) charge per-user license fees.
- Microsoft's Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) cloud offerings (Azure) charge based on cloud resource consumption.

You can also use a trial subscription, but the subscription expires after a specific amount of time or consumption charges. You can convert a trial subscription to a paid subscription.

Organizations can have multiple subscriptions for Microsoft's cloud offerings. Figure 1 shows a single organization that has multiple Microsoft 365 subscriptions, a Dynamics 365 subscription, and multiple Azure subscriptions.

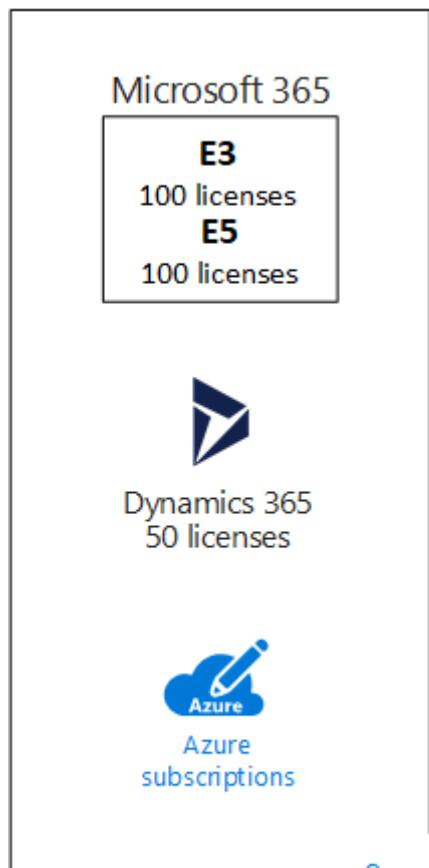
Figure 1: Example of multiple subscriptions for an organization



Licenses

For Microsoft's SaaS cloud offerings, a license allows a specific user account to use the services of the cloud offering. You are charged a fixed monthly fee as part of your subscription. Administrators assign licenses to individual user accounts in the subscription. For the example in Figure 2, the Contoso Corporation has a Microsoft 365 E5 subscription with 100 licenses, which allows up to 100 individual user accounts to use Microsoft 365 E5 features and services.

Figure 2: Licenses within the SaaS-based subscriptions for an organization



① Note

A security best practice is to use separate user accounts that are assigned specific roles for administrative functions. These dedicated administrator accounts do not need to be assigned a license for the cloud services that they administer. For example, a SharePoint administrator account does not need to be assigned a Microsoft 365 license.

For Azure PaaS-based cloud services, software licenses are built into the service pricing.

For Azure IaaS-based virtual machines, additional licenses to use the software or application installed on a virtual machine image might be required. Some virtual machine images have licensed versions of software installed and the cost is included in the per-minute rate for the server. Examples are the virtual machine images for SQL Server 2014 and SQL Server 2016.

Some virtual machine images have trial versions of applications installed and need additional software application licenses for use beyond the trial period. For example, the SharePoint Server 2016 Trial virtual machine image includes a trial version of SharePoint Server 2016 pre-installed. To continue using SharePoint Server 2016 after the trial expiration date, you must purchase a SharePoint Server 2016 license and client licenses.

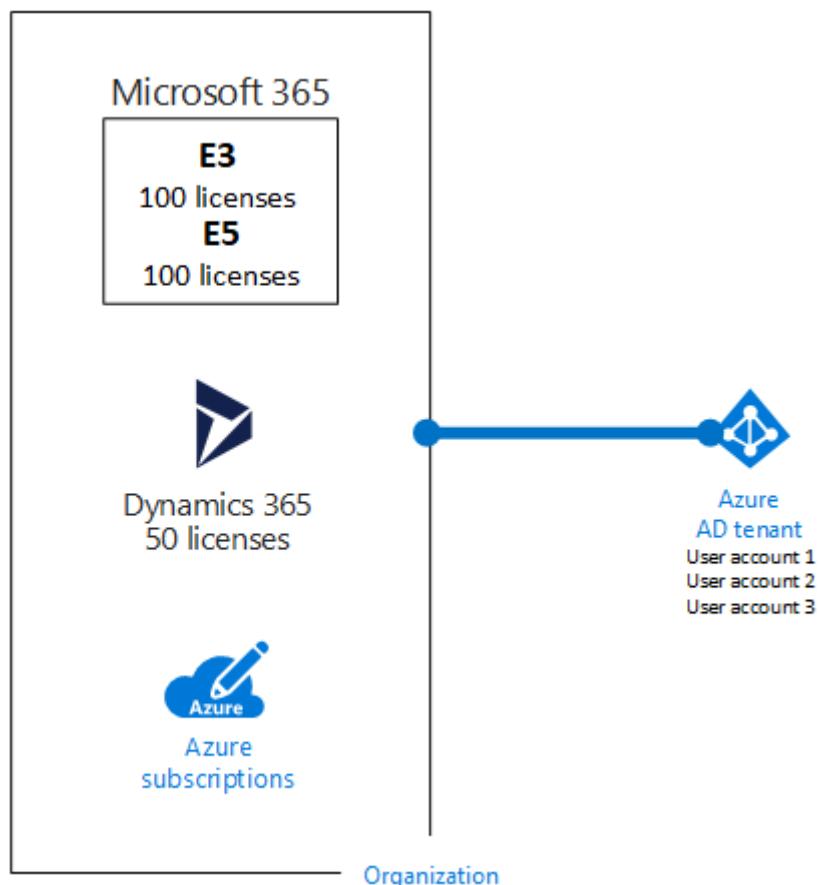
from Microsoft. These charges are separate from the Azure subscription and the per-minute rate to run the virtual machine still applies.

User accounts

User accounts for all of Microsoft's cloud offerings are stored in a Microsoft Entra tenant, which contains user accounts and groups. A Microsoft Entra tenant can be synchronized with your existing Active Directory Domain Services (AD DS) accounts using Microsoft Entra Connect, a Windows server-based service. This is known as directory synchronization.

Figure 3 shows an example of multiple subscriptions of an organization using a common Microsoft Entra tenant that contains the organization's accounts.

Figure 3: Multiple subscriptions of an organization that use the same Microsoft Entra tenant



Tenants

For SaaS cloud offerings, the tenant is the regional location that houses the servers providing cloud services. For example, the Contoso Corporation chose the European region to host its Microsoft 365, EMS, and Dynamics 365 subscriptions for the 15,000 workers in their Paris headquarters.

Azure PaaS services and virtual machine-based workloads hosted in Azure IaaS can have tenancy in any Azure datacenter across the world. You specify the Azure datacenter, known as the location, when you create the Azure PaaS app or service or element of an IaaS workload.

A Microsoft Entra tenant is a specific instance of Microsoft Entra ID containing accounts and groups. Paid or trial subscriptions of Microsoft 365 or Dynamics 365 include a free Microsoft Entra tenant. This Microsoft Entra tenant does not include other Azure services and is not the same as an Azure trial or paid subscription.

Summary of the hierarchy

Here is a quick recap:

- An organization can have multiple subscriptions.
 - A subscription can have multiple licenses.
 - Licenses can be assigned to individual user accounts.
 - User accounts are stored in a Microsoft Entra tenant.

Here is an example of the relationship of organizations, subscriptions, licenses, and user accounts:

- An organization identified by its public domain name.
 - A Microsoft 365 E3 subscription with user licenses.
 - A Microsoft 365 E5 subscription with user licenses.
 - A Dynamics 365 subscription with user licenses.
 - Multiple Azure subscriptions.
 - The organization's user accounts in a common Microsoft Entra tenant.

Multiple Microsoft cloud offering subscriptions can use the same Microsoft Entra tenant that acts as a common identity provider. A central Microsoft Entra tenant that contains the synchronized accounts of your on-premises AD DS provides cloud-based Identity as a Service (IDaaS) for your organization.

Figure 4: Synchronized on-premises accounts and IDaaS for an organization

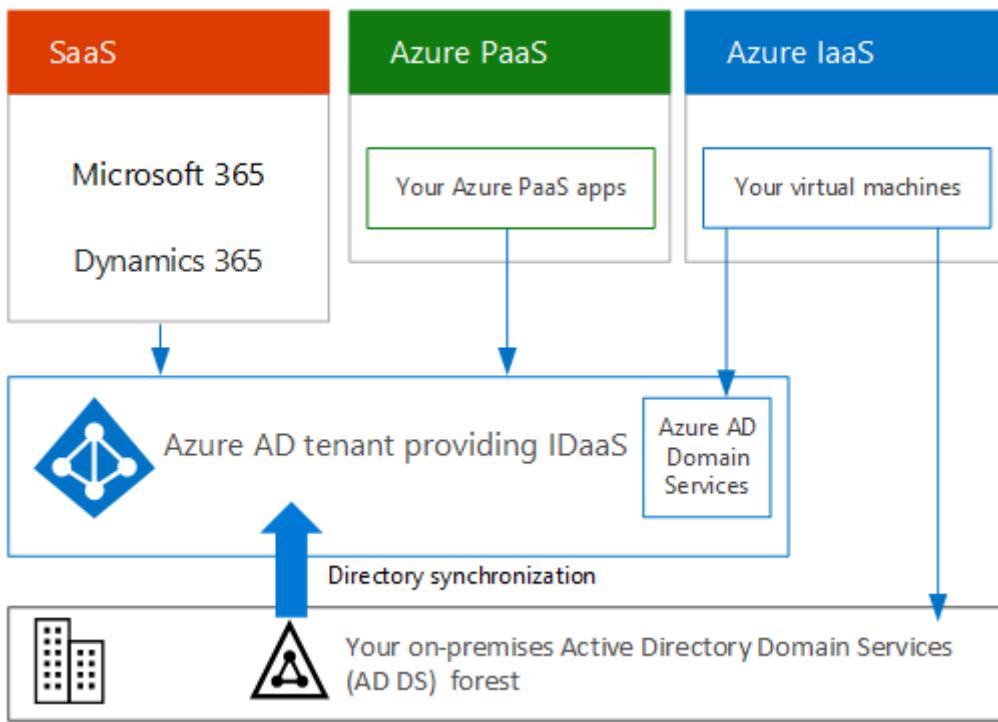


Figure 4 shows how a common Microsoft Entra tenant is used by Microsoft's SaaS cloud offerings, Azure PaaS apps, and virtual machines in Azure IaaS that use Microsoft Entra Domain Services. Microsoft Entra Connect synchronizes the on-premises AD DS forest with the Microsoft Entra tenant.

Combining subscriptions for multiple Microsoft cloud offerings

The following table describes how you can combine multiple Microsoft cloud offerings based on already having a subscription for one type of cloud offering (the labels going down the first column) and adding a subscription for a different cloud offering (going across the columns).

[Expand table](#)

	Microsoft 365	Azure	Dynamics 365
Microsoft 365	NA	You add an Azure subscription to your organization from the Azure portal.	You add a Dynamics 365 subscription to your organization from the Microsoft 365 admin center.
Azure	You add a Microsoft 365 subscription to your organization.	NA	You add a Dynamics 365 subscription to your organization.

	Microsoft 365	Azure	Dynamics 365
Dynamics 365	You add a Microsoft 365 subscription to your organization.	You add an Azure subscription to your organization from the Azure portal.	NA

An easy way to add subscriptions to your organization for Microsoft SaaS-based services is through the admin center:

1. Sign in to the Microsoft 365 admin center (<https://admin.microsoft.com>) with your **User Admin** account.
2. From the left navigation of the **Admin center** home page, click **Billing**, and then **Purchase services**.
3. On the **Purchase services** page, purchase your new subscriptions.

The admin center assigns the organization and Microsoft Entra tenant of your Microsoft 365 subscription to the new subscriptions for SaaS-based cloud offerings.

To add an Azure subscription with the same organization and Microsoft Entra tenant as your Microsoft 365 subscription:

1. Sign in to the Azure portal (<https://portal.azure.com>) with your Microsoft 365 **Microsoft Entra DC admin** account.
2. In the left navigation, click **Subscriptions**, and then click **Add**.
3. On the **Add subscription** page, select an offer and complete the payment information and agreement.

If you purchased Azure and Microsoft 365 subscriptions separately and want to access the Microsoft 365 Microsoft Entra tenant from your Azure subscription, see the instructions in [Add an existing Azure subscription to your Microsoft Entra tenant](#).

See also

[Microsoft cloud for enterprise architects illustrations](#)

[Architectural models for SharePoint, Exchange, Skype for Business, and Lync](#)

[Hybrid solutions](#)

Next step

Assessing Microsoft 365 network connectivity

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Plan for third-party SSL certificates for Microsoft 365

Article • 03/21/2024

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

To encrypt communications between your clients and the Microsoft 365 environment, third-party Secure Socket Layer (SSL) certificates must be installed on your infrastructure servers.

This article is part of [Network planning and performance tuning for Microsoft 365](#).

Certificates are required for the following Microsoft 365 components:

- Exchange on-premises
- Single sign-on (SSO) (for both the Active Directory Federation Services (AD FS) federation servers and AD FS federation server proxies)
- Exchange Online services, such as Autodiscover, Outlook Anywhere, and Exchange Web Services
- Exchange hybrid server

Certificates for Exchange on-premises

For an overview about how to use digital certificates to make the communication between the on-premises Exchange organization and Exchange Online secure, see the TechNet article [Understanding Certificate Requirements](#).

Certificates for single sign-on

To provide your users with a simplified single sign-on experience that includes robust security, the certificates shown in the following table are required on either the federation servers or the federation server proxies. The table below focuses on Active Directory Federation Services (AD FS), we also have more information on [using third-party identity providers](#).

[+] Expand table

Certificate Type	Description	What you need to know before you deploy
SSL certificate (also called a server authentication certificate)	This is a standard SSL certificate that is used to make communications between federation servers, clients, and federation server proxy computers secure.	<p>AD FS requires an SSL certificate. By default, AD FS uses the SSL certificate that is configured for the default website in Internet Information Services (IIS). The subject name of this SSL certificate is used to determine the Federation Service (FS) name for each instance of AD FS that you deploy. Consider choosing a subject name for any new certification authority (CA)-issued certificates that best represents the name of your company or organization to Microsoft 365. This name must be Internet-routable.</p> <p>Caution: AD FS requires that this SSL certificate have no dotless (short-name) subject name.</p> <p>Recommendation: Because this certificate must be trusted by clients of AD FS, we recommend that you use an SSL certificate issued by a public (third-party) CA or by a CA that is subordinate to a publicly trusted root; for example, VeriSign or Thawte.</p>
Token-signing certificate	This is a standard X.509 certificate that's used for securely signing all tokens that the federation server issues and that Microsoft 365 accepts and validates.	<p>The token-signing certificate must contain a private key that chains to a trusted root in the FS. By default, AD FS creates a self-signed certificate. However, depending on the needs of your organization, you can change this certificate to a CA-issued certificate by using the AD FS management snap-in.</p> <p>Caution: The token-signing certificate is critical to the stability of the FS. If the certificate is changed, Microsoft 365 must be notified of the change. If notification isn't provided, users can't sign in to their Microsoft 365 service offerings.</p> <p>Recommendation: We recommend that you use the self-signed token-signing certificate that is generated by AD FS. By doing so, it manages this certificate for you by default. For example, when this certificate is about to expire, AD FS will generate a new self-signed certificate.</p>

Federation server proxies require the certificate that is described in the following table.

[Expand table](#)

Certificate Type	Description	What you need to know before you deploy
SSL certificate	<p>This is a standard SSL certificate that is used for securing communications between a federation server, a federation server proxy, and Internet client computers.</p>	<p>This SSL certificate must be bound to the default website in IIS before you can successfully run the AD FS Federation Server Proxy Configuration wizard.</p> <p>This certificate must have the same subject name as the SSL certificate that was configured on the federation server in the corporate network.</p> <p>Recommendation: We recommend that you use the same server authentication certificate that is configured on the federation server that this federation server proxy connects to.</p>

Certificates for Autodiscover, Outlook Anywhere, and Active Directory Synchronization

Your external-facing Exchange 2013, Exchange 2010, Exchange 2007, and Exchange 2003 Client Access servers (CASs) require a third-party SSL certificate for secure connections for Autodiscover, Outlook Anywhere, and Active Directory synchronization services. You may already have this certificate installed in your on-premises environment.

Certificate for an Exchange Hybrid Server

Your external-facing Exchange hybrid server or servers require a third-party SSL certificate for secure connectivity with the Exchange Online service. You need to get this certificate from your third-party SSL provider.

Microsoft 365 Certificate Chains

This article describes the certificates you might need to install on your infrastructure. For more information on the certificates installed on our Microsoft 365 servers, see [Microsoft 365 Certificate Chains](#).

See also

[Microsoft 365 Enterprise overview](#)

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Advanced deployment guides for Microsoft 365 and Office 365 products

Article • 12/19/2023

Microsoft 365 and Office 365 advanced deployment guides give you tailored guidance and resources for planning and deploying your tenant, apps, and services. These guides are created using the same best practices that [Microsoft 365 FastTrack](#) onboarding specialists share in individual interactions. They provide information on product setup, enabling security features, deploying collaboration tools, and provide scripts to speed up advanced deployments.

All advanced deployment guides are available in the Microsoft 365 admin center as described in the section below, and most guides can also be found in the [Microsoft 365 Setup portal](#).

Access to advanced deployment guides in the admin center requires authentication to a Microsoft 365 tenant as an administrator or other role with access to the admin center. Advanced deployment guides in the Microsoft 365 Setup portal can be accessed by anyone. We have provided links to both locations for each guide, where available, in the tables below.

Note that guides are still being added to the setup portal, but there are a few guides that will only be available in the admin center because they require authentication to a tenant to function.

In this article:

- [How to access advanced deployment guides in the Microsoft 365 admin center](#)
- [Guides for initial setup](#)
- [Guides for authentication and access](#)
- [Guides for security and compliance](#)
- [Guides for collaboration](#)
- [Advanced guides](#)

How to access advanced deployment guides in the Microsoft 365 admin center

Advanced deployment guides are accessible from the [Advanced deployment guides & assistance](#) page in the Microsoft 365 admin center. When you access advanced deployment guides from the admin center, you can keep track of the status of your

progress and return at any time to complete a guide. This functionality is not available when you access guides from the [Microsoft 365 Setup portal](#).

Note

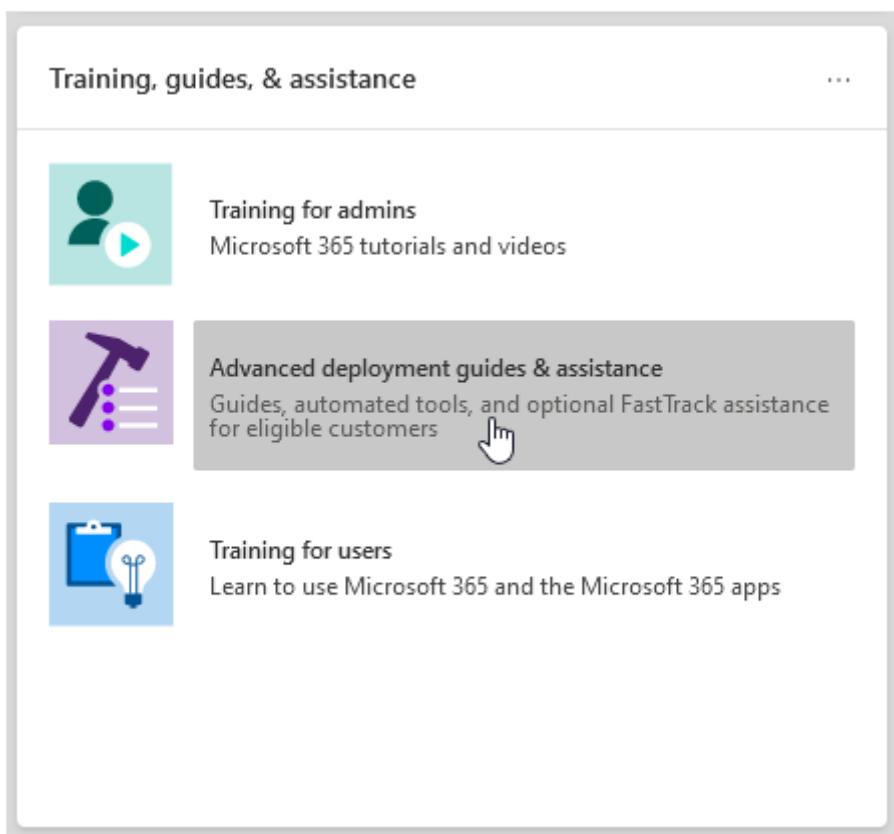
You must be assigned an admin role such as *Global Reader* to access advanced deployment guides in the Microsoft 365 admin center. Only admins with the *Global Administrator* role can use the guides to change settings in the tenant.

Important

Any selections, task assignments, and progress status saved **before January 10, 2023** within each advanced deployment guide in the admin center were reset due to EU data regulations.

To reach the **Advanced deployment guides & assistance** page:

1. In the [Microsoft 365 admin center](#), go to the **Home** page.
2. Find the *Training, guides & assistance* card and select **Advanced deployment guides & assistance**.
3. If you don't see that card, access the page directly at (<https://aka.ms/advanceddeploymentguides>).



Guides for initial setup

Advanced deployment guides in the admin center require authentication to a Microsoft 365 tenant as an administrator or other role with access to the admin center, but guides in the Microsoft 365 Setup portal can be accessed by anyone.

[+] Expand table

Guide - Setup Portal	Guide - Admin Center	Description
Microsoft 365 Copilot setup guide	Microsoft 365 Copilot setup guide	The Microsoft 365 Copilot setup guide gets you up to speed on Copilot, which revolutionizes collaboration and takes advantage of AI to automate tasks such as writing, editing, and data visualization across Word, Excel, PowerPoint, Outlook, and Teams. Copilot also simplifies the creation of meeting summaries. Our setup guide facilitates smooth integration, allowing your organization to automate work processes and enhance collaboration seamlessly.
Prepare your environment guide	Prepare your environment guide	The Prepare your environment guide helps you prepare your organization's environment for Microsoft 365 and Office 365 services. Whatever your goals are, there are tasks you'll need to complete to ensure a successful deployment. To avoid any errors while preparing your environment, you're provided with step-by-step instructions to connect your domain, add users, assign licenses, set up email with Exchange Online, and install or deploy Office apps.
Email setup guide	Email setup guide	The Email setup guide provides you with the step-by-step guidance needed for configuring Exchange Online for your organization. This guidance includes setting up new email accounts, migrating email, and configuring email protection. For a successful email setup, use this advisor and you'll receive the recommended migration method based on your organization's current mail system, the number of mailboxes being migrated, and how you want to manage users and their access.
Gmail contacts and calendar advisor	Gmail contacts and calendar advisor	When you migrate a Gmail user's mailbox to Microsoft 365, email messages are migrated, but contacts and calendar items are not. The Gmail contacts and calendar advisor provides steps for importing Google contacts and Google calendar items to Microsoft 365 using import and export methods with Outlook.com, the Outlook client, or PowerShell.

Guide - Setup Portal ↗	Guide - Admin Center ↗	Description
	Microsoft 365 setup guide ↗	<p>The Microsoft 365 setup guide provides you with guidance when setting up productivity tools, security policies, and device management capabilities. With a Microsoft 365 Business Premium or Microsoft 365 for enterprise subscription, you can use this guide to set up and configure your organization's devices.</p> <p>You'll receive guidance and access to resources to enable your cloud services, update devices to the latest supported version of Windows 10, and join devices to Microsoft Entra ID, all in one central location.</p>
	Remote work setup guide ↗	<p>The Remote work setup guide provides organizations with the tips and resources needed to ensure your users can successfully work remotely, your data is secure, and users' credentials are safeguarded.</p> <p>You'll receive guidance to optimize remote workers' device traffic to both Microsoft 365 resources in the cloud and your organization's network, which will reduce the strain on your remote access VPN infrastructure.</p>
Windows 11 and Surface setup guide ↗	Windows 11 and Surface setup guide ↗	<p>The Windows 11 and Surface setup guide provides information on deployment capabilities, tools, and strategies for deploying Windows 11 for new devices, existing devices, and Surface devices. You'll gain knowledge on setting up co-management with Intune, using autopilot for customizing the out-of-box experience, and reviewing endpoint security features. This information will provide a starting point for planning your Windows 11 deployment.</p>
Microsoft Edge setup guide ↗	Microsoft Edge setup guide ↗	<p>Microsoft Edge has been rebuilt from the ground up to bring you world-class compatibility and performance, the security and privacy you deserve, and new features designed to bring you the best of the web.</p> <p>The Microsoft Edge setup guide will help you configure Enterprise Site Discovery to see which sites accessed in your org might need to use IE mode, review and configure important security features, configure privacy policies and compliance policies to meet your org's requirements, and manage web access on your devices. You can download Microsoft Edge to individual devices, or we'll show you how to deploy to multiple users in your org with Group Policy, Configuration Manager, or Microsoft Intune.</p>
Configure IE mode for Microsoft Edge guide ↗	Configure IE mode for Microsoft Edge guide ↗	<p>If you've already deployed Microsoft Edge and only want to configure IE mode, the Configure IE mode for Microsoft Edge guide will give you scripts to automate the configuration of Enterprise Site Discovery. You'll also get IE</p>

Guide - Setup Portal	Guide - Admin Center	Description
		mode recommendations from a cloud-based tool that will help you create an Enterprise Mode Site List to deploy to your users.
Microsoft Search setup guide ↗		<p>Microsoft Search helps your organization find what they need to complete what they're working on. Whether it's searching for people, files, org charts, sites, or answers to common questions, your org can use Microsoft Search throughout their workday to get answers.</p> <p>The Microsoft Search setup guide helps you configure Microsoft Search whether you want to pilot it to a group of users or roll it out to everyone in your org. You'll assign Search admins and Search editors and then customize the search experience for your users with answers and more options, like adding the Bing extension to Chrome or setting Bing as your default search engine.</p>
Block use of Internet Explorer in your organization guide ↗		<p>Microsoft support for Internet Explorer 11 is ending soon for most versions of Windows 10. The Block use of Internet Explorer in your organization guide ensures that your users can still run legacy web apps that rely on Internet Explorer. This guide also helps you move those users to Microsoft Edge with IE mode.</p>

Guides for authentication and access

[Expand table](#)

Guide - Setup Portal	Guide - Admin Center	Description
Configure multifactor authentication (MFA) guide ↗		<p>The Configure multifactor authentication (MFA) guide provides customers who have the Microsoft Entra ID P1 or Microsoft Entra ID P2 license with customizable Conditional Access templates that include the most common and least intrusive security standards. Customers with the P2 license can also use risk-based Conditional Access policies. Customers without a P1 or P2 license can use a one-click solution to enable security defaults, a baseline protection policy for all users. They can also enable legacy (per-user) MFA.</p>
Identity security for Teams guide ↗		<p>The Identity security for Teams guide helps you with some basic security steps you can take to ensure your</p>

Guide - Setup Portal ↗	Guide - Admin Center ↗	Description
		users are safe and have the most productive time using Teams.
Microsoft Entra setup guide ↗	Microsoft Entra setup guide ↗	<p>The Microsoft Entra setup guide provides information to ensure your organization has a strong security foundation. In this guide you'll set up initial features, like Azure Role-based access control (Azure RBAC) for admins, Microsoft Entra Connect for your on-premises directory, and Microsoft Entra Connect Health, so you can monitor your hybrid identity's health during automated syncs. It also includes essential information on enabling self-service password resets, conditional access, and integrated third party sign-on including optional advanced identity protection and user provisioning automation.</p>
Add or sync users to Microsoft Entra ID guide ↗	Add or sync users to Microsoft Entra ID guide ↗	<p>The Add or sync users to Microsoft Entra ID guide will help streamline the process of getting your user accounts set up in Microsoft 365. Based on your environment and needs, you can choose to add users individually, migrate your on-premises directory with Microsoft Entra Cloud Sync or Microsoft Entra Connect, or troubleshoot existing sync problems when necessary.</p>
	Plan your passwordless deployment guide ↗	<p>Use the Plan your passwordless deployment guide to discover the best passwordless authentication methods to use and receive guidance on how to upgrade to an alternative sign-in approach that allows users to access their devices securely with one of the following passwordless authentication methods:</p> <ul style="list-style-type: none"> • Windows Hello for Business • The Microsoft Authenticator app • Security keys • Temporary Access Pass
	Secure your cloud apps with Single Sign on (SSO) guide ↗	<p>This guide is designed to help you add cloud apps to Microsoft 365. In our guide, you can add an application to your tenant, add users to the app, assign roles, and more. If the app supports single sign-on (SSO), we'll walk you through that configuration.</p>
Plan your self-service password reset (SSPR)	Plan your self-service password reset (SSPR) deployment guide ↗	<p>Give users the ability to change or reset their password independently, if their account is locked, or they forget their password without the need to contact a helpdesk engineer.</p> <p>Use the Plan your self-service password reset (SSPR)</p>

Guide - Setup Portal	Guide - Admin Center	Description
deployment guide ↗		deployment guide to receive relevant articles and instructions for configuring the appropriate Azure portal options to help you deploy SSPR in your environment.
Migrate from AD FS to Microsoft Entra ID ↗	Migrate from AD FS to Microsoft Entra ID ↗	In Migrate from AD FS to Microsoft Entra ID we offer custom guidance for migrating from Active Directory Federation Services (AD FS) to Microsoft Entra ID. You'll first answer a few questions about your AD FS infrastructure. Then implement either pass-through authentication (PTA) or password hash sync (PHS) to give users a streamlined experience while accessing your organization's apps.

Guides for security and compliance

[+] Expand table

Guide - Setup Portal	Guide - Admin Center	Description
Security analyzer ↗	Security analyzer ↗	The Security analyzer will analyze your security approach and introduce you to Microsoft integrated security and compliance solutions that can improve your security posture. You'll learn about advanced features, such as managing identities and helping to protect against modern attacks. You can then sign up for a trial subscription and be pointed to the corresponding setup guidance for each solution.
Set up your Microsoft Zero Trust security model ↗	Set up your Microsoft Zero Trust security model ↗	Use the Set up your Zero Trust security model guide to configure security that effectively adapts to the complexity of the modern environment, embraces the hybrid workplace, and helps protect people, devices, apps, and data wherever they're located. Key recommendations include: always authenticate, limit user access, minimize the blast radius, segment access, verify end-to-end encryption, and use analytics to get visibility, drive threat detection, and improve defenses.
Deploy and set up Microsoft Intune ↗	Deploy and set up Microsoft Intune ↗	Set up Microsoft Intune to manage devices in your organization. For full control of corporate devices, you'll use Intune's mobile device management (MDM) features. To manage your organization's data on shared and personal devices, you can use Intune's mobile application management (MAM) features.

Guide - Setup Portal	Guide - Admin Center	Description
		With the Deploy and set up Microsoft Intune guide , you'll set up device and app compliance policies, assign app protection policies, and monitor the device and app protection status.
Microsoft Defender for Endpoint setup guide ↗	Microsoft Defender for Endpoint setup guide ↗	<p>The Microsoft Defender for Endpoint setup guide provides instructions that will help your enterprise network prevent, detect, investigate, and respond to advanced threats. Make an informed assessment of your organization's vulnerability and decide which deployment package and configuration methods are best.</p> <p>NOTE: A Microsoft Volume License is required for Microsoft Defender for Endpoint.</p>
	Exchange Online Protection setup guide ↗	Microsoft Exchange Online Protection (EOP) is a cloud-based email filtering service for protection against spam and malware, with features to safeguard your organization from messaging policy violations. Use the Exchange Online Protection setup guide to set up EOP by selecting which of the three deployment scenarios—on-premises mailboxes, hybrid (mix of on-premises and cloud) mailboxes, or all cloud mailboxes—fits your organization. The guide provides information and resources to set up and review your user's licensing, assign permissions in the Microsoft 365 admin center, and configure your organization's anti-malware and spam policies in the Security & Compliance Center.
Microsoft Defender for Office 365 setup guide ↗	Microsoft Defender for Office 365 setup guide ↗	The Microsoft Defender for Office 365 setup guide safeguards your organization against malicious threats that your environment might come across through email messages, links, and third party collaboration tools. This guide provides you with the resources and information to help you prepare and identify the Defender for Office 365 plan to fit your organization's needs.
Microsoft Defender for Identity setup guide ↗	Microsoft Defender for Identity setup guide ↗	The Microsoft Defender for Identity setup guide provides security solution set-up guidance to identify, detect, and investigate advanced threats that might compromise user identities. These include detecting suspicious user activities and malicious insider actions directed at your organization. You'll create a Defender for Identity instance, connect to your organization's Active Directory, and then set up sensors, alerts,

Guide - Setup Portal ↗	Guide - Admin Center ↗	Description
		notifications, and configure your unique portal preferences.
Microsoft Purview Communication Compliance and Insider Risk Management setup guide ↗	Microsoft Purview Communication Compliance and Insider Risk Management setup guide ↗	<p>The Microsoft Purview Communication Compliance and Insider Risk Management setup guide helps you protect your organization against insider risks that can be challenging to identify and difficult to mitigate. Insider risks occur in a variety of areas and can cause major problems for organizations, ranging from the loss of intellectual property to workplace harassment, and more.</p> <p>The solutions in this guide will help you gain visibility into user activities, actions, and communications with native signals and enrichments from across your organization:</p> <ul style="list-style-type: none"> With the communication compliance solution, you can identify and act on communication risks for items like workplace violence, insider trading, harassment, code of conduct, and regulatory compliance violations. The insider risk management solution helps you identify, investigate, and take action on risks for intellectual property theft, sensitive data leaks, security violations, data spillage, and confidentiality violations.
Microsoft Purview Information Protection setup guide ↗	Microsoft Purview Information Protection setup guide ↗	<p>Get an overview of the capabilities you can apply to your information protection strategy so you can be confident your sensitive information is protected. Use a four-stage lifecycle approach in which you discover, classify, protect, and monitor sensitive information. The Microsoft Purview Information Protection setup guide provides guidance for completing each of these stages.</p>
Microsoft Purview Data Lifecycle Management setup guide ↗	Microsoft Purview Data Lifecycle Management setup guide ↗	<p>The Microsoft Purview Data Lifecycle Management setup guide provides you with the information you'll need to set up and manage your organization's governance strategy, to ensure that your data is classified and managed according to the specific lifecycle guidelines you set. With this guide, you'll learn how to create, auto-apply, or publish retention labels, retention label policies, and retention policies that are applied to your organization's content and compliance records. You'll also get information on importing CSV files with a file plan for bulk scenarios</p>

Guide - Setup Portal	Guide - Admin Center	Description
		or for applying them manually to individual documents.
Microsoft Defender for Cloud Apps setup guide	Microsoft Defender for Cloud Apps setup guide	<p>The Microsoft Defender for Cloud Apps setup guide provides easy to follow deployment and management guidance to set up your Cloud Discovery solution. With Cloud Discovery, you'll integrate your supported security apps, and then you'll use traffic logs to dynamically discover and analyze the cloud apps that your organization uses. You'll also set up features available through the Defender for Cloud Apps solution, including threat detection policies to identify high-risk use, information protection policies to define access, and real-time session controls to monitor activity. With these features, your environment gets enhanced visibility, control over data movement, and analytics to identify and combat cyberthreats across all your Microsoft and third party cloud services.</p>
Microsoft Purview Auditing solutions in Microsoft 365 guide	Microsoft 365 Auditing solutions in Microsoft 365 guide	<p>The Microsoft Purview Auditing solutions in Microsoft 365 guide provides an integrated solution to help organizations effectively respond to security events, forensic investigations, and compliance obligations. When you use the auditing solutions in Microsoft 365, you can search the audit log for activities performed in different Microsoft 365 services.</p>
Microsoft Purview eDiscovery solutions setup guide	Microsoft Purview eDiscovery solutions setup guide	<p>eDiscovery is the process of identifying and delivering electronic information that can be used as evidence in legal cases. The Microsoft Purview eDiscovery solutions setup guide assists in the use of eDiscovery tools in Microsoft Purview that allow you to search for content in Exchange Online, OneDrive for Business, SharePoint Online, Microsoft Teams, Microsoft 365 Groups, and Viva Engage communities.</p>

Guides for collaboration

[\[+\] Expand table](#)

Guide - Setup Portal	Guide - Admin Center	Description
Deploy employee experience with Microsoft Viva	Deploy employee experience with Microsoft Viva	Viva is an integrated, employee experience platform (EXP) that brings together communications, knowledge, learning, resources, and insights into the flow of work and fosters a culture where people and teams thrive and are empowered to be their best from anywhere. You can use the steps and guidance in the guides linked here to deploy one or more Viva apps and achieve better employee engagement throughout your organization.
Enable Microsoft Viva Connections	Enable Microsoft Viva Connections	Encourage meaningful connections while fostering a culture of inclusion and aligning the entire organization around your vision, mission, and strategic priorities.
Enable Microsoft Viva Engage	Enable Microsoft Viva Engage	Bring people together across the organization to connect with leaders, coworkers, and communities; crowdsource answers and ideas; share their work and experience; and find belonging at work.
Enable Microsoft Viva Goals	Enable Microsoft Viva Goals	Align teams with your organization's strategic priorities, driving results and a thriving business.
Enable Microsoft Viva Insights	Enable Microsoft Viva Insights	Viva Insights helps improve productivity and wellbeing through data-driven, privacy-protected insights and recommendations.
Enable Microsoft Viva Learning	Enable Microsoft Viva Learning	Bring enterprise learning into the flow of work by connecting content from your organization, learning management systems, non-Microsoft providers, and Microsoft.
Enable Microsoft Viva Topics	Enable Microsoft Viva Topics	Use AI to automatically organize content and expertise across your systems and teams into related topics, like projects, products, processes, and customers.
Enable Microsoft Viva Amplify	Enable Microsoft Viva Amplify	Centralize campaign management, publishing, and reporting to reach and engage employees.
Enable Microsoft Viva Glint	Enable Microsoft Viva Glint	Improve engagement and performance with recommended actions and data-driven insights across employee lifecycle and organization-wide surveys.
Enable Microsoft Viva Pulse	Enable Microsoft Viva Pulse	Empower managers to seek out and act on confidential feedback using smart templates, research-backed questions and analytics.
Microsoft 365 Apps setup guide	Microsoft 365 Apps setup guide	The Microsoft 365 Apps setup guide provides comprehensive guidance for setting up and deploying the latest versions of Office products like Word, Excel,

Guide - Setup Portal ↗	Guide - Admin Center ↗	Description
		<p>PowerPoint, and OneNote on your users' devices. You'll be walked through the activation process for your Microsoft 365 product key, as well as various deployment methods including easy self-install options and enterprise deployments with management tools. Additionally, the guide offers instructions on assessing your environment, determining your specific deployment requirements, and implementing the necessary support tools to ensure a successful installation.</p>
	Mobile apps setup guide ↗	<p>The Mobile apps setup guide provides instructions for the download and installation of Office apps on your Windows, iOS, and Android mobile devices. This guide provides you with step-by-step information to download and install Microsoft 365 and Office 365 apps on your phone and tablet devices.</p>
Microsoft Teams setup guide ↗	Microsoft Teams setup guide ↗	<p>The Microsoft Teams setup guide provides your organization with guidance to set up team workspaces that host real-time conversations through messaging, calls, and audio or video meetings for both team and private communication. Use the tools in this guide to configure Guest access, set who can create teams, and add team members from a .csv file, all without the need to open a PowerShell session. You'll also get best practices for determining your organization's network requirements and ensuring a successful Teams deployment.</p>
Plan and implement your Microsoft Teams Phone deployment ↗	Plan and implement your Microsoft Teams Phone deployment ↗	<p>This guide will help you transition from your existing voice solution to Microsoft Teams Phone. You'll be guided through discovery and planning phases, or you can go straight to deployment. You'll be able to configure a calling plan, Operator Connect, Teams Phone Mobile, Direct Routing, caller ID, and other features.</p>
Plan and deploy Teams Premium features ↗	Plan and deploy Teams Premium features ↗	<p>Microsoft Teams Premium helps make every meeting more intelligent, engaging, and protected. This guide will help you to plan for and deploy one or more Teams Premium features and take advantage of your Teams Premium licenses.</p>
SharePoint setup guide ↗	SharePoint setup guide ↗	<p>The SharePoint setup guide helps you set up your SharePoint document storage and content management, create sites, configure external sharing, migrate data and configure advanced settings, and drive user engagement and communication within your organization. You'll follow steps for configuring your content-sharing</p>

Guide - Setup Portal	Guide - Admin Center	Description
		permission policies, choose your migration sync tools, and enable the security settings for your SharePoint environment.
Surface Hub and Microsoft Teams Rooms setup guide ↗	Surface Hub and Microsoft Teams Rooms setup guide ↗	The Surface Hub and Microsoft Teams Rooms setup guide will customize your experience based on your environment. If you're hosted in Exchange Online and using Microsoft Teams, the guide will automatically create your device account with the correct settings.
OneDrive setup guide ↗	OneDrive setup guide ↗	Use the OneDrive setup guide to get started with OneDrive file storage, sharing, collaboration, and syncing capabilities. OneDrive provides a central location where users can sync their Microsoft 365 Apps files, configure external sharing, migrate user data, and configure advanced security and device access settings. The OneDrive setup guide can be deployed using a OneDrive subscription or a standalone OneDrive plan.
Viva Engage deployment advisor ↗	Viva Engage deployment advisor ↗	Connect and engage across your organization with Viva Engage. The Viva Engage deployment advisor prepares your Viva Engage network by adding domains, defining admins, and combining Viva Engage networks. You'll get guidance to deploy Viva Engage and then customize the look, configure security and compliance, and refine the settings.

Advanced guides

[+] Expand table

Guide - Setup Portal	Guide - Admin Center	Description
In-place upgrade with Configuration Manager guide ↗		Use the In-place upgrade with Configuration Manager guide when upgrading Windows 7 and Windows 8.1 devices to the latest version of Windows 10. You'll use the script provided to check the prerequisites and automatically configure an in-place upgrade.
Deploy Office to your users guide ↗		Deploy Office apps from the cloud with the ability to customize your installation by using the Office Deployment Tool. The Deploy Office to your users guide helps you create a customized Office configuration with advanced settings, or you can use a pre-built recommended configuration.

Guide - Setup Portal ↗ Center ↗	Guide - Admin Admin Center ↗	Description
		Whether your users are conducting a self-install or you're deploying to your users individually or in bulk, this advanced guide provides you with step-by-step instructions to give users an Office installation tailored to your organization.
Deploy Office to remote users guide ↗		<p>Now that working remotely is the norm, users need to receive your organization's Office settings when they're not connected to your internal network or when using their own devices.</p> <p>Use the Deploy Office to remote users guide to create a customized Office installation and then send users a generated PowerShell script that will seamlessly install Office with your configuration.</p>
Deploy and update Microsoft 365 Apps with Configuration Manager advisor ↗		<p>For organizations using Configuration Manager, you can use the Deploy and update Microsoft 365 Apps with Configuration Manager advisor to generate a script that will automatically configure your Microsoft 365 Apps deployment using best practices recommended by FastTrack engineers. Use this guide to build your deployment groups, customize your Office apps and features, configure dynamic or lean installations, and then run the script to create the applications, automatic deployment rules, and device collections you need to target your deployment.</p>
Intune Configuration Manager co-management setup guide ↗		<p>Use the Intune Configuration Manager co-management setup guide to set up existing Configuration Manager client devices and new internet-based devices that your org wants to co-manage with both Microsoft Intune and Configuration Manager. Co-management allows you to manage Windows 10 devices and adds new functionality to your org's devices, while receiving the benefits of both solutions.</p>
SDS Rollover setup guide ↗		<p>The SDS Rollover setup guide provides the steps to help your organization sync student information data to Microsoft Entra ID and Office 365. This guide streamlines the term lifecycle management process by creating Office 365 Groups for Exchange Online and SharePoint Online, class teams for Microsoft Teams and OneNote, as well as Intune for Education, and rostering and single sign-on integration for third-party apps. You'll perform end-of-year closeout, tenant cleanup and archive, new school year preparation, and new school year launch. Then you can create new profiles using the sync deployment method that suits your organization.</p>
Windows 365	Windows 365 Enterprise	<p>The Windows 365 Enterprise deployment checklist provides customers with information for provisioning and hosting Cloud PCs. With the deployment checklist, you can determine</p>

Guide - Setup Portal	Guide - Admin Center	Description
Enterprise checklist ↗	deployment checklist ↗	if Microsoft Entra join, Azure virtual network, or Microsoft-hosted networks path fits your organization. You can review resources that will assist with the required configuration for deployment features, health checks, updates, and maintenance for image configuration.

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Integrated apps and Microsoft Entra ID for Microsoft 365 administrators

Article • 02/14/2024

There's more to managing integrated apps than just [managing user consent to apps](#). With the advent of the Microsoft 365 REST APIs, users can grant apps access to their Microsoft 365 data, such as mail, calendars, contacts, users, groups, files, and folders. By default, users need to individually grant permissions to each app.

But this doesn't scale well if you want to authorize an app once at the **Microsoft Entra DC admin**, or **Global admin** level and roll it out to your whole organization through the app launcher. To do this, you must register the app in Microsoft Entra ID. There are some steps you need to take before you can register an app in Microsoft Entra ID and some background information you should know that can help you manage apps in your Microsoft 365 organization.

Microsoft Entra resources for Microsoft 365 admins

You have to do these two tasks before you can manage your Microsoft 365 apps in Microsoft Entra ID.

[] [Expand table](#)

Prerequisites	Comments
Use your free Microsoft Entra subscription	Every paid subscription to Microsoft 365 comes with a free subscription to Microsoft Entra ID. You can use Microsoft Entra ID to manage your apps and to create and manage user and group accounts. To use Microsoft Entra ID, just go to the Azure portal at https://portal.azure.com and sign in using your Microsoft 365 account.
Manage user consent to apps	You must manage user consent to apps to allow third-party apps to access user Microsoft 365 information and for you to register apps in Microsoft Entra ID. For example, when someone uses a third-party app, that app might ask for permission to access their calendar and to edit files that are in a OneDrive folder.

Managing Microsoft 365 apps requires you to have knowledge of apps in Microsoft Entra ID. Use these articles to give you the background you need.

Article	Comments
Meet the Microsoft 365 app launcher	If you're new to the app launcher, you might be wondering what it is and how to use it. The app launcher is designed to help you get to your apps from anywhere in Microsoft 365.
Office 365 management APIs overview	The Microsoft 365 management APIs let you provide access to your Microsoft 365 data, including the things they care about most—their mail, calendars, contacts, users and groups, files, and folders.
Integrating applications in Microsoft Entra ID	Learn about applications that are integrated with Microsoft Entra ID, and how to register your application, understand concepts behind a registered application, and learn about branding guidelines for multi-tenant applications.
Add custom tiles to the app launcher	The app launcher in Microsoft 365 makes it easier for users to find and access their apps. This article describes the ways you as a developer can get your apps to appear in users' app launchers and also give them a single sign-on (SSO) experience using their Microsoft 365 credentials.
Microsoft Entra integration tutorials	The objective of these tutorials is to show you how to configure Microsoft Entra SSO for third-party SaaS applications.
Authentication scenarios for Microsoft Entra ID	Microsoft Entra ID simplifies authentication for developers by providing identity as a service, with support for industry-standard protocols such as OAuth 2.0 and OpenID Connect, as well as open source libraries for different platforms to help you quickly start coding. This document helps you understand the various scenarios Microsoft Entra ID supports and shows you how to get started.
Application access	Microsoft Entra ID enables easy integration to many of today's popular software as a service (SaaS) applications. It provides identity and access management, and it delivers an Access Panel for users where they can discover what application access they have and where they can use SSO to access their applications. This article provides you with links to the related resources that enable you to learn more about the application access enhancements for Microsoft Entra ID and how you can contribute to them.
Personalize your Office 365 experience	You can get quick access to the apps you use every day by adding or removing apps in the Microsoft 365 app launcher.

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Microsoft 365 integration with on-premises environments

Article • 12/19/2023

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

You can integrate Microsoft 365 with your existing on-premises Active Directory Domain Services (AD DS) and with on-premises installations of Exchange Server, Skype for Business Server 2015, or SharePoint Server.

- When you integrate AD DS, you can synchronize and manage user accounts for both environments. You can also add *password hash synchronization* (PHS) or *single sign-on* (SSO) so users can sign in both environments with their on-premises credentials.
- When you integrate with on-premises server products, you create a hybrid environment. A hybrid environment can help as you migrate users or information to Microsoft 365, or you can continue to have some users or some information on-premises and some in the cloud. For more information about hybrid environments, see [hybrid cloud](#).

You can also use the Microsoft Entra advisors for customized setup guidance in the Microsoft 365 admin center (you must be signed in to Microsoft 365):

- [Microsoft Entra setup guide ↗](#)
- [Sync users from your org's directory ↗](#)
- [Active Directory Federation Services \(AD FS\) deployment advisor ↗](#)

Before you begin

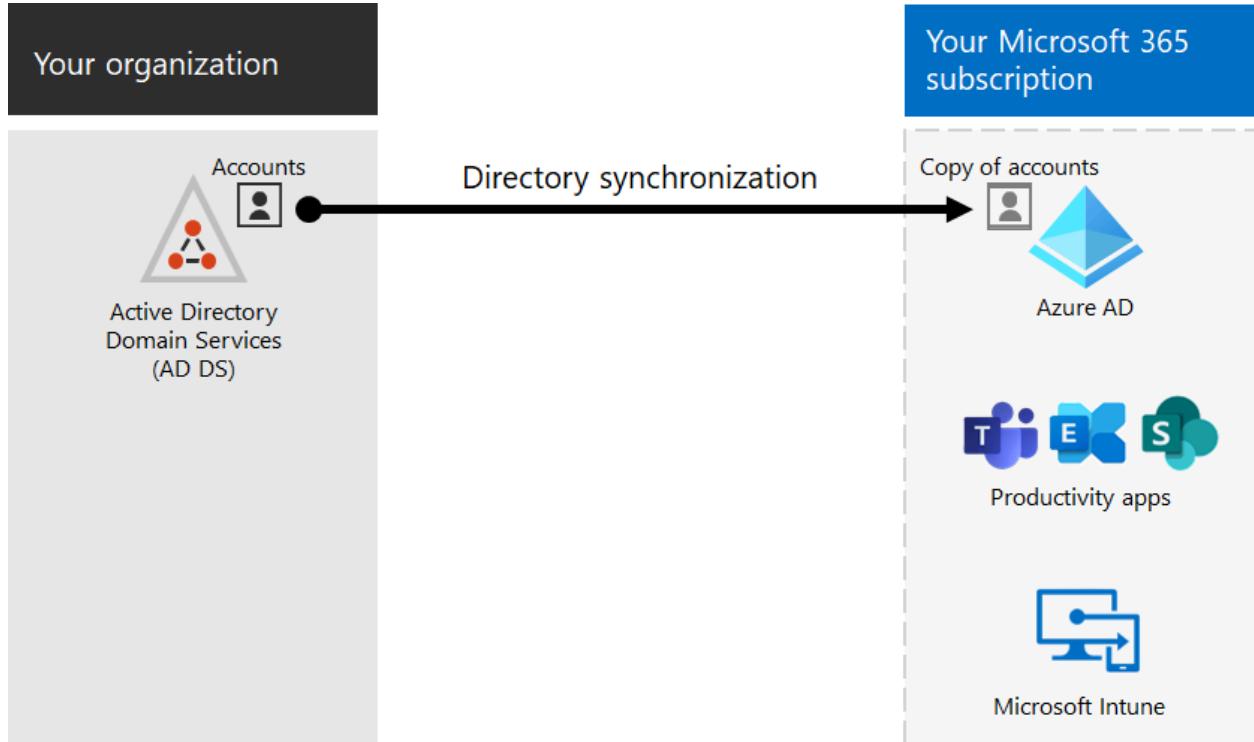
Before you integrate Microsoft 365 and an on-premises environment, you also need to do [network planning and performance tuning](#). You want to understand the available identity models.

See [manage Microsoft 365 accounts](#) for a list of tools you can use to manage Microsoft 365 user accounts.

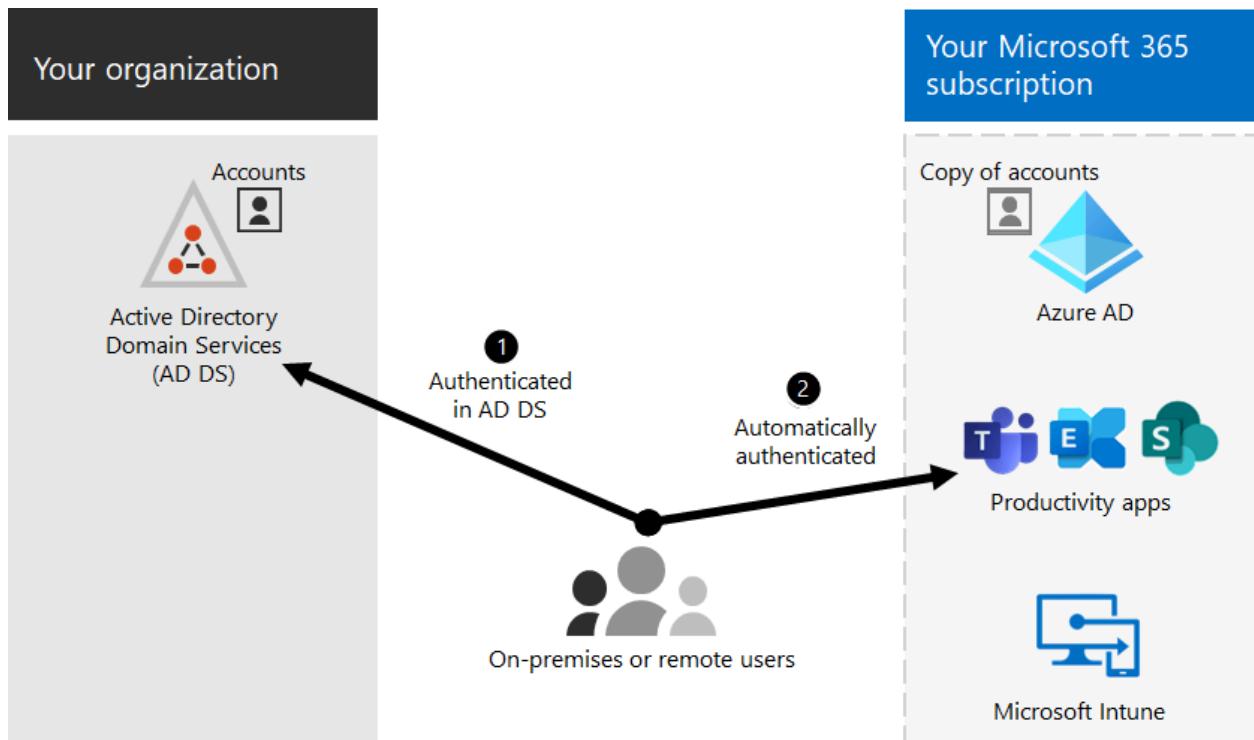
Integrate Microsoft 365 with AD DS

If you have existing user accounts in AD DS, you don't want to re-create all of those accounts in Microsoft 365 and risk introducing differences or errors between the

environments. Directory synchronization helps you mirror those accounts between your on-premises and online environments. With directory synchronization, your users don't have to remember new information for each environment, and you don't have to create or update accounts twice. You need to [prepare your on-premises directory](#) for directory synchronization.



If you want users to be able to sign in to Microsoft 365 with their on-premises credentials, you can also configure SSO. With SSO, Microsoft 365 is configured to trust the on-premises environment for user authentication.



Directory synchronization with or without password hash synchronization or pass-through authentication (PTA)

A user signs in to their on-premises environment with their user account (domain\username). When they go to Microsoft 365, they must sign in again with their work or school account (user@domain.com). The user name is the same in both environments. When you add PHS or PTA, the user has the same password for both environments. The user has to provide those credentials again when logging on to Microsoft 365. Directory synchronization with PHS is the most commonly used directory synchronization.

To set up directory synchronization, use Microsoft Entra Connect. For instructions, see [Set up directory synchronization for Microsoft 365](#) and [Microsoft Entra Connect with express settings](#).

Learn more about [preparing for directory synchronization to Microsoft 365](#).

Directory synchronization with SSO

A user signs in to their on-premises environment with their user account. When they go to Microsoft 365, they're either logged on automatically, or they sign in using the same credentials they use for their on-premises environment (domain\username).

To set up SSO, you also use Microsoft Entra Connect. For instructions, see [Custom installation of Microsoft Entra Connect](#).

For more information, see [single sign-on](#).

Microsoft Entra Connect

Microsoft Entra Connect replaces older versions of identity integration tools such as DirSync and Azure AD Sync. If you want to update from Azure Active Directory Sync to Microsoft Entra Connect, see [the upgrade instructions](#).

See also

[Microsoft 365 Enterprise overview](#)

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Azure integration with Microsoft 365

Article • 12/28/2023

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Microsoft 365 uses Microsoft Entra ID to manage user identities behind the scenes. Your Microsoft 365 subscription includes a free Microsoft Entra subscription. You can integrate your on-premises Active Directory Domain Services (AD DS) to synchronize user accounts and passwords or set up single sign-on. You can also purchase advanced features to better manage your accounts.

Microsoft Entra ID also offers other functionality, like managing integrated apps, that you can use to extend and customize your Microsoft 365 subscriptions.

You can use the Microsoft Entra deployment advisors for a guided setup and configuration experience in the Microsoft 365 admin center (you must be signed in to Microsoft 365):

- [Microsoft Entra Connect advisor ↗](#)
- [AD FS deployment advisor ↗](#)
- [Microsoft Entra setup guide ↗](#)

Microsoft Entra editions and Microsoft 365 identity management

If you have a paid subscription to Microsoft 365, you also have a free Microsoft Entra subscription. You can use Microsoft Entra ID to create and manage user and group accounts. To activate this subscription, you have to complete a one-time registration. Afterward, you can access Microsoft Entra ID from your Microsoft 365 admin center.

For instructions to register your free Microsoft Entra subscription, see [use your free Microsoft Entra subscription](#). Don't go directly to azure.microsoft.com to sign up because you'll get a trial or paid subscription to Microsoft Azure that is separate from your free Microsoft Entra subscription with Microsoft 365.

With the free subscription you can synchronize with on-premises directories, set up single sign-on, and synchronize with many SaaS applications, such as Salesforce, DropBox, and many more.

If you want enhanced AD DS functionality, bi-directional synchronization, and other management capabilities, you can upgrade your free subscription to a paid premium

subscription. For the details, see [Microsoft Entra editions](#).

For more information about Microsoft 365 and Microsoft Entra ID, see [Microsoft 365 identity models](#).

Extend the capabilities of your Microsoft 365 tenant

[] [Expand table](#)

Feature	Description
Integrated apps	<p>You can grant individual apps access to your Microsoft 365 data, such as mail, calendars, contacts, users, groups, files, and folders. You can also authorize these apps at the Microsoft Entra DC admin level and make them available to your entire company by registering the apps in Microsoft Entra ID. For more information, see Integrated Apps and Microsoft Entra ID for Microsoft 365 administrators. For more information, see About admin roles. Also see Single sign-on.</p>
Power Apps	<p>Power Apps are focused apps for mobile devices that can connect to your existing data sources like SharePoint lists and other data apps. See Create a Power App for a list in SharePoint Online and the Power Apps page for details.</p>

See also

[Microsoft 365 Enterprise overview](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Hybrid modern authentication overview and prerequisites for using it with on-premises Skype for Business and Exchange servers

Article • 12/19/2023

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Modern Authentication is a method of identity management that offers more secure user authentication and authorization. It's available for Office 365 hybrid deployments of Skype for Business server on-premises and Exchange server on-premises, and split-domain Skype for Business hybrids. This article links to related docs about prerequisites, setup/disabling modern authentication, and to some of the related client (ex. Outlook and Skype clients) information.

- [What is modern authentication?](#)
- [What changes when I use modern authentication?](#)
- [Check the modern authentication status of your on-premises environment](#)
- [Do you meet modern authentication prerequisites?](#)
- [What else do I need to know before I begin?](#)

What is modern authentication?

Modern authentication is an umbrella term for a combination of authentication and authorization methods between a client (for example, your laptop or your phone) and a server, as well as some security measures that rely on access policies that you might already be familiar with. It includes:

- **Authentication methods:** Multifactor authentication (MFA); smart card authentication; client certificate-based authentication
- **Authorization methods:** Microsoft's implementation of Open Authorization (OAuth)
- **Conditional access policies:** Mobile Application Management (MAM) and Microsoft Entra Conditional Access

Managing user identities with modern authentication gives administrators many different tools to use when it comes to securing resources and offers more secure methods of identity management to both on-premises (Exchange and Skype for Business), Exchange hybrid, and Skype for Business hybrid/split-domain scenarios.

Because Skype for Business works closely with Exchange, the sign in behavior Skype for Business client users will be affected by the modern authentication status of Exchange. It's also applicable if you have a Skype for Business *split-domain* hybrid architecture, in which you have both Skype for Business Online and Skype for Business on-premises, with users homed in both locations.

For more information about modern authentication in Office 365, see [Office 365 Client App Support - Multi-factor authentication](#).

Important

As of August of 2017, all new Office 365 tenants that include Skype for Business online and Exchange online will have modern authentication enabled by default. Pre-existing tenants won't have a change in their default MA state, but all new tenants automatically support the expanded set of identity features you see listed previously. To check your MA status, see the [Check the modern authentication status of your on-premises environment](#) section.

What changes when I use modern authentication?

When using modern authentication with on-premises Skype for Business or Exchange server, you're still *authenticating* users on-premises, but the story of *authorizing* their access to resources (like files or emails) changes. This is why, though modern authentication is about client and server communication, the steps taken during configuring MA result in evoSTS (a Security Token Service used by Microsoft Entra ID) being set as Auth Server for Skype for Business and Exchange server on-premises.

The change to evoSTS allows your on-premises servers to take advantage of OAuth (token issuance) for authorizing your clients, and also lets your on-premises use security methods common in the cloud (like Multi-factor Authentication). Additionally, the evoSTS issues tokens that allow users to request access to resources without supplying their password as part of the request. No matter where your users are homed (of online or on-premises), and no matter which location hosts the needed resource, EvoSTS would become the core of authorizing users and clients once modern authentication is configured.

For example, if a Skype for Business client needs to access Exchange server to get calendar information on behalf of a user, it uses the Microsoft Authentication Library (MSAL) to do so. MSAL is a code library designed to make secured resources in your

directory available to client applications using OAuth security tokens. MSAL works with OAuth to verify claims and to exchange tokens (rather than passwords), to grant a user access to a resource. In the past, the authority in a transaction like this one--the server that knows how to validate user claims and issue the needed tokens--might have been a Security Token Service on-premises, or even Active Directory Federation Services. However, modern authentication centralizes that authority by using Microsoft Entra ID.

This also means that even though your Exchange server and Skype for Business environments might be entirely on-premises, the authorizing server is online, and your on-premises environment must have the ability to create and maintain a connection to your Office 365 subscription in the Cloud (and the Microsoft Entra instance that your subscription uses as its directory).

What doesn't change? Whether you're in a split-domain hybrid or using Skype for Business and Exchange server on-premises, all users must first authenticate *on-premises*. In a hybrid implementation of modern authentication, *LyncDiscovery* and *Autodiscovery* both point to your on-premises server.

 **Important**

If you need to know the specific Skype for Business topologies supported with MA, that's [documented right here](#).

Check the modern authentication status of your on-premises environment

Because modern authentication changes the authorization server used when services apply OAuth/S2S, you need to know if modern authentication is enabled or disabled for your on-premises Skype for Business and Exchange environments. You can check the status on your Exchange servers by running the following PowerShell command:

PowerShell

```
Get-OrganizationConfig | ft OAuth*
```

If the value of the *OAuth2ClientProfileEnabled* property is **False**, then modern authentication is disabled.

For more information about the `Get-OrganizationConfig` cmdlet, see [Get-OrganizationConfig](#).

You can check your Skype for Business servers by running the following PowerShell command:

```
PowerShell
```

```
Get-CsOAuthConfiguration
```

If the command returns an empty *OAuthServers* property, or if the value of the *ClientADALAuthOverride* property isn't **Allowed**, then modern authentication is disabled.

For more information about the `Get-CsOAuthConfiguration` cmdlet, see [Get-CsOAuthConfiguration](#).

Do you meet modern authentication prerequisites?

Verify and check these items off your list before you continue:

- **Skype for Business specific**
 - All servers must have May 2017 cumulative update (CU5) for Skype for Business Server 2015 or later
 - **Exception** - Survivability Branch Appliance (SBA) can be on the current version (based on Lync 2013)
 - Your SIP domain is added as a Federated domain in Office 365
 - All SFB Front Ends must have connections outbound to the internet, to Office 365 Authentication URLs (TCP 443) and well-known certificate root CRLs (TCP 80) listed in Rows 56 and 125 of the 'Microsoft 365 Common and Office' section of [Office 365 URLs and IP address ranges](#).
- **Skype for Business on-premises in a hybrid Office 365 environment**
 - A Skype for Business Server 2019 deployment with all servers running Skype for Business Server 2019.
 - A Skype for Business Server 2015 deployment with all servers running Skype for Business Server 2015.
 - A deployment with a maximum of two different server versions as listed below:
 - Skype for Business Server 2015
 - Skype for Business Server 2019
 - All Skype for Business servers must have the latest cumulative updates installed, see [Skype for Business Server updates](#) to find and manage all available updates.
 - There's no Lync Server 2010 or 2013 in the hybrid environment.

Note

If your Skype for Business front-end servers use a proxy server for Internet access, the proxy server IP and Port number used must be entered in the configuration section of the web.config file for each front end.

- C:\Program Files\Skype for Business Server 2015\Web Components\Web ticket\int\web.config
- C:\Program Files\Skype for Business Server 2015\Web Components\Web ticket\ext\web.config

XML

```
<configuration>
  <system.net>
    <defaultProxy>
      <proxy
        proxyaddress="https://192.168.100.60:8080"
        bypassonlocal="true" />
    </defaultProxy>
  </system.net>
</configuration>
```

Important

Be sure to subscribe to the RSS feed for [Office 365 URLs and IP address ranges](#) to stay current with the latest listings of required URLs.

- **Exchange Server specific**
 - You're using either Exchange server 2013 CU19 and up, Exchange server 2016 CU8 and up, or Exchange Server 2019 CU1 and up.
 - There's no Exchange server 2010 in the environment.
 - SSL Offloading is not configured. SSL termination and re-encryption are supported.
 - In the event your environment utilizes a proxy server infrastructure to allow servers to connect to the Internet, be sure all Exchange servers have the proxy server defined in the [InternetWebProxy](#) property.
- **Exchange Server on-premises in a hybrid Office 365 environment**
 - If you're using Exchange Server 2013, at least one server must have the Mailbox and Client Access server roles installed. While it's possible to install the Mailbox and Client Access roles on separate servers, we strongly recommend that you

install both roles on the same server to provide more reliability and improved performance.

- If you're using Exchange server 2016 or later version, at least one server must have the Mailbox server role installed.
- There's no Exchange server 2007 or 2010 in the Hybrid environment.
- All Exchange servers must have the latest cumulative updates installed. See [Upgrade Exchange to the latest Cumulative Updates](#) to find and manage all available updates.

- **Exchange client and protocol requirements**

The availability of modern authentication is determined by the combination of the client, protocol, and configuration. If modern authentication isn't supported by the client, protocol, and/or configuration, then the client continues to use legacy authentication.

The following clients and protocols support modern authentication with on-premises Exchange when modern authentication is enabled in the environment:

[+] [Expand table](#)

Clients	Primary Protocol	Notes
Outlook 2013 and later	MAPI over HTTP	MAPI over HTTP must be enabled within Exchange in order to use modern authentication with these clients (enabled or True for new installs of Exchange 2013 Service Pack 1 and above); for more information, see How modern authentication works for Office 2013 and Office 2016 client apps . Ensure you're running the minimum required build of Outlook; see Latest updates for versions of Outlook that use Windows Installer (MSI) .
Outlook 2016 for Mac and later	Exchange Web Services	
Outlook for iOS and Android	Microsoft sync technology	See Using hybrid Modern Authentication with Outlook for iOS and Android for more information.
Exchange ActiveSync clients (for example, iOS11 Mail)	Exchange ActiveSync	For Exchange ActiveSync clients that support modern authentication, you must recreate the profile in order to switch from basic authentication to modern authentication.

Clients and/or protocols that aren't listed (for example, POP3) don't support modern authentication with on-premises Exchange and continue to use legacy authentication mechanisms even after modern authentication is enabled in the environment.

- **General prerequisites**

- Resource forest scenarios require a two-way trust with the account forest to ensure proper SID lookups are performed during hybrid modern authentication requests.
- If you use AD FS, you should have Windows 2012 R2 AD FS 3.0 and above for federation.
- Your identity configurations are any of the types supported by Microsoft Entra Connect, such as password hash sync, pass-through authentication, and on-premises STS supported by Office 365.
- You have Microsoft Entra Connect configured and functioning for user replication and sync.

 **Note**

Any user accounts that are not synchronized to Microsoft Entra Identity won't be provided an authorization token via Hybrid Modern Authentication. Once the on-premises application is configured to use evoSTS as the default authorization endpoint, these user accounts that aren't synchronized will encounter issues with their access to the application if appropriate configuration isn't available.

- You have verified that hybrid is configured using Exchange Classic Hybrid Topology mode between your on-premises and Office 365 environment. Official support statement for Exchange hybrid says you must have either current CU or current CU - 1.

 **Note**

Hybrid modern authentication is not supported with the [Hybrid Agent](#).

- Make sure both an on-premises test user, and a hybrid test user homed in Office 365, can sign in to the Skype for Business desktop client (if you want to

use modern authentication with Skype) and Microsoft Outlook (if you want to use modern authentication with Exchange).

- Make sure the SignInOptions setting in Microsoft Office isn't configured to its most restrictive setting. For more information, see [How to allow Office to connect to the internet](#).

What else do I need to know before I begin?

- All the scenarios for on-premises servers involve setting up modern authentication on-premises (in fact, for Skype for Business there's a list of supported topologies) so that the server responsible for authentication and authorization is in the Microsoft Cloud (Microsoft Entra ID's security token service, called 'evoSTS'), and updating Microsoft Entra ID about the URLs or namespaces used by your on-premises installation of either Skype for Business or Exchange. Therefore, on-premises servers take on a Microsoft Cloud dependency. Taking this action could be considered configuring 'hybrid auth'.
- This article links out to others that help you choose supported modern authentication topologies (necessary only for Skype for Business), and how-to articles that outline the setup steps, or steps to disable modern authentication, for Exchange on-premises and Skype for Business on-premises. Favorite this page in your browser if you're going to need a home-base for using modern authentication in your server environment.

Related Topics

- [How to configure Exchange Server on-premises to use Modern Authentication](#)
- [Skype for Business topologies supported with Modern Authentication](#)
- [Removing or disabling Hybrid Modern Authentication from Skype for Business and Exchange](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

How to configure Exchange Server on-premises to use Hybrid Modern Authentication

Article • 06/17/2024

Overview

Hybrid Modern Authentication (HMA) in Microsoft Exchange Server is a feature that allows users to access mailboxes, which are hosted on-premises, by using authorization tokens obtained from the cloud.

HMA enables Outlook to obtain Access and Refresh OAuth tokens from Microsoft Entra ID, either directly for password hash sync or Pass-Through Auth identities, or from their own Secure Token Service (STS) for federated identities. Exchange on-premises accepts these tokens and provide mailbox access. The method of obtaining these tokens and the credentials required are determined by the capabilities of the identity provider (iDP), which could range from simple username and password to more complex methods such as certificates, phone auth, or biometric methods.

For HMA to work, the user's identity must be present in Microsoft Entra ID, and some configuration is required, which is handled by the Exchange Hybrid Configuration Wizard (HCW).

In comparison to legacy authentication methods such as NTLM, HMA offers several advantages. It provides a more secure and flexible authentication method, leveraging the power of cloud-based authentication. Unlike NTLM, which relies on a challenge-response mechanism and doesn't support modern authentication protocols, HMA uses OAuth tokens, which are more secure and offer better interoperability.

HMA is a powerful feature that enhances the flexibility and security of accessing on-premises applications, leveraging the power of cloud-based authentication. It represents a significant improvement over legacy authentication methods, offering enhanced security, flexibility, and user convenience.

Steps to follow to configure and enable Hybrid Modern Auth

To enable Hybrid Modern Authentication (HMA), you must ensure that your organization meets all necessary prerequisites. Additionally, you should confirm that your Office client is compatible with Modern Authentication. For more details, refer to the documentation on [How modern authentication works for Office 2013 and Office 2016 client apps](#).

1. Make sure you [meet the prerequisites](#) before you begin.
2. [Add on-premises web service URLs to Microsoft Entra ID](#). The URLs must be added as `Service Principal Names (SPNs)`. In case that your Exchange Server setup is in hybrid with **multiple tenants**, these on-premises web service URLs must be added as SPNs in the Microsoft Entra ID of all the tenants, which are in hybrid with Exchange Server on-premises.
3. [Ensure that all virtual directories are enabled for HMA](#). If you want to configure [Hybrid Modern Authentication for Outlook on the Web \(OWA\) and Exchange Control Panel \(ECP\)](#), it's important to also verify the respective directories.
4. [Check for the EvoSTS Auth Server object](#).
5. Ensure that the [Exchange Server OAuth certificate](#) is valid. The [MonitorExchangeAuthCertificate script](#) script can be utilized to verify the validity of the OAuth certificate. In the event of its expiration, the script assists in the renewal process.
6. Ensure that all user identities are synchronized with Microsoft Entra ID, especially all accounts, which are used for administration. Otherwise, the login stops working until they're synchronized. Accounts, such as the built-in Administrator, will never be synchronized with Microsoft Entra ID and, therefore, can't be used on any OAuth login once HMA has been enabled. This behavior is due to the `isCriticalSystemObject` attribute, which is set to `True` for some accounts including the default administrator.
7. (Optional) If you want to use the Outlook for iOS and Android client, make sure to [allow the AutoDetect service to connect to your Exchange Server](#).
8. [Enable HMA in Exchange on-premises](#).

Prerequisites to enable Hybrid Modern Auth

In this section, we provide information and steps that need to be done to successfully configure and enable Hybrid Modern Auth in Microsoft Exchange Server.

Exchange Server specific prerequisites

Your Exchange servers must fulfill the following requirements before Hybrid Modern Authentication can be configured and enabled. In case you have a hybrid configuration, you must run the latest Cumulative Update (CU) to be in a supported state. You can find the supported Exchange Server versions and build in the [Exchange Server supportability matrix](#).

- Make sure that there are no end-of-life Exchange servers in the organization.
- Exchange Server 2016 must be running CU8 or later.
- Exchange Server 2019 must be running CU1 or later.
- Make sure that all servers can connect to the internet. If a proxy is required, [configure Exchange Server to use it](#).
- If you already have a hybrid configuration, make sure it's a classic hybrid deployment as modern hybrid doesn't support HMA.
- Make sure that SSL Offloading is not used (it's unsupported). SSL Bridging, however, can be used and is supported.

More information can also be found in the [Hybrid Modern Authentication overview and prerequisites for using it with on-premises Skype for Business and Exchange servers documentation](#).

Protocols that work with Hybrid Modern Auth

Hybrid Modern Authentication works for the following Exchange Server protocols:

[] [Expand table](#)

Protocol	Hybrid Modern Auth Supported
MAPI over HTTP (MAPI/HTTP)	Yes
Outlook Anywhere (RPC/HTTP)	No
Exchange Active Sync (EAS)	Yes
Exchange Web Services (EWS)	Yes
Outlook on the Web (OWA)	Yes
Exchange Admin Center (ECP)	Yes
Offline Address Book (OAB)	Yes
IMAP	No

Protocol	Hybrid Modern Auth Supported
POP	No

Add on-premises web service URLs as SPNs in Microsoft Entra ID

Run the commands that assign your on-premises web service URLs as Microsoft Entra SPNs. SPNs are used by client machines and devices during authentication and authorization. All the URLs that might be used to connect from on-premises to Microsoft Entra ID must be registered in Microsoft Entra ID (including both internal and external namespaces).

1. First, run the following commands on your Microsoft Exchange Server:

PowerShell

```
Get-MapiVirtualDirectory -ADPropertiesOnly | fl server,*url*
Get-WebServicesVirtualDirectory -ADPropertiesOnly | fl server,*url*
Get-ClientAccessService | fl Name, AutodiscoverServiceInternalUri
Get-OABVirtualDirectory -ADPropertiesOnly | fl server,*url*
Get-AutodiscoverVirtualDirectory -ADPropertiesOnly | fl server,*url*
Get-ActiveSyncVirtualDirectory -ADPropertiesOnly | fl server,*url*
```

Ensure the URLs clients might connect to are listed as HTTPS service principal names in Microsoft Entra ID. In case Exchange on-premises is in hybrid with **multiple tenants**, these HTTPS SPNs should be added in the Microsoft Entra ID of all the tenants in hybrid with Exchange on-premises.

2. Install the Microsoft Graph PowerShell module:

PowerShell

```
Install-Module Microsoft.Graph -Scope AllUsers
```

3. Next, connect to Microsoft Entra ID by following [these instructions](#). To consent to the required permissions, run the following command:

PowerShell

```
Connect-MgGraph -Scopes Application.Read.All, Application.ReadWrite.All
```

4. For your Exchange-related URLs, type the following command:

PowerShell

```
Get-MgServicePrincipal -Filter "AppId eq '00000002-0000-0ff1-ce00-000000000000'" | select -ExpandProperty ServicePrincipalNames
```

Note down the output of this command, which should include an `https://autodiscover.yourdomain.com` and `https://mail.yourdomain.com` URL, but mostly consist of SPNs that begin with `00000002-0000-0ff1-ce00-000000000000/`. If there are `https://` URLs from your on-premises that are missing, those specific records should be added to this list.

5. If you don't see your internal and external `MAPI/HTTP`, `EWS`, `ActiveSync`, `OAB`, and `AutoDiscover` records in this list, you must add them. Use the following command to add all URLs that are missing. In our example, the URLs that are added are `mail.corp.contoso.com` and `owa.contoso.com`. Make sure that they're replaced by the URLs that are configured in your environment.

PowerShell

```
$x = Get-MgServicePrincipal -Filter "AppId eq '00000002-0000-0ff1-ce00-000000000000'"
$x.ServicePrincipalNames += "https://mail.corp.contoso.com/"
$x.ServicePrincipalNames += "https://owa.contoso.com/"
Update-MgServicePrincipal -ServicePrincipalId $x.Id -
ServicePrincipalNames $x.ServicePrincipalNames
```

6. Verify that your new records were added by running the `Get-MgServicePrincipal` command from step 4 again, and validate the output. Compare the list from before to the new list of SPNs. You might also note down the new list for your records. If you're successful, you should see the two new URLs in the list. Going by our example, the list of SPNs now includes the specific URLs `https://mail.corp.contoso.com` and `https://owa.contoso.com`.

Verify virtual directories are properly configured

Now verify OAuth is properly enabled in Exchange on all of the virtual directories Outlook might use by running the following commands:

PowerShell

```
Get-MapiVirtualDirectory | fl server,*url*,*auth*
Get-WebServicesVirtualDirectory | fl server,*url*,*oauth*
Get-OABVirtualDirectory | fl server,*url*,*oauth*
Get-AutoDiscoverVirtualDirectory | fl server,*oauth*
Get-ActiveSyncVirtualDirectory | fl server,*url*,*auth*
```

Check the output to make sure `OAuth` is enabled for each of these virtual directories, it looks something like this (and the key thing to look at is `OAuth` as mentioned before):

PowerShell

```
Get-MapiVirtualDirectory | fl server,*url*,*auth*

Server : EX1
InternalUrl : https://mail.contoso.com/mapi
ExternalUrl : https://mail.contoso.com/mapi
IISAuthenticationMethods : {Ntlm, OAuth, Negotiate}
InternalAuthenticationMethods : {Ntlm, OAuth, Negotiate}
ExternalAuthenticationMethods : {Ntlm, OAuth, Negotiate}
```

If OAuth is missing from any server and any of the five virtual directories, you need to add it by using the relevant commands before proceeding ([Set-MapiVirtualDirectory](#), [Set-WebServicesVirtualDirectory](#), [Set-OABVirtualDirectory](#), [Set-AutodiscoverVirtualDirectory](#), and [Set-ActiveSyncVirtualDirectory](#)).

Confirm the EvoSTS Auth Server Object is Present

Now on the Exchange Server on-premises Management Shell (EMS) run this last command. You can validate that your Exchange Server on-premises returns an entry for the evoSTS authentication provider:

PowerShell

```
Get-AuthServer | where {$_.Name -like "EvoSts*"} | ft name(enabled)
```

Your output should show an AuthServer of the Name `EvoSts - <GUID>` and the `Enabled` state should be `True`. If that's not the case, you should download and run the most recent version of the [Hybrid Configuration Wizard](#).

In case that Exchange Server on-premises runs a hybrid configuration with **multiple tenants**, your output shows one AuthServer with the Name `EvoSts - <GUID>` for each

tenant in hybrid with Exchange Server on-premises and the `Enabled` state should be `True` for all of these AuthServer objects. Please make a note of the identifier `EvoSTS - <GUID>`, as it will be required in the subsequent step.

Enable HMA

Run the following commands in the Exchange Server on-premises Management Shell (EMS) and replace the `<GUID>` in the command line with the GUID from the output of the last command you ran. In older versions of the Hybrid Configuration Wizard the EvoSTS AuthServer was named `EvoSTS` without a GUID attached. There's no action you need to take, just modify the preceding command line by removing the GUID portion of the command.

PowerShell

```
Set-AuthServer -Identity "EvoSTS - <GUID>" -IsDefaultAuthorizationEndpoint $true  
Set-OrganizationConfig -OAuth2ClientProfileEnabled $true
```

If the Exchange Server on-premises version is Exchange Server 2016 (CU18 or higher) or Exchange Server 2019 (CU7 or higher) and hybrid was configured by the help of the HCW downloaded **after September 2020**, run the following command in the Exchange Server on-premises Management Shell (EMS). For the `DomainName` parameter, use the tenant domain value, which is usually in the form `contoso.onmicrosoft.com`:

PowerShell

```
Set-AuthServer -Identity "EvoSTS - <GUID>" -DomainName "Tenant Domain" -  
IsDefaultAuthorizationEndpoint $true  
Set-OrganizationConfig -OAuth2ClientProfileEnabled $true
```

In case Exchange Server on-premises is in hybrid with **multiple tenants**, there are multiple AuthServer objects present in the Exchange Server on-premises organizations with domains corresponding to each tenant. The `IsDefaultAuthorizationEndpoint` flag should be set to `True` for any one of these AuthServer objects. The flag can't be set to true for all the AuthServer objects and HMA would be enabled even if one of these AuthServer object `IsDefaultAuthorizationEndpoint` flag is set to true.

 **Important**

When working with **multiple tenants** they must all be in the same cloud environment such as all in **Global** or all in **GCC**. They cannot exist in mix environments such as one tenant in **Global** and another one in **GCC**.

Verify

Once you enable HMA, a client's next sign in will use the new auth flow. Just turning on HMA won't trigger a reauthentication for any client, and it might take a while for Exchange Server to pick up the new settings. This process does not necessitate the creation of a new profile.

You should also hold down the **CTRL** key at the same time you right-click the icon for the Outlook client (also in the Windows Notifications tray) and select **Connection Status**. Look for the client's SMTP address against an **AuthN** type of **Bearer***, which represents the bearer token used in OAuth.

Enable Hybrid Modern Authentication for OWA and ECP

Hybrid Modern Authentication can now also be enabled for **OWA** and **ECP**. Make sure that the [Prerequisites](#) are fulfilled before you continue.

After the Hybrid Modern Authentication was enabled for **OWA** and **ECP**, each end user and administrator who tries to log in into **OWA** or **ECP** will be redirected to the Microsoft Entra ID authentication page first. After the authentication was successful, the user will be redirected to **OWA** or **ECP**.

Prerequisites to enable Hybrid Modern Authentication for OWA and ECP

ⓘ Important

All servers must have at least the [Exchange Server 2019 CU14](#) update installed. They must also run the [Exchange Server 2019 CU14 April 2024 HU](#) or a later update.

To enable Hybrid Modern Authentication for **OWA** and **ECP**, all user identities must be synchronized with Microsoft Entra ID. In addition to this it's important that OAuth setup

between Exchange Server on-premises and Exchange Online has been established before further configuration steps can be done.

Customers who have already run the Hybrid Configuration Wizard (HCW) to configure hybrid, have an OAuth configuration in place. If OAuth wasn't configured before, it can be done by running the HCW or by following the steps as outlined in the [Configure OAuth authentication between Exchange and Exchange Online organizations](#) documentation.

It's recommended to document the `OwaVirtualDirectory` and `EcpVirtualDirectory` settings before making any changes. This documentation will enable you to restore the original settings if any issues arise after configuring the feature.

Steps to enable Hybrid Modern Authentication for OWA and ECP

Warning

Publishing Outlook Web App (OWA) and Exchange Control Panel (ECP) through Microsoft Entra application proxy is unsupported.

1. Query the `OWA` and `ECP` URLs that are configured on your Exchange Server on-premises. This is important because they must be added as reply url to Microsoft Entra ID:

PowerShell

```
Get-OwaVirtualDirectory -ADPropertiesOnly | fl name, *url*
Get-EcpVirtualDirectory -ADPropertiesOnly | fl name, *url*
```

2. Install the Microsoft Graph PowerShell module if it hasn't yet been installed:

PowerShell

```
Install-Module Microsoft.Graph -Scope AllUsers
```

3. Connect to Microsoft Entra ID with [these instructions](#). To consent to the required permissions, run the following command:

PowerShell

```
Connect-Graph -Scopes User.Read, Application.ReadWrite.All
```

4. Specify your `OWA` and `ECP` URLs and update your application with the reply URLs:

PowerShell

```
$servicePrincipal = Get-MgServicePrincipal -Filter "appId eq '00000002-0000-0ff1-ce00-000000000000'"
$servicePrincipal.replyUrls += "https://YourDomain.contoso.com/owa"
$servicePrincipal.replyUrls += "https://YourDomain.contoso.com/ecp"
Update-MgServicePrincipal -ServicePrincipalId $servicePrincipal.Id -appId "00000002-0000-0ff1-ce00-000000000000" -ReplyUrls
$servicePrincipal.replyUrls
```

5. Verify that the reply URLs have been added successfully:

PowerShell

```
(Get-MgServicePrincipal -Filter "appId eq '00000002-0000-0ff1-ce00-000000000000").ReplyUrls
```

6. To enable Exchange Server on-premises ability to perform Hybrid Modern Authentication, follow the steps outlined in the [Enable HMA](#) section.

7. (Optional) Only required if [Download Domains](#) are used:

Create a new global setting override by running the following commands from an elevated Exchange Management Shell (EMS). Run these commands on one Exchange Server:

PowerShell

```
New-SettingOverride -Name "OWA HMA Download Domain Support" -Component "OAuth" -Section "OAuthIdentityCacheFixForDownloadDomains" -Parameters ("Enabled=true") -Reason "Enable support for OWA HMA when Download Domains are in use"
Get-ExchangeDiagnosticInfo -Process Microsoft.Exchange.Directory.TopologyService -Component VariantConfiguration -Argument Refresh
Restart-Service -Name W3SVC, WAS -Force
```

8. (Optional) Only required in [Exchange resource forest topology](#) scenarios:

Add the following keys to the `<appSettings>` node of the

`<ExchangeInstallPath>\ClientAccess\Owa\web.config` file. Do this on each

Exchange Server:

notepad

```
<add key="OAuthHttpModule.ConvertToSidBasedIdentity" value="true"/>
<add key="OAuthHttpModule.UseMasterAccountSid" value="true"/>
```

Create a new global setting override by running the following commands from an elevated Exchange Management Shell (EMS). Run these commands on one Exchange Server:

PowerShell

```
New-SettingOverride -Name "OWA HMA AFRF Support" -Component "OAuth" -
Section "OwaHMAFixForAfRfScenarios" -Parameters ("Enabled=true") -
Reason "Enable support for OWA HMA in AFRF scenarios"
Get-ExchangeDiagnosticInfo -Process
Microsoft.Exchange.Directory.TopologyService -Component
VariantConfiguration -Argument Refresh
Restart-Service -Name W3SVC, WAS -Force
```

9. To enable Hybrid Modern Authentication for `OWA` and `ECP`, you must first disable any other authentication method on these virtual directories. It's important to perform the configuration in the given order. Failing to do so may result in an error message during the command execution.

Run these commands for each `OWA` and `ECP` virtual directory on each Exchange Server to disable all other authentication methods:

PowerShell

```
Get-OwaVirtualDirectory -Server <computername> | Set-
OwaVirtualDirectory -AdfsAuthentication $false -BasicAuthentication
	assertFalse -FormsAuthentication $false -DigestAuthentication $false
Get-EcpVirtualDirectory -Server <computername> | Set-
EcpVirtualDirectory -AdfsAuthentication $false -BasicAuthentication
	assertFalse -FormsAuthentication $false -DigestAuthentication $false
```

ⓘ Important

Ensure that all accounts are synchronized to Microsoft Entra ID, especially all accounts, which are used for administration. Otherwise, the login stops working until they're synchronized. Accounts, such as the built-in Administrator, won't be synchronized with Microsoft Entra ID and, therefore,

can't be used for administration once HMA for OWA and ECP has been enabled. This behavior is due to the `isCriticalSystemObject` attribute, which is set to `True` for some accounts.

10. Enable OAuth for the `OWA` and `ECP` virtual directory. It's important to perform the configuration in the given order. Failing to do so may result in an error message during the command execution. For each `OWA` and `ECP` virtual directory on every Exchange Server, these commands must be run:

PowerShell

```
Get-EcpVirtualDirectory -Server <computername> | Set-
EcpVirtualDirectory -OAuthAuthentication $true
Get-OwaVirtualDirectory -Server <computername> | Set-
OwaVirtualDirectory -OAuthAuthentication $true
```

Using Hybrid Modern Authentication with Outlook for iOS and Android

If you want to use the Outlook for iOS and Android client together with Hybrid Modern Authentication, make sure to allow the AutoDetect service to connect to your Exchange Server on `TCP 443` (`HTTPS`):

Console

```
<email_domain>.outlookmobile.com
<email_domain>.outlookmobile.us
52.125.128.0/20
52.127.96.0/23
```

The IP address ranges can also be found in the [Additional endpoints not included in the Office 365 IP Address and URL Web service documentation](#).

Related articles

[Modern Authentication configuration requirements for transition from Office 365 dedicated/ITAR to vNext](#)

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Removing or disabling Hybrid Modern Authentication from Skype for Business and Exchange

Article • 08/13/2024

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

If you've enabled Hybrid Modern Authentication (HMA) only to find it's unsuitable for your current environment, you can disable HMA. This article explains how.

Who is this article for?

If you've enabled Modern Authentication in Skype for Business Online or On-premises, and/or Exchange Online or On-premises and found you need to disable HMA, these steps are for you.

ⓘ Important

See the '[Skype for Business topologies supported with Modern Authentication](#)' article if you're in Skype for Business Online or On-premises, have a mixed-topology HMA, and need to look at supported topologies before you begin.

How to disable Hybrid Modern Authentication (Exchange)

1. **Exchange On-premises:** [Open the Exchange Management Shell](#) and run the following commands:

PowerShell

```
Set-OrganizationConfig -OAuth2ClientProfileEnabled $false  
Set-AuthServer -Identity evoSTS -IsDefaultAuthorizationEndpoint $false
```

2. **Exchange Online:** [Connect to Exchange Online PowerShell](#). Run the following command to disable Modern Authentication:

PowerShell

```
Set-OrganizationConfig -OAuth2ClientProfileEnabled:$false
```

How to disable Hybrid Modern Authentication (Skype for Business)

1. **Skype for Business On-premises:** Run the following commands in Skype for Business Management Shell:

PowerShell

```
Set-CsOAuthConfiguration -ClientAuthorizationOAuthServerIdentity ""
```

2. **Skype for Business Online:** [Connect to Skype for Business Online PowerShell](#). Run the following command to disable Modern Authentication:

PowerShell

```
Set-CsOAuthConfiguration -ClientAdalAuthOverride Disallowed
```

[Link back to the Modern Authentication overview.](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

How modern authentication works for Office 2016 and Office 2019 client apps

Article • 05/03/2024

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Read this article to learn how Office 2016 and Office 2019 client apps use modern authentication features based on the authentication configuration on the Microsoft 365 tenant for Exchange Online, SharePoint Online, and Skype for Business Online.

ⓘ Note

Legacy client apps, such as Office 2010 and Office for Mac 2011, do not support modern authentication and can only be used with basic authentication.

Availability of modern authentication for Microsoft 365 services

For the Microsoft 365 services, the default state of modern authentication is:

- Turned **on** for Exchange Online by default. See [Enable or disable modern authentication in Exchange Online](#) to turn it off or on.
- Turned **on** for SharePoint Online by default.
- Turned **on** for Skype for Business Online by default. See [Enable Skype for Business Online for modern authentication](#) to turn it off or on.

ⓘ Note

For tenants created **before** August 1, 2017, modern authentication is turned **off** by default for Exchange Online and Skype for Business Online.

Select the links below to see how Office 2016 and Office 2019 client authentication works with the Microsoft 365 services depending on whether or not modern authentication is turned on.

- [Exchange Online](#)

- SharePoint Online
- Skype for Business Online

Exchange Online

The following table describes the authentication behavior for Office 2016 and Office 2019 client apps when they connect to Exchange Online with or without modern authentication.

[\[+\] Expand table](#)

Office client app version	Registry key present?	Modern authentication on?	Authentication behavior with modern authentication turned on for the tenant (default)	Authentication behavior with modern authentication turned off for the tenant
Office 2019	No, AlwaysUseMSOAuthForAutoDiscover = 1	Yes	Forces modern authentication on Outlook 2013, 2016, or 2019. More info ↗	Forces modern authentication within the Outlook client.
Office 2019	No, or EnableADAL = 1	Yes	Modern authentication is attempted first. If the server refuses a modern authentication connection, then basic authentication is used. Server refuses modern authentication when the tenant isn't enabled.	Modern authentication is attempted first. If the server refuses a modern authentication connection, then basic authentication is used. Server refuses modern authentication when the tenant isn't enabled.
Office 2019	Yes, EnableADAL = 1	Yes	Modern authentication is attempted first. If the	Modern authentication is attempted first. If the

Office client app version	Registry key present?	Modern authentication on?	Authentication behavior with modern authentication turned on for the tenant (default)	Authentication behavior with modern authentication turned off for the tenant
			server refuses a modern authentication connection, then basic authentication is used. Server refuses modern authentication when the tenant isn't enabled.	server refuses a modern authentication connection, then basic authentication is used. Server refuses modern authentication when the tenant isn't enabled.
Office 2019	Yes, EnableADAL=0	No	Basic authentication	Basic authentication
Office 2016	No, AlwaysUseMSOAuthForAutoDiscover = 1	Yes	Forces modern authentication on 2013, 2016, or 2019. More info ↗	Forces modern authentication within the Outlook client.
Office 2016	No, or EnableADAL = 1	Yes	Modern authentication is attempted first. If the server refuses a modern authentication connection, then basic authentication is used. Server refuses modern authentication when the tenant isn't enabled.	Modern authentication is attempted first. If the server refuses a modern authentication connection, then basic authentication is used. Server refuses modern authentication when the tenant isn't enabled.
Office 2016	Yes, EnableADAL = 1	Yes	Modern authentication is attempted	Modern authentication is attempted

Office client app version	Registry key present?	Modern authentication on?	Authentication behavior with modern authentication turned on for the tenant (default)	Authentication behavior with modern authentication turned off for the tenant
			first. If the server refuses a modern authentication connection, then basic authentication is used. Server refuses modern authentication when the tenant isn't enabled.	first. If the server refuses a modern authentication connection, then basic authentication is used. Server refuses modern authentication when the tenant isn't enabled.
Office 2016	Yes, EnableADAL=0	No	Basic authentication	Basic authentication

SharePoint Online

The following table describes the authentication behavior for Office 2016 and Office 2019 client apps when they connect to SharePoint Online with or without modern authentication.

[Expand table](#)

Office client app version	Registry key present?	Modern authentication on?	Authentication behavior with modern authentication turned on for the tenant (default)	Authentication behavior with modern authentication turned off for the tenant
Office 2019	No, or EnableADAL = 1	Yes	Modern authentication only.	Failure to connect.
Office 2019	Yes, EnableADAL = 1	Yes	Modern authentication only.	Failure to connect.

Office client app version	Registry key present?	Modern authentication on?	Authentication behavior with modern authentication turned on for the tenant (default)	Authentication behavior with modern authentication turned off for the tenant
Office 2019	Yes, EnableADAL = 0	No	Microsoft Online Sign-in Assistant only.	Microsoft Online Sign-in Assistant only.
Office 2016	No, or EnableADAL = 1	Yes	Modern authentication only.	Failure to connect.
Office 2016	Yes, EnableADAL = 1	Yes	Modern authentication only.	Failure to connect.
Office 2016	Yes, EnableADAL = 0	No	Microsoft Online Sign-in Assistant only.	Microsoft Online Sign-in Assistant only.

Skype for Business Online

The following table describes the authentication behavior for Office 2016 and Office 2019 client apps when they connect to Skype for Business Online with or without modern authentication.

[Expand table](#)

Office client app version	Registry key present?	Modern authentication on?	Authentication behavior with modern authentication turned on for the tenant	Authentication behavior with modern authentication turned off for the tenant (default)
Office 2019	No, or EnableADAL = 1	Yes	Modern authentication is attempted first. If the server refuses a modern authentication connection, then Microsoft Online Sign-in Assistant is used. Server refuses modern authentication when Skype for Business	Modern authentication is attempted first. If the server refuses a modern authentication connection, then Microsoft Online Sign-in Assistant is used. Server refuses modern authentication when Skype for Business

Office client app version	Registry key present?	Modern authentication on?	Authentication behavior with modern authentication turned on for the tenant	Authentication behavior with modern authentication turned off for the tenant (default)
			Online tenants aren't enabled.	Online tenants aren't enabled.
Office 2019	Yes, EnableADAL = 1	Yes	Modern authentication is attempted first. If the server refuses a modern authentication connection, then Microsoft Online Sign-in Assistant is used. Server refuses modern authentication when Skype for Business Online tenants aren't enabled.	Modern authentication is attempted first. If the server refuses a modern authentication connection, then Microsoft Online Sign-in Assistant is used. Server refuses modern authentication when Skype for Business Online tenants aren't enabled.
Office 2019	Yes, EnableADAL = 0	No	Microsoft Online Sign-in Assistant only.	Microsoft Online Sign-in Assistant only.
Office 2016	No, or EnableADAL = 1	Yes	Modern authentication is attempted first. If the server refuses a modern authentication connection, then Microsoft Online Sign-in Assistant is used. Server refuses modern authentication when Skype for Business Online tenants aren't enabled.	Modern authentication is attempted first. If the server refuses a modern authentication connection, then Microsoft Online Sign-in Assistant is used. Server refuses modern authentication when Skype for Business Online tenants aren't enabled.
Office 2016	Yes, EnableADAL = 1	Yes	Modern authentication is attempted first. If the server refuses a modern authentication connection, then Microsoft Online Sign-in Assistant is used. Server refuses modern authentication when Skype for Business	Modern authentication is attempted first. If the server refuses a modern authentication connection, then Microsoft Online Sign-in Assistant is used. Server refuses modern authentication when Skype for Business

Office client app version	Registry key present?	Modern authentication on?	Authentication behavior with modern authentication turned on for the tenant	Authentication behavior with modern authentication turned off for the tenant (default)
			Online tenants aren't enabled.	Online tenants aren't enabled.
Office 2016	Yes, EnableADAL = 0	No	Microsoft Online Sign-in Assistant only.	Microsoft Online Sign-in Assistant only.

See also

[Multifactor authentication for Microsoft 365](#)

[Sign in to Microsoft 365 with multifactor authentication ↗](#)

[Microsoft 365 Enterprise overview](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Microsoft 365 isolation controls

Article • 06/10/2024

Microsoft continuously works to ensure that the multitenant architecture of Microsoft 365 supports enterprise-level security, confidentiality, privacy, data integrity, availability, and meets local and international [standards](#). The scale and the scope of services provided by Microsoft make it difficult and impractical to manage with significant human interaction. Microsoft 365 services are provided through globally distributed data centers, each highly automated with few operations requiring a human touch or any access to customer data. Our staff supports these services and data centers using automated tools and highly secure remote access.

Microsoft 365 is composed of multiple services that provide important business functionality and contribute to the overall experience. Each of these services is self-contained and designed to integrate with one another. Microsoft 365 is designed with the following principles:

- Service-oriented architecture: designing and developing software in the form of interoperable services providing well-defined business functionality.
- [Operational security assurance](#): a framework that incorporates the knowledge gained through various capabilities that are unique to Microsoft, including the Microsoft [Security Development Lifecycle](#), the [Microsoft Security Response Center](#), and deep awareness of the cybersecurity threat landscape.

Microsoft 365 services inter-operate with each other but are designed and implemented so they can be deployed and operated as autonomous services, independent of each other. Microsoft segregates duties and areas of responsibility for Microsoft 365 to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. Microsoft 365 teams have defined roles as part of a comprehensive role-based access control mechanism.

Tenant isolation

One of the primary benefits of cloud computing is the concept of a shared, common infrastructure across numerous customers simultaneously, leading to economies of scale.

The two primary goals of maintaining tenant isolation in a multitenant environment are:

- Preventing leakage of, or unauthorized access to, customer data across tenants; and

- Preventing the actions of one tenant from adversely affecting the service for another tenant

Microsoft online services were designed with the assumption that all tenants are potentially hostile to all other tenants, and we have implemented security measures to prevent the actions of one tenant from affecting the security or service of another tenant, or accessing their content.

Multiple forms of protection have been implemented throughout Microsoft 365 to prevent the compromising of services or applications, or gaining unauthorized access to the information of other tenants or the systems themselves, including:

- Logical isolation of customer data within each tenant for Microsoft 365 services is achieved through Microsoft Entra authorization and role-based access control.
- Isolation of data at the storage level for services such as SharePoint Online.
- Microsoft uses rigorous physical security, background screening, and a multi-layered encryption strategy to protect the confidentiality and integrity of customer data. All Microsoft 365 datacenters have biometric access controls, with most requiring palm prints to gain physical access. In addition, all U.S.-based Microsoft employees are required to successfully complete a standard background check as part of the hiring process. For more information on the controls used for administrative access in Microsoft 365, see [Microsoft 365 Account Management](#).
- Microsoft 365 uses service-side technologies that encrypt customer content at rest and in transit, including BitLocker, per-file encryption, Transport Layer Security (TLS) and Internet Protocol Security (IPsec). For specific details about encryption in Microsoft 365, see [Data Encryption Technologies in Microsoft 365](#).

Together, the above-listed protections provide robust logical isolation controls that provide threat protection and mitigation equivalent to that provided by physical isolation alone.

Resources

- [Isolation and access control in Microsoft Entra ID](#)
- [Monitoring and testing tenant boundaries](#)
- [Isolation and access control in Microsoft 365](#)

Feedback

Was this page helpful?



Microsoft 365 Isolation and Access Control in Microsoft Entra ID

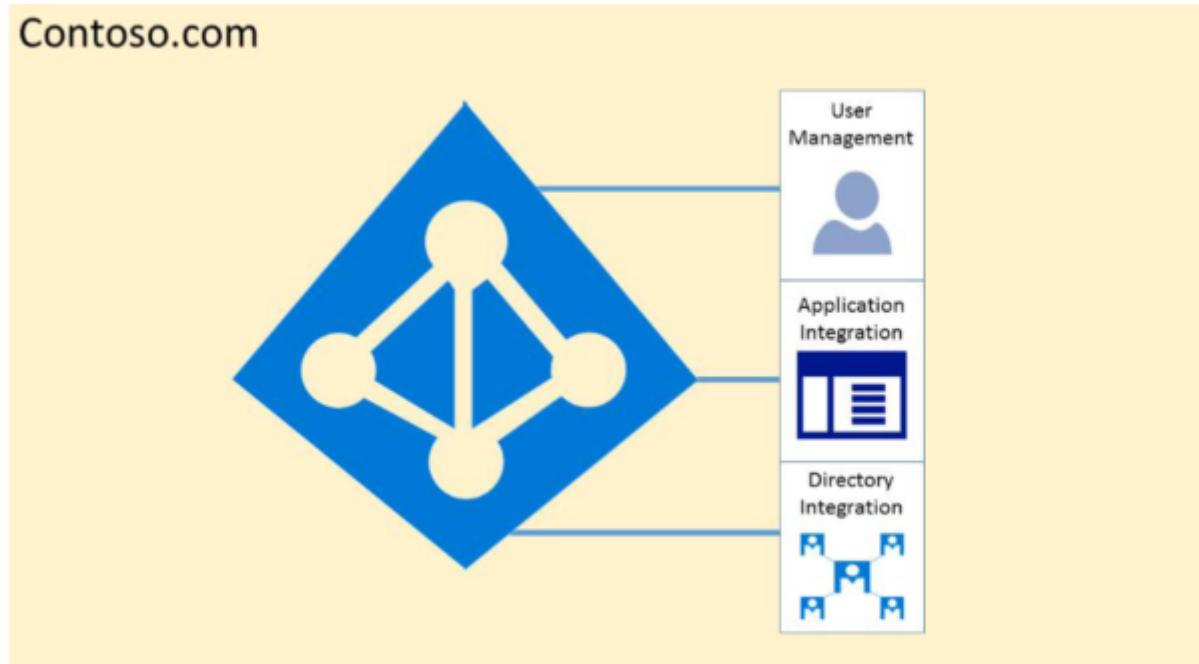
Article • 06/28/2024

Microsoft Entra ID was designed to host multiple tenants in a highly secure way through logical data isolation. Access to Microsoft Entra ID is gated by an authorization layer. Microsoft Entra ID isolates customers using tenant containers as security boundaries to safeguard a customer's content so that the content can't be accessed or compromised by co-tenants. Three checks are performed by Microsoft Entra authorization layer:

- Is the principal enabled for access to Microsoft Entra tenant?
- Is the principal enabled for access to data in this tenant?
- Is the principal's role in this tenant authorized for the type of data access requested?

No application, user, server, or service can access Microsoft Entra ID without the proper authentication and token or certificate. Requests are rejected if they aren't accompanied by proper credentials.

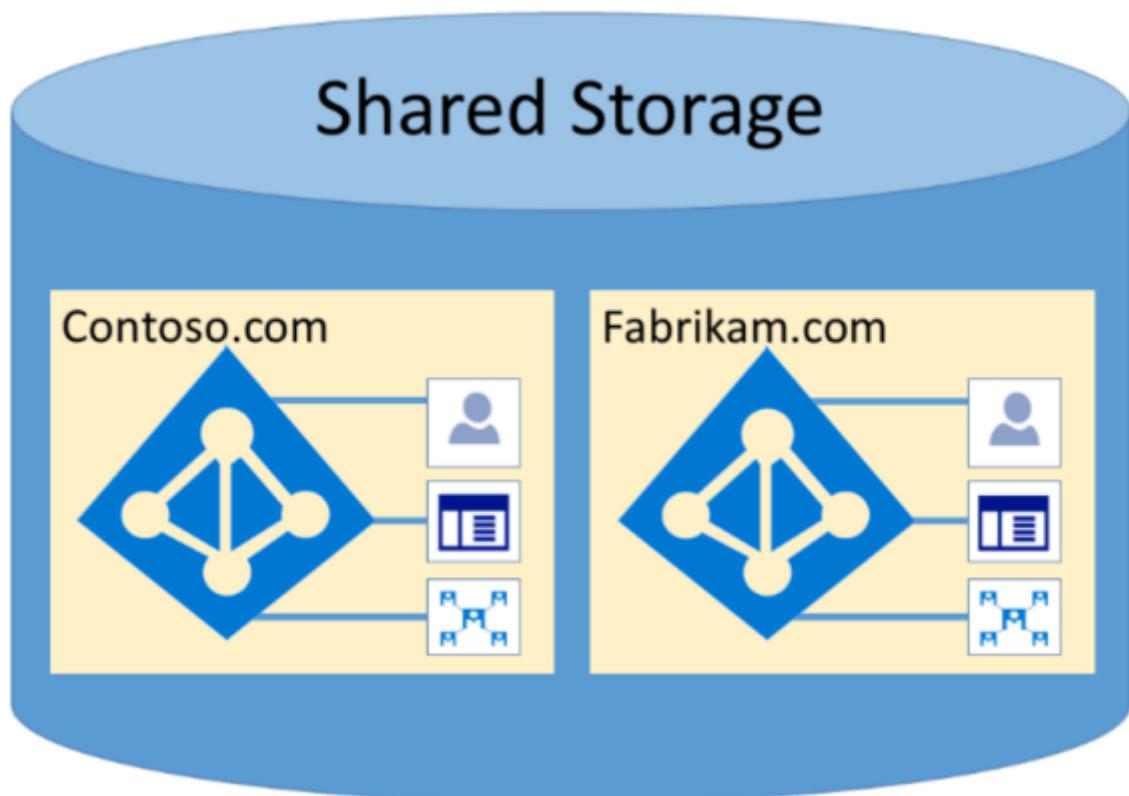
Effectively, Microsoft Entra ID hosts each tenant in its own protected container, with policies and permissions to and within the container solely owned and managed by the tenant.



The concept of tenant containers is deeply ingrained in the directory service at all layers, from portals all the way to persistent storage. Even when multiple Microsoft Entra tenant metadata is stored on the same physical disk, there's no relationship between the

containers other than what is defined by the directory service, which in turn is dictated by the tenant administrator. There can be no direct connections to Microsoft Entra storage from any requesting application or service without first going through the authorization layer.

In the following example, Contoso and Fabrikam both have separate, dedicated containers, and even though those containers can share some of the same underlying infrastructure, such as servers and storage, they remain separate and isolated from each other, and gated by layers of authorization and access control.



In addition, there are no application components that can execute from within Microsoft Entra ID, and it isn't possible for one tenant to forcibly breach the integrity of another tenant, access encryption keys of another tenant, or read raw data from the server.

By default, Microsoft Entra disallows all operations issued by identities in other tenants. Each tenant is logically isolated within Microsoft Entra ID through claims-based access controls. Reads and writes of directory data are scoped to tenant containers, and gated by an internal abstraction layer and a role-based access control (RBAC) layer, which together enforce the tenant as the security boundary. Every directory data access request is processed by these layers and every access request in Microsoft 365 is policed by the previous logic.

Microsoft Entra ID has North America, U.S. Government, European Union, Germany, and World Wide partitions. A tenant exists in a single partition, and partitions can contain

multiple tenants. Partition information is abstracted away from users. A given partition (including all the tenants within it) is replicated to multiple datacenters. The partition for a tenant is chosen based on properties of the tenant (for example, the country code). Secrets and other sensitive information in each partition is encrypted with a dedicated key. The keys are generated automatically when a new partition is created.

Microsoft Entra system functionalities are a unique instance to each user session. In addition, Microsoft Entra ID uses encryption technologies to provide isolation of shared system resources at the network level to prevent unauthorized and unintended transfer of information.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Attack simulation in Microsoft 365

Article • 05/23/2024

Based on detailed analysis of security trends, Microsoft advocates and highlights the need for other investments in reactive security processes and technologies that focus on detection and response to emerging threats, rather than solely the prevention of those threats. Because of changes in the threat landscape and in-depth analysis, Microsoft has refined its security strategy beyond just preventing security breaches to one better equipped to deal with breaches when they do occur; a strategy that considers major security events not as a matter of if, but when.

While Microsoft's [assume breach](#) practices have been in place for many years, many customers are unaware of the work being done behind the scenes to harden the Microsoft cloud. Assume breach is a mindset that guides security investments, design decisions, and operational security practices. Assume breach limits the trust placed in applications, services, identities, and networks by treating them all—internal and external—as insecure and already compromised. Although the assume breach strategy wasn't born from an actual breach of any Microsoft enterprise or cloud services, it was recognized that many organizations across the industry were being breached despite all attempts to prevent it. While preventing breaches is a critical part of any organization's operations, those practices must be continuously tested and augmented to effectively address modern adversaries and advanced persistent threats. For any organization to prepare for a breach, they must first build and maintain robust, repeatable, and thoroughly tested security response procedures.

While prevent breach security processes, such as threat modeling, code reviews, and security testing are useful as part of the [Security Development Lifecycle](#), assume breach provides numerous advantages that help account for overall security by exercising and measuring reactive capabilities in the event of a breach.

At Microsoft, we set out to accomplish this through ongoing war-games exercises and live site penetration testing of our security response plans with the goal of improving our detection and response capability. Microsoft regularly simulates real-world breaches, conducts continuous security monitoring, and practices security incident management to validate and improve the security of Microsoft 365, Azure, and other Microsoft cloud services.

Microsoft executes the assume breach security strategy using two core groups:

- Red Teams (attackers)
- Blue Teams (defenders)

Both Microsoft Azure and Microsoft 365 staff separate full-time Red Teams and Blue Teams.

Referred to as "[Red Teaming](#)", the approach is to test Azure and Microsoft 365 systems and operations using the same tactics, techniques and procedures as real adversaries, against the live production infrastructure, without the foreknowledge of the Engineering or Operations teams. This tests Microsoft's security detection and response capabilities, and helps identify production vulnerabilities, configuration errors, invalid assumptions, and other security issues in a controlled manner. Every Red Team breach is followed by full disclosure between both teams to identify gaps, address findings, and improve breach response.

 **Note**

No customer tenants, data, or applications are deliberately targeted during Red Teaming or live site penetration testing. The tests are against Microsoft 365 and Azure infrastructure and platforms, as well as Microsoft's own tenants, applications, and data.

Red Teams

The Red Team is a group of full-time staff within Microsoft that focuses on breaching Microsoft's infrastructure, platform, and Microsoft's own tenants and applications. They're the dedicated adversary (a group of ethical hackers) performing targeted and persistent attacks against Online Services (Microsoft infrastructure, platforms, and applications but not end-customers' applications or content).

The role of the Red Team is to attack and penetrate environments using the same steps as an adversary:



Among other functions, red teams specifically attempt to breach tenant isolation boundaries to find bugs or gaps in our isolation design.

To help scale testing efforts, the Red Team has created an automated attack simulation tool that runs safely in specific Microsoft 365 environments on a recurring basis. The tool has a wide variety of predefined attacks that are constantly expanded and improved to help reflect the evolving threat landscape. In addition to broadening the coverage of Red Team testing, it helps the Blue Team validate and improve their security monitoring

logic. Regular, ongoing attack emulation provides the Blue Team with a consistent and diverse stream of signals that are compared and validated against expected responses. This leads to improvements in Microsoft 365's security monitoring logic and response capabilities.

Blue Teams

The Blue Team is composed of either a dedicated set of security responders or members from across the security incident response, Engineering, and Operations organizations. Regardless of their make-up, they're independent and operate separately from the Red Team. The Blue Team follows established security processes and uses the latest tools and technologies to detect and respond to attacks and penetration. Just like real-world attacks, the Blue Team doesn't know when or how the Red Team's attacks occur or what methods may be used. Their job, whether it's a Red Team attack or an actual assault, is to detect and respond to all security incidents. For this reason, the Blue Team is continuously on-call and must react to Red Team breaches the same way they would for any other breach.

When an adversary, such as a Red Team, has breached an environment, the Blue Team must:

- Gather evidence left by the adversary
- Detect the evidence as an indication of compromise
- Alert the appropriate Engineering and Operation team(s)
- Triage the alerts to determine whether they warrant further investigation
- Gather context from the environment to scope the breach
- Form a remediation plan to contain or evict the adversary
- Execute the remediation plan and recover from breach

These steps form the security incident response that runs parallel to the adversary, as shown below:



Red Team breaches allow for exercising the Blue Team's ability to detect and respond to real-world attacks end-to-end. Most importantly, it allows for practiced security incident response prior to a genuine breach. Additionally, because of Red Team breaches, the Blue Team enhances their situational awareness, which can be valuable when dealing with future breaches (whether from the Red Team or another adversary). Throughout the detection and response process, the Blue Team produces actionable intelligence and gains visibility into the actual conditions of the environment(s) they're trying to defend.

Frequently this is accomplished via data analysis and forensics, performed by the Blue Team, when responding to Red Team attacks and by establishing threat indicators, such as indicators of compromise. Much like how the Red Team identifies gaps in the security story, blue teams identify gaps in their ability to detect and respond. Furthermore, since the Red Team's model real-world attacks, the Blue Team can be accurately assessed on their ability to deal with determined and persistent adversaries. Finally, Red Team breaches measure both readiness and impact of our breach response.

Feedback

Was this page helpful?



Service resource limits

Article • 06/24/2024

Resource limits are enforced using quotas (limits) and throttling. Microsoft Entra ID and the individual Microsoft 365 services use both. Limits are service-specific and change over time as new capabilities are added. For details on the current limits for the various services, see the following topics:

- [Microsoft Entra service limits and restrictions](#)
- [Exchange Limits](#)
- [SharePoint software boundaries and limits ↗](#)
- [File Size Limits in Sway ↗](#)

In addition to these limits, several throttling mechanisms are used throughout Microsoft Entra ID and Microsoft 365. Throttling within the service is especially important, given that network resources in Microsoft's datacenters are optimized for the broad set of customers that use the services. Throttling mechanisms include:

- Microsoft Entra ID and Microsoft 365 feature user-level throttling, which limit the number of transactions or concurrent calls (by script or code) that can be performed by a single user.
- A default PowerShell throttling policy is assigned to each tenant at tenant creation. These settings affect other items, such as the maximum number of simultaneous PowerShell sessions that can be opened by a single administrator.
- Each Exchange Online customer has a default Exchange Web Services (EWS) policy that is tuned for EWS client operations, and throttling that applies to all Outlook clients.

Feedback

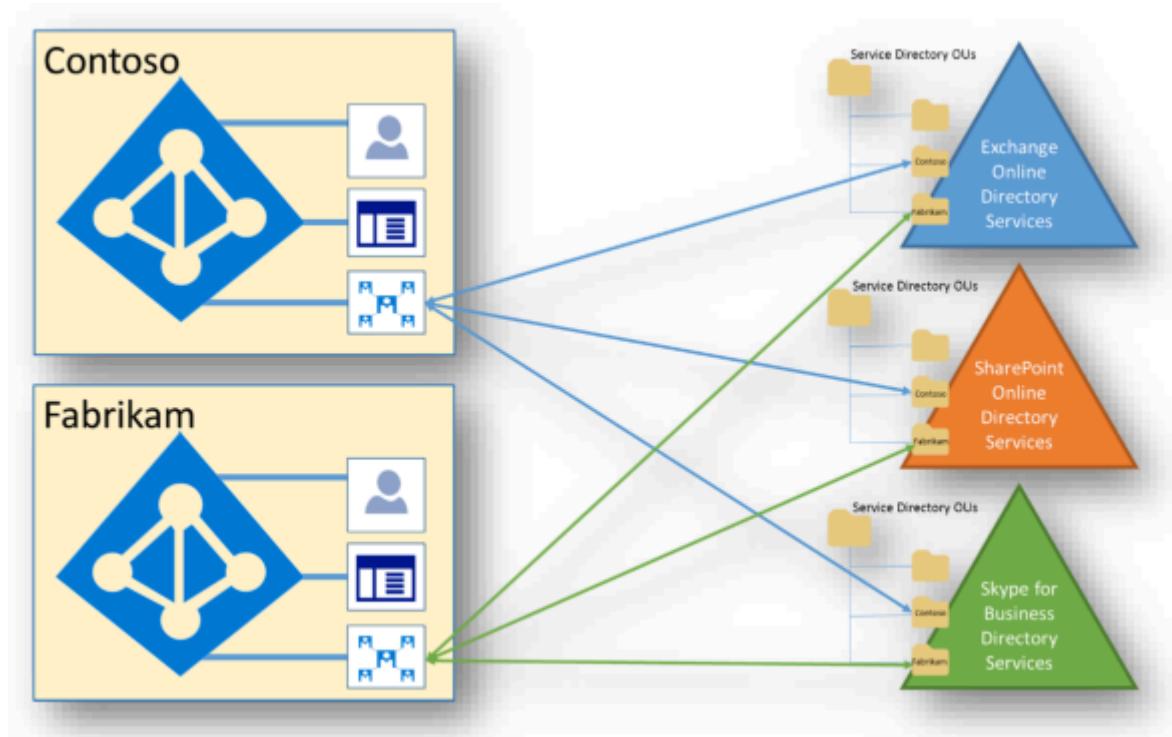
Was this page helpful?



Isolation and Access Control in Microsoft 365

Article • 05/17/2024

Microsoft Entra ID and Microsoft 365 use a highly complex data model that includes tens of services, hundreds of entities, thousands of relationships, and tens of thousands of attributes. At a high level, Microsoft Entra ID and the service directories are the containers of tenants and recipients kept in sync using state-based replication protocols. In addition to the directory information held within Microsoft Entra ID, each of the service workloads have their own directory services infrastructure.



Within this model, there's no single source of directory data. Specific systems own individual pieces of data, but no single system holds all the data. Microsoft 365 services cooperate with Microsoft Entra ID in this data model. Microsoft Entra ID is the "system of truth" for shared data, which is typically small and static data used by every service. The federated model used within Microsoft 365 and Microsoft Entra ID provides the shared view of the data.

Microsoft 365 uses both physical storage and Azure cloud storage. Exchange Online (including Exchange Online Protection) and Skype for Business use their own storage for customer data. SharePoint uses both SQL Server storage and Azure Storage, hence the need for extra isolation of customer data at the storage level.

Exchange Online

Exchange Online stores customer data within mailboxes. Mailboxes are hosted within Extensible Storage Engine (ESE) databases called mailbox databases. This includes user mailboxes, linked mailboxes, shared mailboxes, and public folder mailboxes. User mailboxes include saved Skype for Business content, such as conversation histories.

User mailbox content includes:

- Emails and email attachments
- Calendaring and free/busy information
- Contacts
- Tasks
- Notes
- Groups
- Inference data

Each mailbox database within Exchange Online contains mailboxes from multiple tenants. An authorization code secures each mailbox, including within a tenancy. By default, only the assigned user has access to a mailbox. The access control list (ACL) that secures a mailbox contains an identity authenticated by Microsoft Entra ID at the tenant level. The mailboxes for each tenant are limited to identities authenticated against the tenant's authentication provider, which includes only users from that tenant. Content in tenant A can't in any way be obtained by users in tenant B, unless explicitly approved by tenant A.

Skype for Business

Skype for Business stores data in various places:

- User and account information, which includes connection endpoints, tenant IDs, dial plans, roaming settings, presence state, contact lists, etc., is stored in the Skype for Business Active Directory servers, and in various Skype for Business database servers. Contact lists are stored in the user's Exchange Online mailbox if the user is enabled for both products, or on Skype for Business servers if the user isn't. Skype for Business database servers isn't partitioned per-tenant, but multi-tenancy isolation of data is enforced through Role-based access control (RBAC).
- Meeting content and uploaded-data is stored on Distributed File System (DFS) shares. This content can also be archived in Exchange Online if enabled. The DFS shares are not partitioned per-tenant. the content is secured with ACLs and multi-tenancy is enforced through RBAC.

- Call detail records, which are the activity history, such as call history, IM sessions, application sharing, IM history, etc., can also be stored in Exchange Online, but most call detail records are temporarily stored on call detail record (CDR) servers. Content isn't partitioned per tenant, but multi-tenancy is enforced through RBAC.

SharePoint

SharePoint has several independent mechanisms that provide data isolation. It stores objects as abstracted code within application databases. For example, when a user uploads a file to SharePoint, the file is disassembled, translated into application code, and stored in multiple tables across multiple databases.

If a user could gain direct access to the storage containing the data, the content isn't interpretable to a human or any system other than SharePoint. These mechanisms include security access control and properties. All SharePoint resources are secured by the authorization code and RBAC policy, including within a tenancy. The access control list (ACL) that secures a resource contains an identity authenticated at the tenant level. SharePoint data for a tenant is limited to identities authenticated by the authentication provider for the tenant.

In addition to the ACLs, a tenant level property that specifies the authentication provider (which is the tenant-specific Microsoft Entra ID), is written once and can't be changed once set. Once the authentication provider tenant property has been set for a tenant, it cannot be changed using any APIs exposed to a tenant.

A unique *SubscriptionId* is used for each tenant. All customer sites are owned by a tenant and assigned a *SubscriptionId* unique to the tenant. The *SubscriptionId* property on a site is written once and is permanent. Once assigned to a tenant, a site can't be moved to a different tenant. The *SubscriptionId* is the key used to create the security scope for the authentication provider and is tied to the tenant.

SharePoint uses SQL Server and Azure Storage for content metadata storage. The partition key for the content store is *Siteld* in SQL. When running a SQL query, SharePoint uses a *Siteld* verified as part of a tenant-level *SubscriptionId* check.

SharePoint stores encrypted file content in Microsoft Azure blobs. Each SharePoint farm has its own Microsoft Azure account and all the blobs saved in Azure are encrypted individually with a key stored in the SQL content store. The encryption key protected in code by the authorization layer and not exposed directly to the end user. SharePoint has real-time monitoring to detect when an HTTP request reads or writes data for more than one tenant. The request identity *SubscriptionId* is tracked against the *SubscriptionId* of the accessed resource. Requests to access resources of more than one tenant should

never happen by end users. Service requests in a multi-tenant environment are the only exception. For example, the search crawler pulls content changes for an entire database all at once. This usually involves querying sites of more than one tenant in a single service request, which is done for efficiency reasons.

Teams

Your Teams data is stored differently, depending on the content type.

Check out the [Ignite breakout session on Microsoft Teams architecture](#) for an in-depth discussion.

Core Teams customer data

If your tenant is provisioned in Australia, Canada, the European Union, France, Germany, India, Japan, South Africa, South Korea, Switzerland (which includes Liechtenstein), the United Arab Emirates, the United Kingdom, or the United States, Microsoft stores the following customer data at rest only within that location:

- Teams chats, team and channel conversations, images, voicemail messages, and contacts.
- SharePoint site content and the files stored within that site.
- Files uploaded to OneDrive for work or school.

Chat, channel messages, team structure

Every team in Teams is backed by a Microsoft 365 Group and its SharePoint site and Exchange mailbox. Private chats (including group chats), messages sent as part of a conversation in a channel, and the structure of teams and channels are stored in a chat service running in Azure. The data is also stored in a hidden folder in the user and group mailboxes to enable Information Protection features.

Voicemail and contacts

Voicemails are stored in Exchange. Contacts are stored in Exchange-based cloud data store. Exchange and the Exchange-based cloud store already provide data residency in each of the worldwide datacenter geos. For all teams, voicemail and contacts are stored in-country for Australia, Canada, France, Germany, India, Japan, the United Arab Emirates, the United Kingdom, South Africa, South Korea, Switzerland (which includes Liechtenstein), and the United States. For all other countries/regions, files are stored in the US, Europe, or Asia-Pacific location based on tenant affinity.

Images and media

Media used in chats (except for Giphy GIFs that aren't stored but are a reference link to the original Giphy service URL, Giphy is a non-Microsoft service) is stored in an Azure-based media service that is deployed to the same locations as the chat service.

Files

Files (including OneNote and Wiki) that somebody shares in a channel are stored in the team's SharePoint site. Files shared in a private chat or a chat during a meeting or call are uploaded and stored in the OneDrive for work or school account of the user who shares the file. Exchange, SharePoint, and OneDrive already provide data residency in each of the worldwide datacenter geos. So, for existing customers, all files, OneNote notebooks, Teams wiki content, and mailboxes that are part of the Teams experience are already stored in the location based on your tenant affinity. Files are stored in-country for Australia, Canada, France, Germany, India, Japan, the United Arab Emirates, the United Kingdom, South Africa, South Korea, and Switzerland (which includes Liechtenstein). For all other countries/regions, files are stored in the US, Europe, or Asia Pacific location based on tenant affinity.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback !\[\]\(393646b7c55648f148e9b7703e7f3b1f_img.jpg\)](#)

Add a domain to Microsoft 365

Article • 08/11/2024

[Check the Domains FAQ](#) if you don't find what you're looking for.

Check out all of our small business content on [Small business help & learning](#).

Check out [Microsoft 365 small business help](#) on YouTube.

Before you begin

To add, modify, or remove domains, you **must** be a **Domain Name Administrator** of a [business or enterprise plan](#). These changes affect the whole tenant; *Customized administrators* or *regular users* can't make these changes.

Tip

If you need help with the steps in this topic, consider [working with a Microsoft small business specialist](#). With Business Assist, you and your employees get around-the-clock access to small business specialists as you grow your business, from onboarding to everyday use.

Watch: Add a domain

Check out this video and others on our [YouTube channel](#).

<https://www.microsoft.com/en-us/videoplayer/embed/RE4dN8c?autoplay=false&postJsIMsg=true>

Your company might need multiple domain names for different purposes. For example, you might want to add a different spelling of your company name because customers are already using it and their communications failed to reach you.

Where possible, we recommend that your organization use a custom domain name, as it can enhance your email's appearance and improve its reputation.

Tip

Where possible, we recommend that your organization use a custom domain name, as it can enhance your email's appearance and improve its reputation.

1. In the Microsoft 365 admin center, choose [Setup](#).
2. Select **Get your custom domain set up**, then **Get Started > Add domain**.
3. Enter the new domain name that you want to add, and then select **Next**.
4. Sign in to your domain registrar, and then select **Next**.
5. Choose the services for your new domain.
6. Select **Next > Authorize > Next**, and then **Finish**. Your new domain is added.

Add a domain

Follow these steps to add, set up, or continue setting up a domain.

1. Go to the admin center at <https://portal.partner.microsoftonline.cn>.
2. Go to the **Settings > Domains** page.
3. Select **Add domain**.
4. Enter the name of the domain you want to add, then select **Next**.
5. Choose how you want to verify that you own the domain.
 - a. If your domain registrar uses **Domain Connect**, Microsoft [will set up your records automatically](#) by having you sign in to your registrar and confirm the connection to Microsoft 365. You are returned to the admin center and Microsoft automatically verifies your domain.
 - b. You can use a TXT record to verify your domain. Select this and select **Next** to see instructions for how to add this DNS record to your registrar's website. It can take up to 10 minutes to verify after you add the record although some DNS hosting providers require up to 48 hours.
 - c. You can add a text file to your domain's website. **Select** and download the .txt file from the setup wizard, then **upload** the file to your website's top level folder. The path to the file should look similar to: `http://mydomain.com/ms39978200.txt`. We confirm you own the domain by finding the file on your website.
6. Choose how you want to make the DNS changes required for Microsoft to use your domain.
 - a. Choose **Add the DNS records for me** if your registrar supports **Domain Connect**, and Microsoft [will set up your records automatically](#) by having you sign in to your registrar and confirm the connection to Microsoft 365.

- b. Choose **I'll add the DNS records myself** if you want to attach only specific Microsoft 365 services to your domain or if you want to skip it for now and do this later. **Choose this option if you know exactly what you're doing.**
7. If you chose to *add DNS records yourself*, select **Next** and you see a page with all the records that you need to add to your registrars website to set up your domain.
If the portal doesn't recognize your registrar, you can [follow these general instructions](#).
If you don't know the DNS hosting provider or domain registrar for your domain, see [Find your domain registrar or DNS hosting provider](#).
If you want to wait for later, either unselect all the services and select **Continue**, or in the previous domain connection step, choose **More Options** and select **Skip this for now**.
8. Select **Finish** - you're done!

Add or edit custom DNS records

Follow these steps to add a custom record for a website or third party service.

1. Sign in to the [Microsoft 365 admin center](#).
2. Go to the **Settings > Domains** page.
3. On the **Domains** page, select a domain.
4. Under **DNS records**, select **Custom Records**; then select **Add record**.
5. Select the type of DNS record you want to add and type the information for the new record.
6. Select **Save**.

Registrars with Domain Connect

[Domain Connect](#) enabled registrars let you add your domain to Microsoft 365 in a three-step process that takes minutes.

In the wizard, we confirm that you own the domain, and then automatically set up your domain's records, so that email comes to Microsoft 365 and other Microsoft 365 services, like Teams, work with your domain.

Note

Make sure you disable any popup blockers in your browser before you start the setup wizard.

Domain Connect registrars integrating with Microsoft 365

- [Aruba.it ↗](#)
- [IONOS ↗](#)
- [EuroDNS ↗](#)
- [Cloudflare ↗](#)
- [GoDaddy \(*Media Temple*\) ↗](#)
- [WordPress.com ↗](#)
- [Plesk ↗](#)
- SecureServer or WildWestDomains (GoDaddy resellers using SecureServer DNS hosting)
 - Examples:
 - [DomainsPricedRight ↗](#)
 - [DomainRightNow ↗](#)

What happens to my email and website?

After you finish setup, the MX record for your domain is updated to point to Microsoft 365 and all email for your domain will start coming to Microsoft 365. Make sure you add users and set up mailboxes in Microsoft 365 for everyone who gets email on your domain!

If you have a website that you use with your business, it keeps working where it is. The Domain Connect setup steps don't affect your website.

Add an `onmicrosoft.com` domain

Each Microsoft 365 organization can have up to five `onmicrosoft.com` domains.

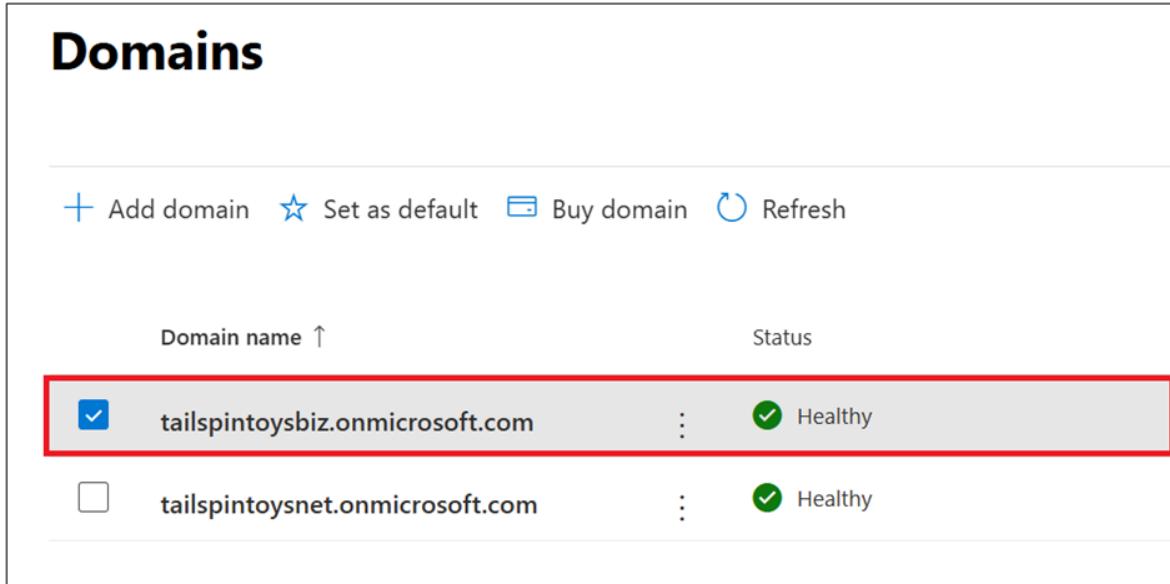
Note

You must be a Domain Name admin to add a domain. Creating an additional `.onmicrosoft` domain and using it as your default will not do a rename for SharePoint Online. To make changes to your `.onmicrosoft` SharePoint domain you would need to use the [SharePoint domain rename preview](#) (currently available to

any tenant with less than 10,000 sites). If you're using Microsoft 365 mail services, removal of your initial .onmicrosoft domain is not supported.

To add an onmicrosoft.com domain:

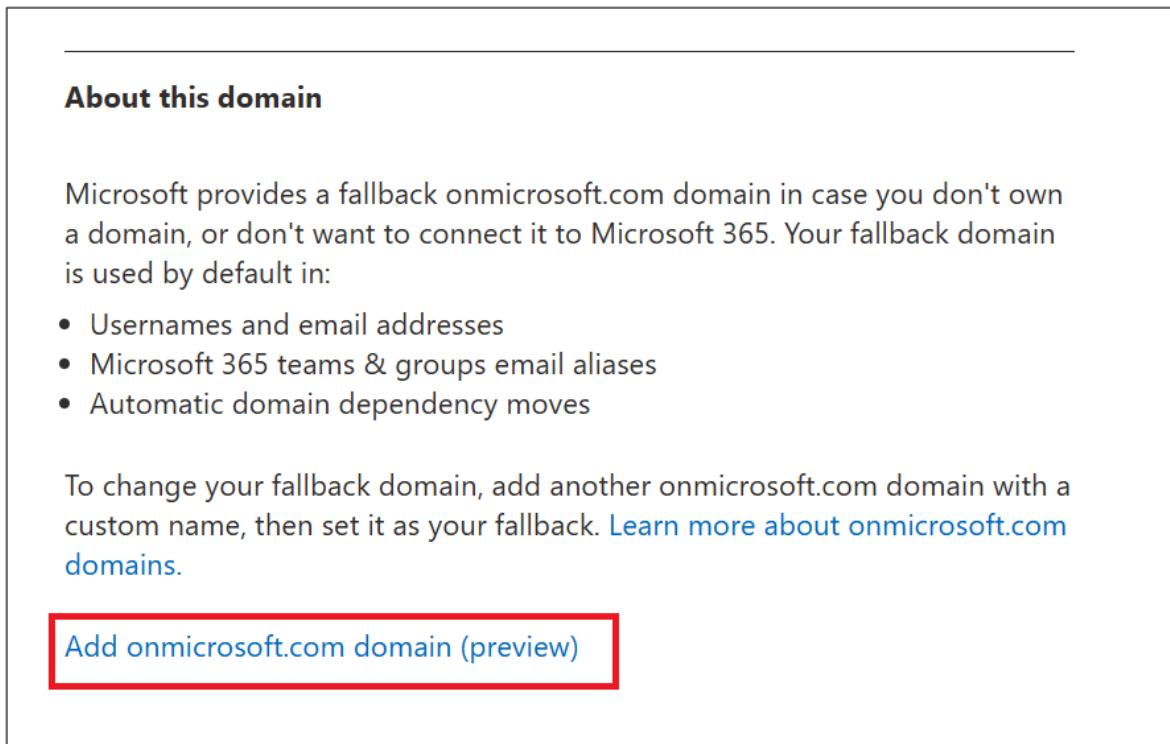
1. In the Microsoft 365 admin center, select **Settings**, and then select **Domains** ↗.
2. Select an existing *.onmicrosoft.com* domain.



The screenshot shows the Microsoft 365 Domains page. At the top, there are buttons for '+ Add domain', 'Set as default', 'Buy domain', and 'Refresh'. Below this is a table with two rows. The first row, containing 'tailspintoybiz.onmicrosoft.com', has a checked checkbox in the first column and a green checkmark in the 'Status' column. The second row, containing 'tailspintoysnet.onmicrosoft.com', has an unchecked checkbox in the first column and a green checkmark in the 'Status' column. A red box highlights the first row.

Domain name ↑		Status
<input checked="" type="checkbox"/>	tailspintoybiz.onmicrosoft.com	: ✓ Healthy
<input type="checkbox"/>	tailspintoysnet.onmicrosoft.com	: ✓ Healthy

3. On the **Overview** tab, select **Add onmicrosoft.com domain**.



The screenshot shows the Microsoft 365 Overview page. Under the 'About this domain' section, it says: 'Microsoft provides a fallback onmicrosoft.com domain in case you don't own a domain, or don't want to connect it to Microsoft 365. Your fallback domain is used by default in:' followed by a bulleted list: '• Usernames and email addresses', '• Microsoft 365 teams & groups email aliases', and '• Automatic domain dependency moves'. Below this, it says: 'To change your fallback domain, add another onmicrosoft.com domain with a custom name, then set it as your fallback. [Learn more about onmicrosoft.com domains](#)'. At the bottom, there is a red-bordered button labeled 'Add onmicrosoft.com domain (preview)'.

4. On the **Add onmicrosoft domain** page, in the **Domain name** box, enter the name for your new onmicrosoft.com domain.

Add an onmicrosoft.com domain (preview)

Use your organization's name or brand to customize a new onmicrosoft.com domain. After it's added, you can make it your fallback domain instead of M365B309532.onmicrosoft.com.

i This domain can't be removed after it's added. Make sure the spelling is correct before you add the domain, as you can only have 5 total onmicrosoft.com domains.

Domain name *

tailspintosbiz

onmicrosoft.com

! Note

Make sure to verify the spelling and accuracy of the domain name you entered. You are limited to five onmicrosoft.com domains, and currently they cannot be deleted once they are created.

5. Select **Add domain**. When successfully added, you'll see a message stating this.

Add an onmicrosoft.com domain (preview)

✓ Domain added. [Go to the new domain](#) to make tailspintosbiz.onmicrosoft.com your fallback.

You can set any domain you own as your default domain.

For more information on how to add an onmicrosoft.com domain, see [Add or replace your onmicrosoft.com domain](#).

Related content

[Domains FAQ](#) (article)

[What is a domain?](#) (article)

[Buy a domain name in Microsoft 365](#) (article)

[Add DNS records to connect your domain \(article\)](#)

[Change nameservers to set up Microsoft 365 with any domain registrar \(article\)](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Microsoft 365 network health status

Article • 06/28/2024

Due to the increased demand for Microsoft's cloud services during the COVID-19 crisis, we're providing information about the health of Microsoft's global network and information about network quality issues that our customers might experience but that we don't control.

This information includes network issues that affect all of our software as service offerings, including Microsoft 365.

There might be delays in the updates to this page. We're updating it manually while we build a more automated solution.

When we detect significant issues within Microsoft's global network or with internet connectivity between our customers and Microsoft's network, we'll post that information here. We recommend that customers continue to use the Microsoft 365 admin center [Service Health dashboard](#) to understand the impact of any significant network issues on their tenant, as we provide much more detailed and targeted information there.

Current network issues

[] [Expand table](#)

Location	Issue Type	Detail
No current issues		

Recommendations to improve network experience

Use these resources to improve your network utilization for Microsoft services.

- [Optimize Microsoft 365 connectivity for remote users using VPN split tunneling](#)
- [Microsoft 365 principles of network connectivity](#)
- [Working remotely using Azure Networking services](#)

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Learn about Microsoft 365 monitoring

Article • 03/21/2024

You can use dashboards in the [Microsoft 365 admin center](#) to monitor the health of various Microsoft services for your organization's Microsoft 365 subscription. This capability began with Exchange Online and has been expanded to other Microsoft services such as Microsoft Teams and Microsoft 365 Apps, with more services being added in the future.

Microsoft 365 Monitoring increases observability and minimizes downtime through providing near real-time user telemetry data with enriched alerts in the Microsoft 365 admin center's Service Health dashboard.

Monitoring provides you with information about incidents and advisories that are collected in these categories:

- **Infrastructure.** Issue is detected in the Microsoft 365 infrastructure that Microsoft owns for providing regular updates and resolving the issue. For example, users can't access Exchange Online because of issues with Exchange or other Microsoft 365 cloud infrastructure.
- **Third-party infrastructure.** Issue is detected in third-party infrastructure on which your organization has taken a dependency and requires action from your organization for resolution. For example, user authentication transactions are getting throttled by a third-party security token service (STS) provider that prevents users from connecting to Exchange Online.
- **Customer infrastructure.** Issue is detected in your organization's infrastructure and requires action from your organization for resolution. For example, users can't access Exchange Online because they're unable to obtain an authentication token from STS provider hosted by your organization because of an expired certificate.

Here's an example of the **Service health** page in the Microsoft 365 admin center, which is available at **Health > Service health** for organization scenarios and [priority account](#) scenarios.

The screenshot shows the Microsoft 365 admin center interface. On the left, there's a navigation sidebar with various options like Home, Users, Devices, etc. The main content area has two sections: 'Active issues' and 'Microsoft service health'. The 'Active issues' section lists several items with columns for Issue title, Affected service, Issue type, Status, and Updated. The 'Microsoft service health' section shows the status of different services (Exchange Online, Microsoft 365 Defender, Microsoft Teams, SharePoint Online, Azure Information Protection, Dynamics 365 Apps) with a 'View' link next to each. A red box highlights the 'View' link for Exchange Online.

If Microsoft 365 monitoring discovers issues that need your attention, these are shown under the **Issues in your environment that require action** in the Active Issues section of the page.

To access detailed monitoring pages for specific services, select **View** under **Organizational-level monitoring** on the service health page.

Here's an example of the Exchange Online monitoring page in the Microsoft 365 admin center that shows the health of organization-level and priority account scenarios available from **Health > Service health > Exchange Online**.

The screenshot shows the Exchange Online monitoring page. It has a header with 'Scenarios' and 'Active issues'. Below is a table titled 'Organization scenarios' with columns for App and activities, Health, Action required, Activity (last 30 min), and Change in activity (last 7 days). Each row represents a different scenario like App connectivity, Basic authentication, etc., with a green 'Healthy' status icon.

App and activities	Health	Action required	Activity (last 30 min)	Change in activity (last 7 days)
App connectivity	Healthy	No	99.581% estimated connectivity	0% change
Basic authentication	Healthy	No	25 authentications	+32% change
Desktop mail apps	Healthy	No	30,524 users read mail	+5% change
iOS and Android mail apps	Healthy	No	3,520 users read mail	+4% change
Mail delivery	Healthy	No	659,528 messages delivered	-14% change
Modern authentication	Healthy	No	12,329 authentications	+28% change
Open Outlook on the web	Healthy	No	228 users opened app	-57% change
Outlook apps for Mac	Healthy	No	939 users read mail	+28% change
Outlook apps for mobile	Healthy	No	6,389 users read mail	-6% change
Outlook on the web	Healthy	No		

With the scenario list page, you can see whether the Microsoft service is healthy or not and whether there are any associated incidents or advisories. For example, with

Exchange Online monitoring, you can look at the service health for specific email scenarios and view near real-time signals to determine the impact by organization-level scenario. You can also see health of priority account scenarios, if available.

Requirements for monitoring

This preview is enabled for customers who meet the following requirements:

- Your organization needs to have a license count of at least 5,000 from one or a combination of these products: Office 365 E3, Microsoft 365 E3, Office 365 E5, or Microsoft 365 E5.

For example, your organization can have 3,000 Office 365 E3 licenses and 2,500 Microsoft 365 E5, for a total of 5,500 licenses from the qualifying products.

- Your organization needs to have at least 50 monthly active users for one or more core Microsoft 365 services, which include Microsoft Teams, OneDrive for Business, SharePoint Online, Exchange Online, and Office apps.
- Any role with Service Health Dashboard level permissions can access Exchange Online Monitoring. For more information, see [How to check Microsoft 365 service health](#).

Additional monitoring for Microsoft services

Service-specific monitoring is also enable for the following Microsoft services. Select the corresponding link to learn more about monitoring for that service.

- [Exchange Online](#)
- [Microsoft 365 Apps](#)
- [Microsoft Teams](#)

Send us feedback

There are two ways you can provide feedback:

- Use the **Give feedback** option available on every page of the Microsoft 365 admin center.
- Submit feedback using the **Is this post helpful? link for a specific incident or advisory.

Users unable to send emails

EXT43260, Exchange Online, Last updated: December 19, 2016 6:00 AM
Start time: May 18, 2016 2:02 AM

Status

Service interruption

Issue type

 Incident

Issue origin

Microsoft

User impact

A large number of customers appear to be impacted by this event. We've received a few isolated customer reports of this issue.

[Are you experiencing this issue?](#)

[Is this post helpful?](#)

Latest message, July 8, 2016 2:05 AM [View history](#)

The Office 365 Suite team is investigating a possible issue impacting acquisition of data from blog sources. If this is affecting you, we apologize for the inconvenience.
Message 2.

Frequently asked questions

1. Why don't I see "view" link under Organizational monitoring column in the Microsoft 365 admin center inside Service Health?

First, make sure you've enabled the new admin center on the [Home](#) page of the [Microsoft 365 admin center](#).

Then make sure you meet both of the following requirements:

- Your organization needs to have a license count of at least 5,000, from one or a combination of these products: Office 365 E3, Microsoft 365 E3, Office 365 E5, or Microsoft 365 E5.

- Your organization needs to have at least 50 monthly active users for one or more core Microsoft 365 services, which include Microsoft Teams, OneDrive, SharePoint, Exchange Online, and Office apps.

If the license count for your organization falls below 5,000 users and the monthly active users falls below 50 users in the core services, Exchange Online monitoring won't be enabled until these requirements are met.

2. Will there be other monitoring scenarios for other services in future?

Yes. We have a few more services in public preview now. We'll continue to work on expanding the footprint to other services.

3. What is the plan for general availability of this experience?

Microsoft's plan is to collect your feedback on the preview experience and then define our plan for general availability.

4. Is this a free (included) or paid (extra) feature?

Microsoft 365 Monitoring features are in preview for eligible customers. While in preview, this feature is available at no additional charge for customers that meet the eligibility requirements.

5. How do I provide feedback?

For general feedback, use the **Give feedback** icon on the bottom-right corner of the monitoring page.

For feedback on incidents or advisories, use the **Is this post helpful?** link.

6. Are there any privacy concerns?

Monitoring focuses on service metadata and user content isn't monitored.

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Exchange Online monitoring for Microsoft 365

Article • 04/12/2024

Exchange Online monitoring supports the following organization-level scenarios:

- **Email clients:** You can view the health for the following email clients based on email read activity:
 - Outlook desktop
 - Outlook on the web
 - Native mail clients of iOS and Android
 - Outlook Mobile app in iOS and Android
 - Outlook Mac client

For these clients, you can see the number of active users in the last 30 minutes based on users reading an email, along with number of incidents and advisories in the dashboard. This data is compared to the same interval for the previous week to see if there's an issue.

⚠ Note

Active user count is measured by a single activity, for example, when a user reads an email. It only accounts for the last 30 minutes of activity.

- **App connectivity:** Estimated connectivity is based on the percentage of successful, synthetic connections between your organization's devices and Exchange Online, and might include issues outside of Microsoft's control. To learn more, see [Microsoft 365 Connectivity Optics](#).
- **Basic Authentication and Modern Authentication:** The number of users successfully validated in the Exchange Online service.
- **Mail flow:** The number of messages successfully delivered to a mailbox without any delay after the message reached the Microsoft 365 network.
- **Open Outlook for the Web:** The number of users successfully signed in and started Outlook on the web.

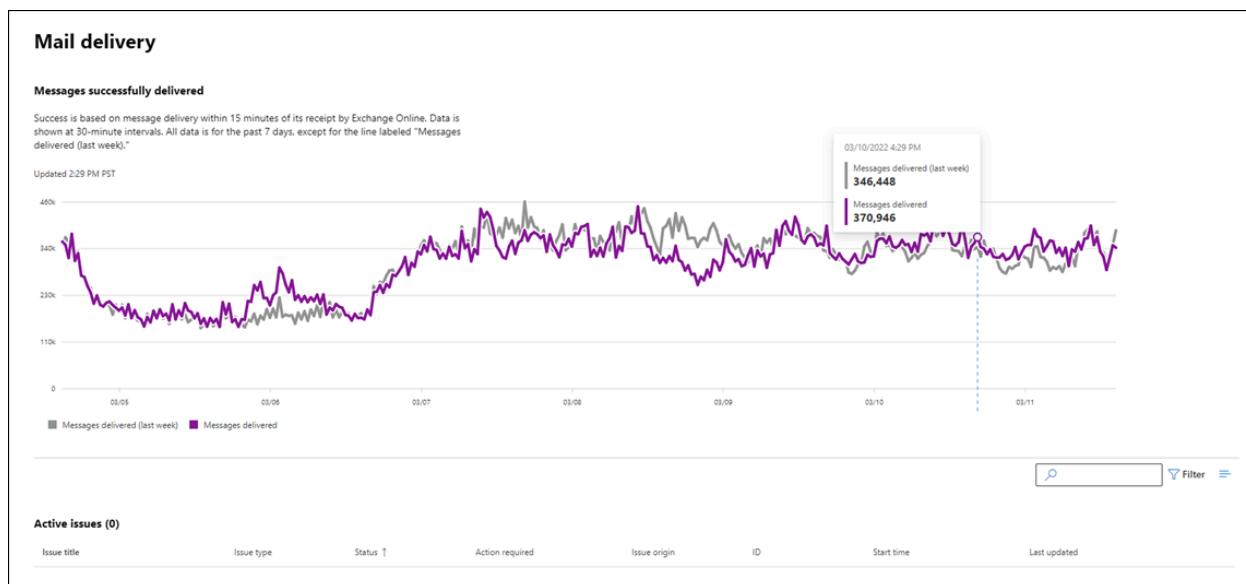
Here's an example of the organization-level scenarios for Exchange Online in the main dashboard.

Exchange Online

We monitor Exchange Online for Microsoft 365 service issues, as well as infrastructure and third-party software issues that might require your action.

Scenarios	Active issues			
Organization scenarios				
App and activities				
App connectivity	Health ↑	Action required	Activity (last 30 min)	Change in activity (last 7 days)
Basic authentication	Healthy	No	99.581% estimated connectivity	0% change
Desktop mail apps	Healthy	No	25 authentications	+32% change
iOS and Android mail apps	Healthy	No	30,524 users read mail	+5% change
Mail delivery	Healthy	No	3,520 users read mail	+4% change
Modern authentication	Healthy	No	659,528 messages delivered	+14% change
Open Outlook on the web	Healthy	No	12,329 authentications	+28% change
Outlook apps for Mac	Healthy	No	228 users opened app	-57% change
Outlook apps for mobile	Healthy	No	939 users read mail	+28% change
Outlook on the web	Healthy	No	6,389 users read mail	-6% change
Outlook on the web	Healthy	No		

For these scenarios, the key numbers are for the last 30 minutes in the main dashboard. Detailed views for each of these scenarios show the near real-time trend for seven days with the 30-minute aggregate compared with the previous week.



You'll notice incidents or advisories created for your organization with "Issue origin" in the communication tagged as "Your org." These are notifications individually targeted to your organization with issues that require your attention for mitigation and resolution. For more information about various types of issues that are created and communicated in service health to inform your organization about the potential impact, see the following articles:

- [Service alerts for mailbox utilization](#)
- [Service alerts for MRS source delays](#)
- [Service alerts for messages pending delivery to external recipients](#)

Priority accounts monitoring scenarios

With Exchange Online priority account monitoring, you can view the health for the following scenarios after configuring [priority accounts](#):

- Exchange licensing
- Mailbox storage
- Message limit
- Subfolders per folder
- Folder hierarchy
- Recoverable items

The Exchange licensing scenario checks if the priority account isn't able to sign in due to invalid license issues, which can be addressed by the tenant admin.

The remaining five scenarios check if your priority account's mailbox is close to reaching or has reached the limits described in [Exchange Online limits](#).

For these scenarios, you can see active and resolved advisories and incidents affecting your priority accounts. Identifiable information for the priority accounts will be displayed in the advisory or incident details along with recommendations. Here's an example from the page at [Health > Service health > Exchange Online](#).

Priority account scenarios		
App and activities	Health ↑	Action required
Exchange licensing	✓ Healthy	No
Folder hierarchy	✓ Healthy	No
Mailbox storage	✓ Healthy	No
Message limit	✓ Healthy	No
Recoverable items	✓ Healthy	No
Subfolders per folder	✓ Healthy	No

In the affected account pane, the **Status** column has these values:

- Fixed: The issue causing the advisory or incident has been addressed for the priority account. There's no longer an issue.

- Active: The issue causing the advisory or incident is ongoing for the priority account. The issue remains.
- Delayed: The issue causing the advisory or incident hasn't been addressed for the priority account in 96 hours, so it's suspended. The issue remains.

Here's an example.

The screenshot shows the Microsoft 365 Admin Center Mailbox storage dashboard. On the left, under 'All active issues (1)', there is one item: 'Mailbox storage quota limit above threshold' (Incident, Service interruption, Yes, Your org, EXO). Under 'Resolved issues, past 7 days (1)', there is one item: 'Mailboxes over storage limit' (Incident, Service restored, Your org, EXO). On the right, under 'N affected accounts' (Incident: Mailboxes over storage limit), there is a table:

Display name	Username	Status	Usage
Michael Scott	michaelscott@contoso.com	Active	100%
Dwight Schrute	dwightschrute@contoso.com	Fixed	100%
Jane Doe	janedoe@contoso.com	Delayed	100%

An advisory or incident will be resolved after no accounts remain in the **Active** state.

Frequently asked questions

1. The active user count in the dashboard for each client appears to be low. We have numerous active licenses assigned to users. What does this mean?

The active user count shown in monitoring is based on a 30-minute window where users have performed the activity called out in the feature. This shouldn't be confused with usage numbers. To view usage numbers, use activity reports in the Microsoft 365 admin center ([Reports > Usage](#)).

2. Where is the data instrumented for the scenarios that show activity trends?

The data is instrumented in the Exchange Online service. If there's a failure that happens before the request reaches Exchange Online or there's a failure in Exchange Online, you'll see a drop in the activity signal.

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Messages Pending Delivery to External Recipients Outside of Exchange Online

Article • 08/02/2024

This advisory informs you of mail queuing to external recipients outside of Exchange Online. Many of these advisories require actions outside of Microsoft and provide administrators with the information needed to remediate.

These advisories are displayed in the Microsoft 365 admin center. To view these advisories, go to [Health > Service health](#) > [Exchange Online](#) and then select the **Active issues** tab. The name for these service alerts is "Message Queueing to External Recipients Above Thresholds".

Exchange Online

We monitor Exchange Online for Microsoft 365 service issues, as well as infrastructure and third-party software issues that might require your action.

Scenarios [Active issues](#)

3 items [Filter](#) [≡](#)

Issue title	Issue type ↑	Status	Action required	Issue origin	ID
Message Queueing To External Recipients Ab...	● Advisory	Investigating	Yes	Your org	EX334064

When you double-click the service alert, a flyout page similar to the following is displayed.

Message Queueing To External Recipients Above Thresholds

EX334064, Exchange Online, Last updated: February 18, 2022 7:05 AM

Estimated start time: February 18, 2022 6:54 AM

Issue type

- Advisory

Issue origin

Your org

Status

Investigating

[Manage notifications for this issue](#)

User impact

Message delivery to recipients outside Exchange Online may be delayed.

Action needed

Ensure network devices and messaging solutions associated with the referenced endpoint are healthy.

Additional diagnostics

messages for tenant **Contoso** are pending delivery to [192.64.119.121]. Messages report SMTP error code 450 4.4.316 Connection refused [Message=Socket error code 10061] [LastAttemptedServerName=192.64.119.121] [LastAttemptedIP=192.64.119.121:25] [CD1PEPF00001326.namprd00.prod.outlook.com].

[Are you experiencing this issue?](#)

What do these service advisories indicate?

This service advisory informs you of messages destined to recipients outside Exchange Online might be delayed. Queueing might be caused by your on-premises environment or third-party messaging\journaling solution. Reasons for queueing might be, but aren't limited to:

- DNS changes
- Excessive sending rates
- MTA\journaling solutions with low to no free disk space

- Certificate issues

Each service advisory contains high level recommendations for administrators in remediating the issue. We also provide the number of messages queued at the time of alert, the domain where the messages are queued to, and the SMTP error code associated with most messages.

For more information for determining the root cause for these service alerts, see [Mail flow intelligence in Exchange Online](#). This article also includes suggested actions to fix the root cause.

 **Note**

As Microsoft cannot account for every SMTP error code provided by third-party vendors, administrators may be required to investigate these errors codes specific to their Message Transfer Agent (MTA) or journaling solutions.

More information

If your organization has recently created or changed mail flow connectors in your on-premises or Exchange Online organization, see the following articles for more information.

- [Queued messages report in the new EAC in Exchange Online](#)
- [Mail flow insights in the EAC](#)
- [Trace an email message in Exchange Online](#)
- [Configure mail flow using connectors in Exchange Online](#)
- [Set up connectors to route mail](#)
- [Mail flow best practices](#)
- [Mail flow reports in the EAC](#)
- [Queued messages report in the EAC](#)

Feedback

Was this page helpful?

 Yes

 No

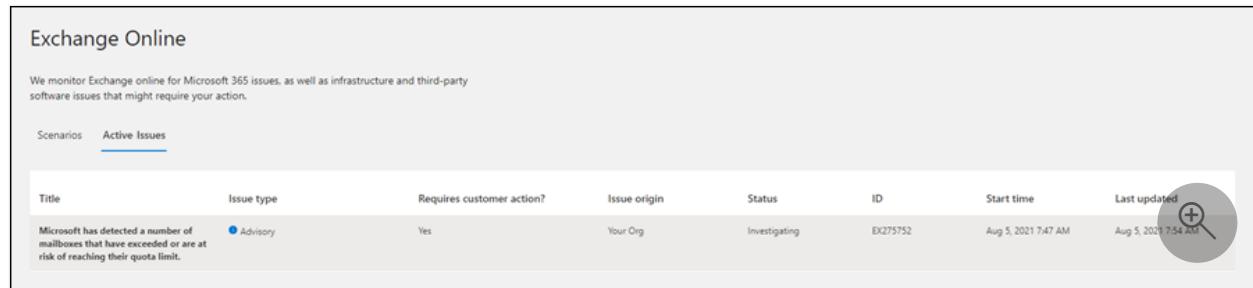
Provide product feedback ↗

Service advisories for mailbox utilization in Exchange Online monitoring

Article • 02/20/2024

An Exchange Online service advisory informs you about mailboxes that are on hold and at risk of reaching or exceeding their quota. These service advisories provide visibility to the number of mailboxes in your organization that might require admin intervention.

These service advisories are displayed in the Microsoft 365 admin center. To view these service advisories, you can go to **Health > Service health > Exchange Online** and then look for **Mailbox Storage Limits under the Organization Scenarios**, or you can go **Health > Service health > Exchange Online** and select the **Active issues** tab. Here's an example of a mailbox utilization service advisory under active issues.



The screenshot shows the Microsoft 365 admin center interface for Exchange Online. At the top, there's a header with the title 'Exchange Online'. Below it, a message states: 'We monitor Exchange online for Microsoft 365 issues, as well as infrastructure and third-party software issues that might require your action.' There are two tabs: 'Scenarios' and 'Active Issues', with 'Active Issues' being the active tab. A table below lists one active issue:

Title	Issue type	Requires customer action?	Issue origin	Status	ID	Start time	Last updated
Microsoft has detected a number of mailboxes that have exceeded or are at risk of reaching their quota limit.	Advisory	Yes	Your Org	Investigating	EX275752	Aug 5, 2021 7:47 AM	Aug 5, 2021 7:54 AM

A circular icon with a plus sign and a magnifying glass is located in the bottom right corner of the table row.

When you access the service advisory, you see a link under **User Impact**. Selecting that link opens a flyout window that lists affected mailbox GUIDs for your tenant. This list is limited to no more than 155 mailboxes.

[←](#) [? Back mode](#) [X](#)

155 affected mailboxes

Advisory: Microsoft has detected a number of mailboxes that have exceeded or are at risk of reaching their quota limit.

Affected Mailboxes

[View more about Service Health](#)

[Export](#) 155 items [☰](#)

Guid	Type ↓	Quota Status
f8b3e52b-47ad-4aad-bb...	PrimaryWithArchive	ProhibitSendReceiveQuota_Warning
fc30c12d-92d8-456f-a47...	Primary	ProhibitSendReceiveQuota_Warning
fb6e9969-f69a-4a10-96...	Primary	ProhibitSendReceiveQuota_Warning
f752b058-d0f7-4a91-84...	Primary	ProhibitSendReceiveQuota_Warning
f7fe478f-31b2-4e9e-872...	Primary	RecoverableItemsQuota_Warning
f38d41bf-fae0-42ce-86c...	Primary	RecoverableItemsQuota_Critical
f4242613-0517-49e7-a5...	Primary	ProhibitSendReceiveQuota_Warning
eea38db0-cd80-4352-a1...	Primary	RecoverableItemsQuota_Warning
fb660143-125d-431b-99...	Primary	ProhibitSendReceiveQuota_Warning
e9c2b68f-c969-4b91-b7...	Primary	RecoverableItemsQuota_Warning
fd902c78-5d5f-41a7-97f...	Primary	RecoverableItemsQuota_Critical
e2ea9cda-183b-438d-9d...	Primary	RecoverableItemsQuota_Critical

If your tenant exceeds more than 155 mailboxes at or nearing their storage quota, visit your admin portal and access your mailbox usage report. Alternatively, the direct URL to the mailbox usage report is <https://admin.microsoft.com/Adminportal/Home?source=applauncher#/reportsUsage/MailboxUsage>.

Note

The mailbox usage report information could be 24 hours behind your mailbox utilization service advisory alert.

What do these service advisories indicate?

The service advisories for mailbox utilization inform admins about mailboxes on hold that are nearing the mailbox storage quota. The type of holds that can be placed on mailboxes include Litigation holds, eDiscovery hold, and Microsoft 365 retention policies (that are configured to retain data). When a mailbox is on hold, users (or automated processes) can't permanently remove data from their mailbox. Instead, admins should configure Messaging Records Management (MRM) retention policies in Exchange Online (in line with their organization's compliance policies related to data retention) to move data from a user's primary mailbox to their archive mailbox.

If a mailbox on hold doesn't have an archive and reaches a critical or warning state, admins should [enable archive mailboxes](#) and [enable auto-expanding archiving](#). Make sure the retention period for the archive policy assigned to the mailbox (which moves email from the primary mailbox to the archive mailbox) only retains data in the main mailbox for as long as needed. If nothing is done to resolve the quota issues identified by the mailbox utilization service advisory, users might not be able to send or receive email messages or meeting invites.

Mailboxes on hold without an archive

If a mailbox is on hold and is nearing or has reached its quota and doesn't have an archive, an admin can [enable an archive mailbox](#) (and potentially [enable auto-expanding archiving](#)) along with ensuring an MRM archive policy is applied to the mailbox. (An MRM archive policy is a retention policy in Exchange Online that moves items to the archive mailbox.) For more information about how holds interact with quotas and recommended quota sizes for the main mailbox and Recoverable Items folder, see [Increase the Recoverable Items quota for mailboxes on hold](#).

Mailboxes on hold with an archive

If a mailbox is on hold, has an archive, and is nearing or has reached its Recoverable Items Quota, an admin can increase the quota for the Recoverable Items folder. For more information, see [Increase the Recoverable Items quota for mailboxes on hold](#).

If an admin increases the Recoverable Items Quota, they should also make sure that an MRM archive policy that moves items to the archive mailbox is applied to the mailboxes. The retention period for the archive policy must be short enough so that items aren't retained too long in the primary mailbox before they're moved to the archive.

 **Note**

MRM archive policies also move items from the Recoverable Items folder in the primary mailbox to the Recoverable Items folder in the corresponding archive mailbox. This capability helps prevent the mailbox from exceeding the quota for the Recoverable Items quota.

MRM retention policies in your organization

Archive retention policies can be configured in various ways, depending on your organization's needs. For detailed information about retention policies, see [Retention tags and retention policies in Exchange Online](#). An admin can view existing retention policies by running the following command:

PowerShell

```
Get-RetentionPolicy | FL
```

Retention policies can be applied to and take different actions on mailboxes with or without archives. The following is a brief overview of common archive retention policy actions:

- MovePrimaryToArchive and MoveDumpsterToArchive instruct the retention policy to move the contents of the main mailbox, or Recoverable Items folder respectively, to the mailbox's archive once the policy's conditions have been met. These tags are set by admins and apply regardless of a user's individual settings.
 - The retention policy applied to moving Recoverable Items content should be relatively short to ensure the user's primary mailbox doesn't reach its Recoverable Items quota.
- A Personal Archive tag means this policy can be applied by users to their personal folders to archive content on the specified schedule.

MRM retention policies don't function as expected

Administrators possess the necessary tools to evaluate the cause of a nonfunctional retention policy and address any errors. Some common scenarios of failure include the policy not being correctly applied or failure to process a mailbox.

For information on troubleshooting retention policies, see [Troubleshooting Retention Policies in Exchange Online](#).

How often will I see these service advisories?

If you don't resolve the quota issues, you can expect to see this type of service advisory every seven days. Subsequent service advisories might contain higher mailbox counts for other mailboxes that are nearing their quota. If you resolve quota issues, this service advisory only occurs when another mailbox with quota issues is identified.

More information

- For information about troubleshooting and resolving archive mailbox issues, see [Microsoft Purview troubleshooting](#).
 - For guidance about identifying the holds placed on a mailbox, see [How to identify the type of hold placed on a mailbox](#).
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) 

Service advisories for auto-expanding archive utilization in Exchange Online monitoring

Article • 08/08/2024

We released a new Exchange Online service advisory that informs you of auto-expanding archives attached to mailboxes at risk of reaching the 1.5TB limit on total auto-expanding archive size. These service advisories provide visibility to the mailboxes in your organization that can require admin intervention.

These service advisories are displayed in the Microsoft 365 admin center. To view these service advisories, go to **Health > Service health > Exchange Online** and then select the **Active issues** tab.

What do these service advisories indicate?

This service advisory informs you of potential data storage limits being reached in your organization. Mailboxes with archive mailboxes that have the auto-expanding archive feature enabled can store a maximum of 1.5 TB of data in the auto-expanding archive. The service advisory contains a link under "User Impact" that shows a flyout window listing impacted mailbox Globally Unique Identifiers (GUIDs) for your tenant.

Auto-expanding archive mailbox(es) in your tenant are approaching or have exceeded the 1.5 TB limit

EX64087, Last updated: March 21, 2023 8:21 PM

Estimated start time: March 21, 2023 8:21 PM

Affected services

Exchange Online

Filter 

Issue type

Advisory

Issue origin

Microsoft

Status

Investigating

[Manage notifications for this issue](#)

Microsoft

EX64087

User impact

No further data will be archived and end users may not be able to send or receive email messages or meeting invites.

[View 175 affected mailboxes](#)



Here's an example of the flyout:

Auto-Expanding Archive:



175 affected mailboxes

Advisory: Auto-expanding archive mailbox(es) in your tenant are approaching or have exceeded the 1.5 TB limit

Affected Mailboxes

 Export

175 items



Guid

Status ↑

Size in GB

085ce318-[REDACTED] Critical 1643

001caa27-[REDACTED] Critical 1441

055825ed-[REDACTED] Critical 1486



The following list describes each column in the previous example.

- **mailboxGuid** : The GUID of the main archive for the mailbox or one of the other storage units in the auxiliary archive ("AuxArchive").
- **Status** : *Warning* if the auto-expanding archive total size is over 1.2 TB but less than 1.4 TB; *Critical* if the auto-expanding archive total size is over 1.4TB.
- **SizeInGB** : The total size of the auto-expanding archive associated with the mailbox.

Identifying affected users

Use PowerShell to determine the user associated with the archive: `Get-Mailbox
yourtenantdomain.onmicrosoft.com\GUID-of-archive`

More information

For more information about auto-expanding archive limits and considerations, see the following articles:

- [Learn about auto-expanding archiving](#)
- [Customize an archive and deletion policy for mailboxes in your organization](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Service advisories for eDiscovery cmdlet exception spike in Exchange Online monitoring

Article • 07/25/2024

We've released a new Exchange Online service advisory that informs you regarding spike in eDiscovery cmdlet exceptions. The purpose of these advisories is to provide visibility into reasons behind user difficulties in submitting Compliance Search PowerShell cmdlets.

These service advisories are displayed in the Microsoft 365 admin center. To view these service advisories, go to **Health > Service health > Exchange Online**. Here's an example of eDiscovery service advisory.

We have detected compliance search query failures in your tenant due to invalid search criteria

EX66379, Last updated: July 12, 2023 at 2:12 PM PDT

Estimated start time: July 12, 2023 at 2:12 PM PDT

Affected services



Issue type



Issue origin

Your environment

Status

Investigating

[Manage notifications for this issue](#)

User impact

Admins will continue to see failed compliance searches unless corrections are made to the search criteria.

Action needed

In order to submit a successful query, please leverage the diagnostics provided to resolve the errors present in the search criteria.

Additional diagnostics

The cmdlet used to create the search query is invalid. Possible causes include:

- 1.Specified argument was out of the range of valid values.
- 2.Double quotation mark in the middle of string property value is not supported by KQL.
- 3.Please adjust the email type. Make sure the email type is supported.
- 4.There is an unexpected character in the query.
- 5.The query exceeds the number of keywords allowed for statistics, limit keyword list to 20.

For guidance on how to create a compliance search query, please reference: [New-ComplianceSearch \(ExchangePowerShell\) | Microsoft Learn](#)

For guidance on keyword queries and search conditions, please reference: [Keyword queries and search conditions for eDiscovery - Microsoft Purview \(compliance\) | Microsoft Learn](#)

[Are you experiencing this issue?](#)

What does this service advisory indicate?

The advisory informs administrators about the issue and its potential impact on eDiscovery operations. It highlights that users encounter errors when executing Compliance Search cmdlets due to invalid search queries which can hinder their ability to perform necessary eDiscovery tasks effectively.

For guidance on how to create a compliance search query, please reference: [New-ComplianceSearch \(ExchangePowerShell\) | Microsoft Learn](#)

For guidance on keyword queries and search conditions, please reference: [Keyword queries and search conditions for eDiscovery - Microsoft Purview \(compliance\) | Microsoft Learn](#)

How often will I see these service advisories?

Once the spike in eDiscovery cmdlet exceptions is resolved, the advisory will be updated accordingly or removed from the service health dashboard.

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Service advisories for eDiscovery throttling in Exchange Online monitoring

Article • 08/02/2024

We've released a new Exchange Online service advisory that informs you of eDiscovery being throttled. These service advisories provide visibility into the instances when the user is unable to submit Search and Export because of throttling.

These service advisories are displayed in the Microsoft 365 admin center. To view these service advisories, go to [Health | Service health](#) | Exchange Online. Here's an example of an eDiscovery service advisory.

The screenshot shows the Microsoft 365 Admin Center with the 'Service health' page open. In the top navigation bar, 'Home > Service health' is visible. Below the navigation, there are tabs for 'Overview', 'Issue history', and 'Reported issues', with 'Overview' being the active tab. A sub-header 'Service health' is present. On the left, a sidebar lists 'Active issues' under 'Microsoft service health' (7 items) and 'Issues in your environment that require action' (2 items). The main content area displays a detailed service advisory card for 'eDiscovery keyword searches and export jobs throttled in your tenant'. The card includes the ID 'EX443330', last updated time 'October 6, 2022 2:50 PM', and estimated start time 'October 6, 2022 2:50 PM'. It lists 'Affected services' as 'Exchange Online'. Under 'Issue type', it shows 'Advisory'. The 'Status' is 'Investigating'. There is a link 'Manage notifications for this issue'. The 'User impact' section notes that if action is not taken, eDiscovery keyword searches and export jobs may fail. The 'Action needed' section advises waiting for existing queries to complete before processing new ones. It also mentions ensuring users are operating within defined search limits. The 'Additional diagnostics' section links to 'Limits for eDiscovery search | Microsoft Docs'. At the bottom right of the card, there are links for 'Are you experiencing this issue?' and 'Is this post helpful?'. A footer at the bottom of the page says 'All updates' and shows the date 'October 6, 2022 2:50 PM'.

What does this service advisory indicate?

The service advisories for eDiscovery throttling inform admins about their tenant being throttled due to number of Search and Export jobs exceeding the limit set by Microsoft. Various limits are applied to eDiscovery search tools in the [Microsoft Purview](#) compliance portal. This includes searches run on the [Content Search](#) page and searches that are associated with an eDiscovery case on the [eDiscovery \(Standard\)](#) page. These limits help to maintain the health and quality of services provided to organizations. These advisories provide awareness so that you can take these limits into consideration when planning, running, and troubleshooting eDiscovery searches and exports.

For limits related to the Microsoft Purview eDiscovery (Standard) tool, see [Limits for Content search and eDiscovery \(Standard\) in the compliance center](#).

How often will I see these service advisories?

You can expect to see this type of advisory until the time where the Search and Export jobs are within the defined limit.

More information

- For information about troubleshooting and resolving eDiscovery compliance issues, see [Microsoft Purview troubleshooting](#).
- For information about Microsoft Purview, see [What is Microsoft Purview?](#)
- To learn more about Microsoft Purview eDiscovery solutions, see [Microsoft Purview eDiscovery solutions](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Service advisories for MRS source delays in Exchange Online monitoring

Article • 08/09/2024

Mailbox Replication Service (MRS) source delay service advisories inform you of storage limitations or high processor utilization issues on the tenant side (migration source) that might be delaying mailbox migrations in your Microsoft 365 organization. These service advisories also include links to Microsoft resources to help you resolve these issues.

These service advisories are displayed in the Microsoft 365 admin center. To view these service advisories, go to [Health > Service health](#) > [Exchange Online](#) and then click the [Active issues](#) tab.

What do these service advisories indicate?

This service advisory informs you of potential delays to mailbox migrations in your organization. This includes cross-forest migrations, onboarding migrations, and offboarding migrations. The service advisory contains a table with information about the current migrations in your organization. Here's an example of the table with information about migration delays.

[Expand table](#)

BatchGuid	ExchangeGuid	RequestGuid	DelayReason	QueuedHours	DelayInHours	SourceServer	RemoteDatabaseName
12345678-1234-1234-1234-1234567891011	246c21f7-ca3c-4bba-ab5d-1234567891011	3d7fab16-7d8e-4c81-a849-e0795054292a	DiskLatency	35.2	27.3	RD1GBL01EXCH003	GBL01EDAG001-db002
87654321-4321-4321-4321-1101987654321	21e9a608-78c3-44ef-a4dd-d5e7222aae82	9974aeb4-2aa4-4a2c-aeb6-d94d78cc25c9	DiskLatency	0.4	0.9	RD1GBL01EXCH010	GBL01EDAG010-db003

The following list describes each column in the previous example.

- **BatchGuid:** Unique GUID for the migration job.
- **ExchangeGuid:** The globally unique identifier (GUID) of the user mailbox that's being migrated.
- **RequestGuid:** The GUID of the migration request.
- **DelayReason:** The reason for the delayed migration.
- **QueueHours:** The duration the migration has been queued and waiting.
- **DelayInHours:** The duration the migration has been delayed.
- **SourceServer:** The on-premises server the migration originates from.
- **RemoteDatabaseName:** The database name the migration originates from.

More information

For more information about MRS and mailbox migrations, see the following articles:

- [Mailbox moves in Exchange](#)
- [Microsoft 365 and Office 365 migration performance and best practices](#)
- [Mailbox migration performance analysis](#)
- [Troubleshooting slow migrations](#)

- [Ways to migrate multiple email accounts to Microsoft 365](#)
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

Service advisories for OAB size limits

Article • 08/09/2024

This advisory informs you when your Offline Address Book has reached the size limit outlined in the [Address Book Limits](#) within the [Exchange Online limits](#).

These advisories are displayed in the Microsoft 365 admin center. To view these advisories, navigate to **Health > Service Health > Exchange Online** and finally, the **Active Issues** tab. This advisory will be listed as "Offline Address Book."

What Do These Service Advisories Indicate?

This service advisory informs you that the maximum size of a single Offline Address Book within your tenant has exceeded 1 GB. If you receive this advisory, we ask that you review any recent changes made to the Offline Address Book(s) in your environment. Your users may observe missing or incomplete data if the size issue isn't corrected.

More information

For more information about Offline Address Books, see the following articles:

- [Offline address books in Exchange Online | Microsoft Docs](#)
- [Exchange Online limits - Address Book Limits](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Microsoft 365 Apps monitoring

Article • 07/31/2024

Microsoft 365 Apps monitoring supports the following organizational-level scenarios for these desktop Office applications: Access, Excel, OneNote, Outlook, PowerPoint, Publisher, and Word.

- **Excessive Client Runtime Errors.** The runtime error rate of specific Office application has increased significantly over the last 24 hours.
- **Long Local File Load Time.** The average file load time from local storage has exceeded the recommended threshold over the last 24 hours.
- **Long Application Load Time.** The average application load time has exceeded the recommended threshold over the last 24 hours.
- **Excessive Macro Errors.** The macro error rate has exceeded the recommended threshold over the last 24 hours.
- **Excessive Add-in Errors.** The add-in error rate has exceeded the recommended threshold over the last 24 hours.
- **Long SharePoint File Load Time.** The average file load time from SharePoint has exceeded the recommended threshold over the last 24 hours.

Here's an example of the Apps monitoring dashboard:

The screenshot shows the Microsoft 365 Apps monitoring dashboard. At the top, there is a breadcrumb navigation: Home > Service health > Microsoft 365 Apps. Below the header, the title "Microsoft 365 Apps" is displayed, followed by a sub-header: "We monitor Microsoft 365 Apps for service issues in the past 7 days, as well as infrastructure and third-party software issues that might require your action." There are two tabs at the top of the main content area: "Scenarios" (which is selected) and "Active issues". To the right of these tabs, there is a search bar and a filter icon. A table below the tabs lists the following information for each app:

App and activities	Health ↑	Action required	Affected sessions	Total sessions
Access Desktop	Healthy	No	0	0
Excel Desktop	Healthy	No	0	0
OneNote Desktop	Healthy	No	0	0
Outlook Desktop	Healthy	No	0	0
PowerPoint Desktop	Healthy	No	0	0
Publisher Desktop	Healthy	No	0	0
Word Desktop	Healthy	No	0	0

When Microsoft detects an error condition, a post is created to notify the tenant admin to go to the Microsoft 365 App Health dashboard for further information to remediate issues. For more information, see [Microsoft 365 Apps health](#).

Feedback

Was this page helpful?

 Yes

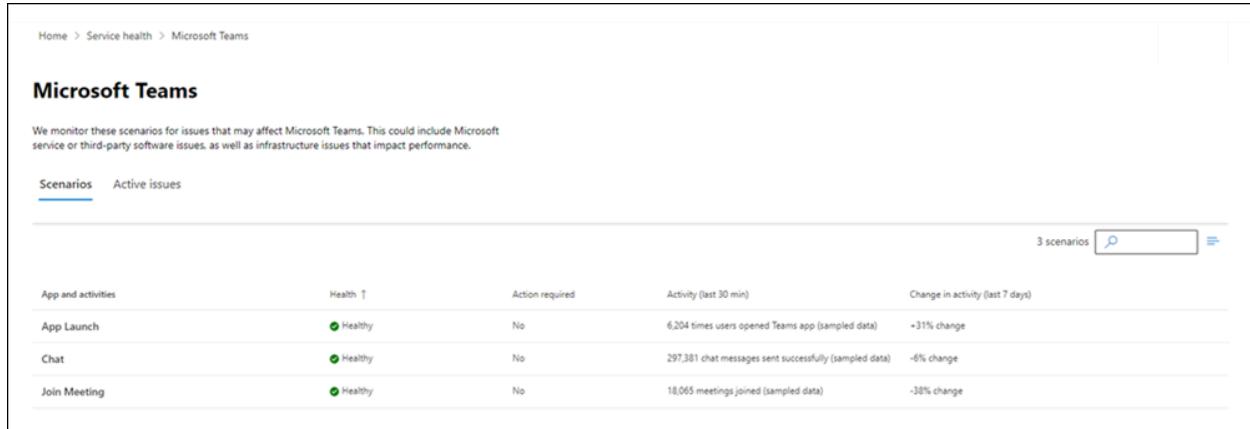
 No

Provide product feedback ↗

Microsoft 365 Teams monitoring

Article • 05/17/2024

Microsoft Teams monitoring supports the following organizational scenarios with near real-time information:



The screenshot shows the Microsoft Teams monitoring dashboard. At the top, there's a breadcrumb navigation: Home > Service health > Microsoft Teams. Below that, a section titled "Microsoft Teams" with a subtitle: "We monitor these scenarios for issues that may affect Microsoft Teams. This could include Microsoft service or third-party software issues, as well as infrastructure issues that impact performance." There are two tabs: "Scenarios" (which is selected) and "Active issues". On the right, there's a search bar and a button labeled "3 scenarios". The main area displays a table with four rows, each representing a scenario:

App and activities	Health	Action required	Activity (last 30 min)	Change in activity (last 7 days)
App Launch	Healthy	No	6,204 times users opened Teams app (sampled data)	+31% change
Chat	Healthy	No	297,381 chat messages sent successfully (sampled data)	-6% change
Join Meeting	Healthy	No	18,065 meetings joined (sampled data)	-38% change

- **App Launch.** The number of times users opened the Teams client without errors. Data is sampled and retrieved every 30 minutes.
- **Chat.** The number of chat messages sent and delivered in Teams. Data is sampled and retrieved every 30 minutes.
- **Join Meeting.** The number of times users joined Teams meetings without errors. Data is sampled and retrieved every 30 minutes.
- **Quality of Experience.** The percentage of audio streams for which Quality of Experience (QoE) telemetry was received by the Teams service. Data can be received up to 3 days after call completion. If the rate drops, investigate your network configuration to ensure that the Microsoft Teams telemetry URLs are not being blocked. The telemetry URLs can be found here: [Office 365 URLs and IP address ranges - Microsoft 365 Common and Office Online](#)
- **UDP Stream Establishment.** The percentage of audio streams established over UDP (User Datagram Protocol). Real-time media established over UDP is more efficient and provides better call quality. If the rate drops, investigate your network configuration to ensure that the ports and protocols required by Microsoft Teams are not being blocked. The required IP addresses, hostnames, ports, and protocols can be found here: [Office 365 URLs and IP address ranges - Skype for Business Online and Microsoft Teams](#)

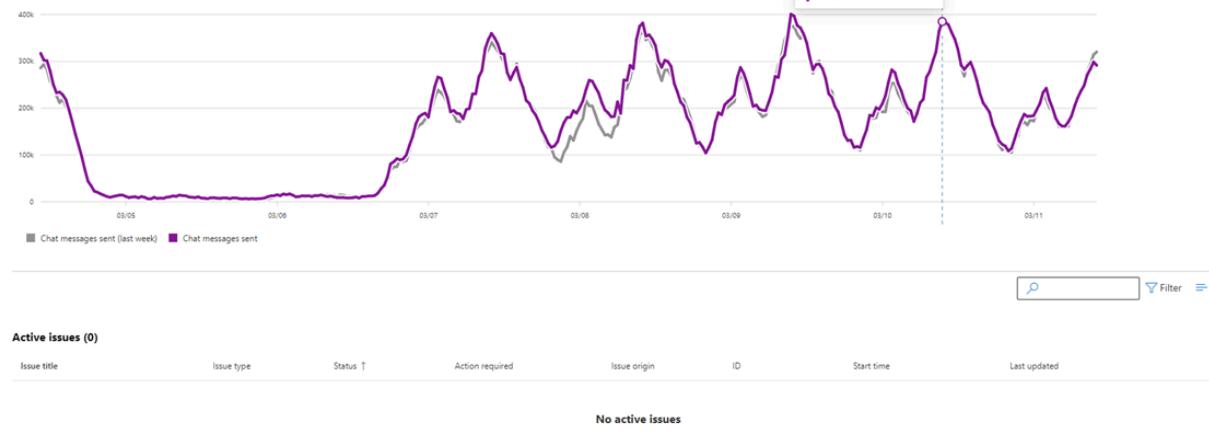
Admins can use the information to correlate any Microsoft-reported issues with the usage data to confirm any actual impact to their organization. Also, admins can view any usage from the last two weeks of usage data to identify any anomalies.

Chat

Chat messages sent successfully

The number of chat messages sent and delivered in Teams. Data is sampled and retrieved every 30 minutes.

Updated 10:02 AM PST



Feedback

Was this page helpful?

Yes

No

Provide product feedback ↗

Microsoft 365 for the web monitoring

Article • 07/25/2024

You can use Microsoft 365 for the web monitoring in the [Microsoft 365 admin center](#) to monitor the health of the Microsoft 365 for the web service for your organization's Microsoft 365 subscription. Microsoft 365 for the web monitoring provides you with information about incidents and advisories related to any issue detected in the Microsoft 365 infrastructure that Microsoft owns for providing regular updates and resolving the issue. For example, users cannot open or save Excel for the web application because of issues with Excel or the Microsoft 365 cloud infrastructure.

To go to the Service health dashboard in the Microsoft 365 admin center, select **Health > Service health**.

Issues in your organization are identified and used by organizational-level monitoring. The value in the **Health** column under **Microsoft service health** indicates that the service is healthy or has advisories or incidents based on the cloud services that Microsoft maintains.

Here's an example of the Microsoft 365 for the web monitoring page in the Microsoft 365 admin center that shows the health of organization-level scenarios available by going to **Health > Service health > Microsoft 365 for the web**.

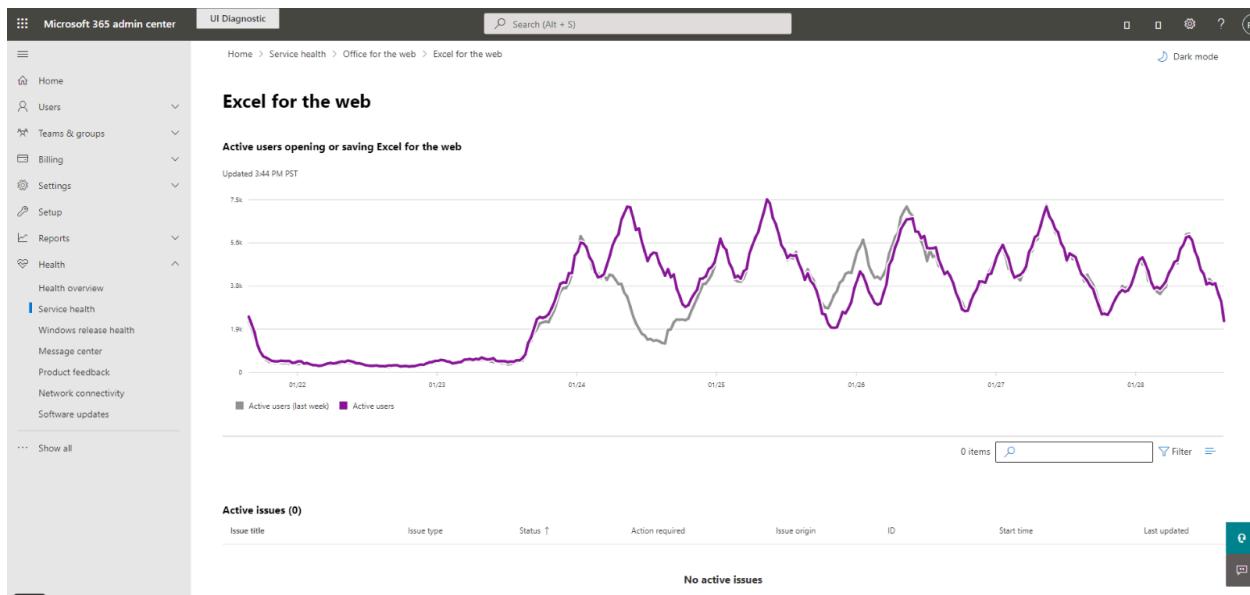
App and activities	Health	Action required	Activity (last 30 min)	Change in activity (last 7 days)
Excel for the web	Healthy	No	7,575 users opened or saved sheet	-15% change
OneNote for the web	Healthy	No	1,187 users opened or saved note	-39% change
PowerPoint for the web	Healthy	No	5,508 users opened or saved deck	-11% change
Visio for the web	Healthy	No	96 users opened or saved diagram	-29% change
Word for the web	Healthy	No	3,599 users opened or saved doc	-14% change

With the **Microsoft 365 for the web** monitoring page, you can see whether the Microsoft 365 for the web service is healthy or not and whether there are any associated incidents or advisories for any underlying Microsoft 365 for the web apps. With Microsoft 365 for the web monitoring, you can look at the service health for specific app scenarios and view near real-time signals to determine the impact by organization-level scenario.

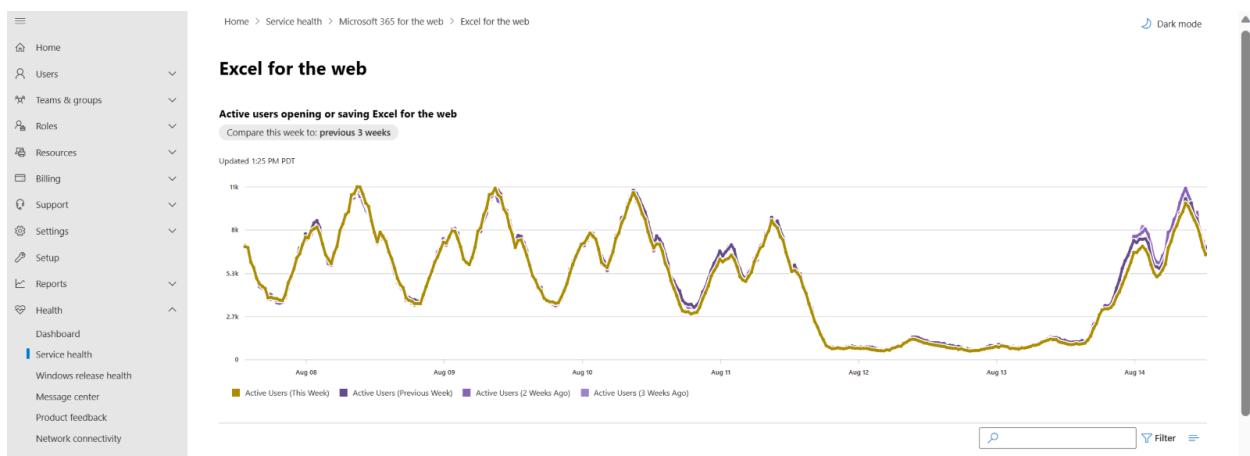
Organization-level scenarios

Microsoft 365 for the web monitoring supports the following scenarios:

- **Word for the web:** View the health for “Document Open” and “Document Save” scenarios.
- **Excel for the web:** View the health for “Sheet Open” and “Sheet Save” scenarios.
- **PowerPoint for the web:** View the health for “Deck Open” and “Deck Save” scenarios.
- **OneNote for the web:** View the health for “Note Open” and “Note Save” scenarios.
- **Visio for the web:** View the health for “Diagram Open” and “Diagram Save” scenarios.



Detailed views for each of these scenarios show the near real-time trend for the past seven days with the 60-minute aggregate compared with the previous week.



Send us feedback

Use the **Give feedback** option available on every page of the Microsoft 365 admin center.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Advanced deployment guides for Microsoft 365 and Office 365 products

Article • 12/19/2023

Microsoft 365 and Office 365 advanced deployment guides give you tailored guidance and resources for planning and deploying your tenant, apps, and services. These guides are created using the same best practices that [Microsoft 365 FastTrack](#) onboarding specialists share in individual interactions. They provide information on product setup, enabling security features, deploying collaboration tools, and provide scripts to speed up advanced deployments.

All advanced deployment guides are available in the Microsoft 365 admin center as described in the section below, and most guides can also be found in the [Microsoft 365 Setup portal](#).

Access to advanced deployment guides in the admin center requires authentication to a Microsoft 365 tenant as an administrator or other role with access to the admin center. Advanced deployment guides in the Microsoft 365 Setup portal can be accessed by anyone. We have provided links to both locations for each guide, where available, in the tables below.

Note that guides are still being added to the setup portal, but there are a few guides that will only be available in the admin center because they require authentication to a tenant to function.

In this article:

- [How to access advanced deployment guides in the Microsoft 365 admin center](#)
- [Guides for initial setup](#)
- [Guides for authentication and access](#)
- [Guides for security and compliance](#)
- [Guides for collaboration](#)
- [Advanced guides](#)

How to access advanced deployment guides in the Microsoft 365 admin center

Advanced deployment guides are accessible from the [Advanced deployment guides & assistance](#) page in the Microsoft 365 admin center. When you access advanced deployment guides from the admin center, you can keep track of the status of your

progress and return at any time to complete a guide. This functionality is not available when you access guides from the [Microsoft 365 Setup portal](#).

Note

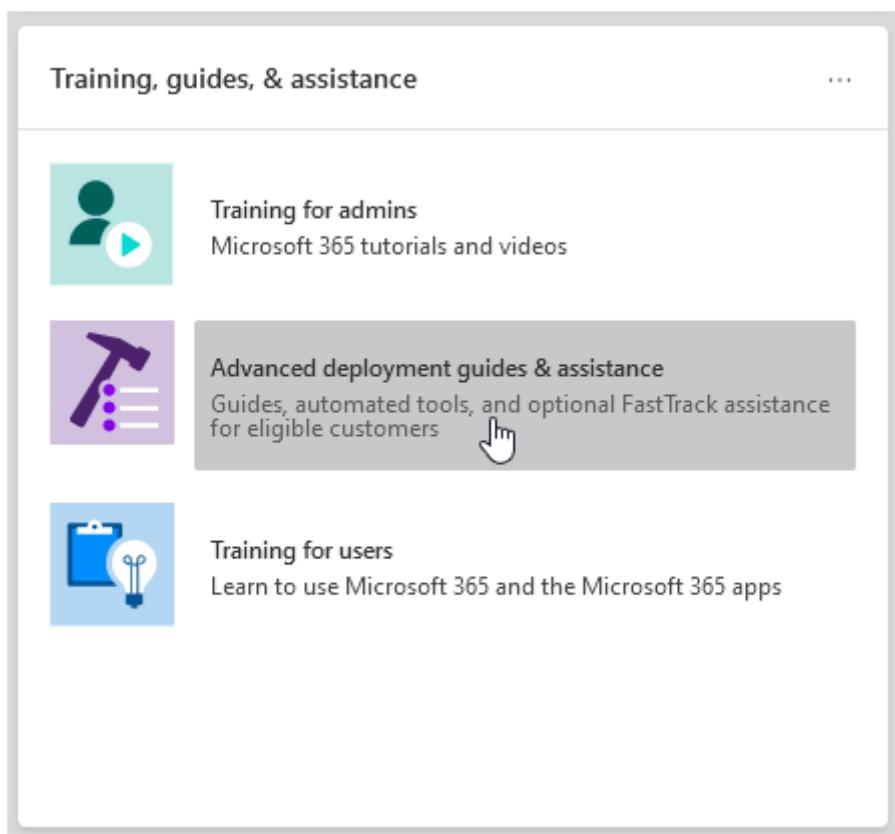
You must be assigned an admin role such as *Global Reader* to access advanced deployment guides in the Microsoft 365 admin center. Only admins with the *Global Administrator* role can use the guides to change settings in the tenant.

Important

Any selections, task assignments, and progress status saved **before January 10, 2023** within each advanced deployment guide in the admin center were reset due to EU data regulations.

To reach the **Advanced deployment guides & assistance** page:

1. In the [Microsoft 365 admin center](#), go to the **Home** page.
2. Find the *Training, guides & assistance* card and select **Advanced deployment guides & assistance**.
3. If you don't see that card, access the page directly at (<https://aka.ms/advanceddeploymentguides>).



Guides for initial setup

Advanced deployment guides in the admin center require authentication to a Microsoft 365 tenant as an administrator or other role with access to the admin center, but guides in the Microsoft 365 Setup portal can be accessed by anyone.

[+] Expand table

Guide - Setup Portal	Guide - Admin Center	Description
Microsoft 365 Copilot setup guide	Microsoft 365 Copilot setup guide	The Microsoft 365 Copilot setup guide gets you up to speed on Copilot, which revolutionizes collaboration and takes advantage of AI to automate tasks such as writing, editing, and data visualization across Word, Excel, PowerPoint, Outlook, and Teams. Copilot also simplifies the creation of meeting summaries. Our setup guide facilitates smooth integration, allowing your organization to automate work processes and enhance collaboration seamlessly.
Prepare your environment guide	Prepare your environment guide	The Prepare your environment guide helps you prepare your organization's environment for Microsoft 365 and Office 365 services. Whatever your goals are, there are tasks you'll need to complete to ensure a successful deployment. To avoid any errors while preparing your environment, you're provided with step-by-step instructions to connect your domain, add users, assign licenses, set up email with Exchange Online, and install or deploy Office apps.
Email setup guide	Email setup guide	The Email setup guide provides you with the step-by-step guidance needed for configuring Exchange Online for your organization. This guidance includes setting up new email accounts, migrating email, and configuring email protection. For a successful email setup, use this advisor and you'll receive the recommended migration method based on your organization's current mail system, the number of mailboxes being migrated, and how you want to manage users and their access.
Gmail contacts and calendar advisor	Gmail contacts and calendar advisor	When you migrate a Gmail user's mailbox to Microsoft 365, email messages are migrated, but contacts and calendar items are not. The Gmail contacts and calendar advisor provides steps for importing Google contacts and Google calendar items to Microsoft 365 using import and export methods with Outlook.com, the Outlook client, or PowerShell.

Guide - Setup Portal ↗	Guide - Admin Center ↗	Description
	Microsoft 365 setup guide ↗	<p>The Microsoft 365 setup guide provides you with guidance when setting up productivity tools, security policies, and device management capabilities. With a Microsoft 365 Business Premium or Microsoft 365 for enterprise subscription, you can use this guide to set up and configure your organization's devices.</p> <p>You'll receive guidance and access to resources to enable your cloud services, update devices to the latest supported version of Windows 10, and join devices to Microsoft Entra ID, all in one central location.</p>
	Remote work setup guide ↗	<p>The Remote work setup guide provides organizations with the tips and resources needed to ensure your users can successfully work remotely, your data is secure, and users' credentials are safeguarded.</p> <p>You'll receive guidance to optimize remote workers' device traffic to both Microsoft 365 resources in the cloud and your organization's network, which will reduce the strain on your remote access VPN infrastructure.</p>
Windows 11 and Surface setup guide ↗	Windows 11 and Surface setup guide ↗	<p>The Windows 11 and Surface setup guide provides information on deployment capabilities, tools, and strategies for deploying Windows 11 for new devices, existing devices, and Surface devices. You'll gain knowledge on setting up co-management with Intune, using autopilot for customizing the out-of-box experience, and reviewing endpoint security features. This information will provide a starting point for planning your Windows 11 deployment.</p>
Microsoft Edge setup guide ↗	Microsoft Edge setup guide ↗	<p>Microsoft Edge has been rebuilt from the ground up to bring you world-class compatibility and performance, the security and privacy you deserve, and new features designed to bring you the best of the web.</p> <p>The Microsoft Edge setup guide will help you configure Enterprise Site Discovery to see which sites accessed in your org might need to use IE mode, review and configure important security features, configure privacy policies and compliance policies to meet your org's requirements, and manage web access on your devices. You can download Microsoft Edge to individual devices, or we'll show you how to deploy to multiple users in your org with Group Policy, Configuration Manager, or Microsoft Intune.</p>
Configure IE mode for Microsoft Edge guide ↗	Configure IE mode for Microsoft Edge guide ↗	<p>If you've already deployed Microsoft Edge and only want to configure IE mode, the Configure IE mode for Microsoft Edge guide will give you scripts to automate the configuration of Enterprise Site Discovery. You'll also get IE</p>

Guide - Setup Portal	Guide - Admin Center	Description
		mode recommendations from a cloud-based tool that will help you create an Enterprise Mode Site List to deploy to your users.
Microsoft Search setup guide ↗		<p>Microsoft Search helps your organization find what they need to complete what they're working on. Whether it's searching for people, files, org charts, sites, or answers to common questions, your org can use Microsoft Search throughout their workday to get answers.</p> <p>The Microsoft Search setup guide helps you configure Microsoft Search whether you want to pilot it to a group of users or roll it out to everyone in your org. You'll assign Search admins and Search editors and then customize the search experience for your users with answers and more options, like adding the Bing extension to Chrome or setting Bing as your default search engine.</p>
Block use of Internet Explorer in your organization guide ↗		<p>Microsoft support for Internet Explorer 11 is ending soon for most versions of Windows 10. The Block use of Internet Explorer in your organization guide ensures that your users can still run legacy web apps that rely on Internet Explorer. This guide also helps you move those users to Microsoft Edge with IE mode.</p>

Guides for authentication and access

[Expand table](#)

Guide - Setup Portal	Guide - Admin Center	Description
Configure multi-factor authentication (MFA) guide ↗		<p>The Configure multifactor authentication (MFA) guide provides customers who have the Microsoft Entra ID P1 or Microsoft Entra ID P2 license with customizable Conditional Access templates that include the most common and least intrusive security standards. Customers with the P2 license can also use risk-based Conditional Access policies. Customers without a P1 or P2 license can use a one-click solution to enable security defaults, a baseline protection policy for all users. They can also enable legacy (per-user) MFA.</p>
Identity security for Teams guide ↗		<p>The Identity security for Teams guide helps you with some basic security steps you can take to ensure your</p>

Guide - Setup Portal ↗	Guide - Admin Center ↗	Description
		users are safe and have the most productive time using Teams.
Microsoft Entra setup guide ↗	Microsoft Entra setup guide ↗	<p>The Microsoft Entra setup guide provides information to ensure your organization has a strong security foundation. In this guide you'll set up initial features, like Azure Role-based access control (Azure RBAC) for admins, Microsoft Entra Connect for your on-premises directory, and Microsoft Entra Connect Health, so you can monitor your hybrid identity's health during automated syncs. It also includes essential information on enabling self-service password resets, conditional access, and integrated third party sign-on including optional advanced identity protection and user provisioning automation.</p>
Add or sync users to Microsoft Entra ID guide ↗	Add or sync users to Microsoft Entra ID guide ↗	<p>The Add or sync users to Microsoft Entra ID guide will help streamline the process of getting your user accounts set up in Microsoft 365. Based on your environment and needs, you can choose to add users individually, migrate your on-premises directory with Microsoft Entra Cloud Sync or Microsoft Entra Connect, or troubleshoot existing sync problems when necessary.</p>
	Plan your passwordless deployment guide ↗	<p>Use the Plan your passwordless deployment guide to discover the best passwordless authentication methods to use and receive guidance on how to upgrade to an alternative sign-in approach that allows users to access their devices securely with one of the following passwordless authentication methods:</p> <ul style="list-style-type: none"> • Windows Hello for Business • The Microsoft Authenticator app • Security keys • Temporary Access Pass
	Secure your cloud apps with Single Sign on (SSO) guide ↗	<p>This guide is designed to help you add cloud apps to Microsoft 365. In our guide, you can add an application to your tenant, add users to the app, assign roles, and more. If the app supports single sign-on (SSO), we'll walk you through that configuration.</p>
Plan your self-service password reset (SSPR)	Plan your self-service password reset (SSPR) deployment guide ↗	<p>Give users the ability to change or reset their password independently, if their account is locked, or they forget their password without the need to contact a helpdesk engineer.</p> <p>Use the Plan your self-service password reset (SSPR)</p>

Guide - Setup Portal	Guide - Admin Center	Description
deployment guide ↗		deployment guide to receive relevant articles and instructions for configuring the appropriate Azure portal options to help you deploy SSPR in your environment.
Migrate from AD FS to Microsoft Entra ID ↗	Migrate from AD FS to Microsoft Entra ID ↗	In Migrate from AD FS to Microsoft Entra ID we offer custom guidance for migrating from Active Directory Federation Services (AD FS) to Microsoft Entra ID. You'll first answer a few questions about your AD FS infrastructure. Then implement either pass-through authentication (PTA) or password hash sync (PHS) to give users a streamlined experience while accessing your organization's apps.

Guides for security and compliance

[+] Expand table

Guide - Setup Portal	Guide - Admin Center	Description
Security analyzer ↗	Security analyzer ↗	The Security analyzer will analyze your security approach and introduce you to Microsoft integrated security and compliance solutions that can improve your security posture. You'll learn about advanced features, such as managing identities and helping to protect against modern attacks. You can then sign up for a trial subscription and be pointed to the corresponding setup guidance for each solution.
Set up your Microsoft Zero Trust security model ↗	Set up your Microsoft Zero Trust security model ↗	Use the Set up your Zero Trust security model guide to configure security that effectively adapts to the complexity of the modern environment, embraces the hybrid workplace, and helps protect people, devices, apps, and data wherever they're located. Key recommendations include: always authenticate, limit user access, minimize the blast radius, segment access, verify end-to-end encryption, and use analytics to get visibility, drive threat detection, and improve defenses.
Deploy and set up Microsoft Intune ↗	Deploy and set up Microsoft Intune ↗	Set up Microsoft Intune to manage devices in your organization. For full control of corporate devices, you'll use Intune's mobile device management (MDM) features. To manage your organization's data on shared and personal devices, you can use Intune's mobile application management (MAM) features.

Guide - Setup Portal	Guide - Admin Center	Description
		With the Deploy and set up Microsoft Intune guide , you'll set up device and app compliance policies, assign app protection policies, and monitor the device and app protection status.
Microsoft Defender for Endpoint setup guide	Microsoft Defender for Endpoint setup guide	<p>The Microsoft Defender for Endpoint setup guide provides instructions that will help your enterprise network prevent, detect, investigate, and respond to advanced threats. Make an informed assessment of your organization's vulnerability and decide which deployment package and configuration methods are best.</p> <p>NOTE: A Microsoft Volume License is required for Microsoft Defender for Endpoint.</p>
	Exchange Online Protection setup guide	Microsoft Exchange Online Protection (EOP) is a cloud-based email filtering service for protection against spam and malware, with features to safeguard your organization from messaging policy violations. Use the Exchange Online Protection setup guide to set up EOP by selecting which of the three deployment scenarios—on-premises mailboxes, hybrid (mix of on-premises and cloud) mailboxes, or all cloud mailboxes—fits your organization. The guide provides information and resources to set up and review your user's licensing, assign permissions in the Microsoft 365 admin center, and configure your organization's anti-malware and spam policies in the Security & Compliance Center.
Microsoft Defender for Office 365 setup guide	Microsoft Defender for Office 365 setup guide	The Microsoft Defender for Office 365 setup guide safeguards your organization against malicious threats that your environment might come across through email messages, links, and third party collaboration tools. This guide provides you with the resources and information to help you prepare and identify the Defender for Office 365 plan to fit your organization's needs.
Microsoft Defender for Identity setup guide	Microsoft Defender for Identity setup guide	The Microsoft Defender for Identity setup guide provides security solution set-up guidance to identify, detect, and investigate advanced threats that might compromise user identities. These include detecting suspicious user activities and malicious insider actions directed at your organization. You'll create a Defender for Identity instance, connect to your organization's Active Directory, and then set up sensors, alerts,

Guide - Setup Portal ↗	Guide - Admin Center ↗	Description
		notifications, and configure your unique portal preferences.
Microsoft Purview Communication Compliance and Insider Risk Management setup guide ↗	Microsoft Purview Communication Compliance and Insider Risk Management setup guide ↗	<p>The Microsoft Purview Communication Compliance and Insider Risk Management setup guide helps you protect your organization against insider risks that can be challenging to identify and difficult to mitigate. Insider risks occur in a variety of areas and can cause major problems for organizations, ranging from the loss of intellectual property to workplace harassment, and more.</p> <p>The solutions in this guide will help you gain visibility into user activities, actions, and communications with native signals and enrichments from across your organization:</p> <ul style="list-style-type: none"> With the communication compliance solution, you can identify and act on communication risks for items like workplace violence, insider trading, harassment, code of conduct, and regulatory compliance violations. The insider risk management solution helps you identify, investigate, and take action on risks for intellectual property theft, sensitive data leaks, security violations, data spillage, and confidentiality violations.
Microsoft Purview Information Protection setup guide ↗	Microsoft Purview Information Protection setup guide ↗	<p>Get an overview of the capabilities you can apply to your information protection strategy so you can be confident your sensitive information is protected. Use a four-stage lifecycle approach in which you discover, classify, protect, and monitor sensitive information. The Microsoft Purview Information Protection setup guide provides guidance for completing each of these stages.</p>
Microsoft Purview Data Lifecycle Management setup guide ↗	Microsoft Purview Data Lifecycle Management setup guide ↗	<p>The Microsoft Purview Data Lifecycle Management setup guide provides you with the information you'll need to set up and manage your organization's governance strategy, to ensure that your data is classified and managed according to the specific lifecycle guidelines you set. With this guide, you'll learn how to create, auto-apply, or publish retention labels, retention label policies, and retention policies that are applied to your organization's content and compliance records. You'll also get information on importing CSV files with a file plan for bulk scenarios</p>

Guide - Setup Portal	Guide - Admin Center	Description
		or for applying them manually to individual documents.
Microsoft Defender for Cloud Apps setup guide	Microsoft Defender for Cloud Apps setup guide	<p>The Microsoft Defender for Cloud Apps setup guide provides easy to follow deployment and management guidance to set up your Cloud Discovery solution. With Cloud Discovery, you'll integrate your supported security apps, and then you'll use traffic logs to dynamically discover and analyze the cloud apps that your organization uses. You'll also set up features available through the Defender for Cloud Apps solution, including threat detection policies to identify high-risk use, information protection policies to define access, and real-time session controls to monitor activity. With these features, your environment gets enhanced visibility, control over data movement, and analytics to identify and combat cyberthreats across all your Microsoft and third party cloud services.</p>
Microsoft Purview Auditing solutions in Microsoft 365 guide	Microsoft 365 Auditing solutions in Microsoft 365 guide	<p>The Microsoft Purview Auditing solutions in Microsoft 365 guide provides an integrated solution to help organizations effectively respond to security events, forensic investigations, and compliance obligations. When you use the auditing solutions in Microsoft 365, you can search the audit log for activities performed in different Microsoft 365 services.</p>
Microsoft Purview eDiscovery solutions setup guide	Microsoft Purview eDiscovery solutions setup guide	<p>eDiscovery is the process of identifying and delivering electronic information that can be used as evidence in legal cases. The Microsoft Purview eDiscovery solutions setup guide assists in the use of eDiscovery tools in Microsoft Purview that allow you to search for content in Exchange Online, OneDrive for Business, SharePoint Online, Microsoft Teams, Microsoft 365 Groups, and Viva Engage communities.</p>

Guides for collaboration

[\[+\] Expand table](#)

Guide - Setup Portal	Guide - Admin Center	Description
Deploy employee experience with Microsoft Viva	Deploy employee experience with Microsoft Viva	Viva is an integrated, employee experience platform (EXP) that brings together communications, knowledge, learning, resources, and insights into the flow of work and fosters a culture where people and teams thrive and are empowered to be their best from anywhere. You can use the steps and guidance in the guides linked here to deploy one or more Viva apps and achieve better employee engagement throughout your organization.
Enable Microsoft Viva Connections	Enable Microsoft Viva Connections	Encourage meaningful connections while fostering a culture of inclusion and aligning the entire organization around your vision, mission, and strategic priorities.
Enable Microsoft Viva Engage	Enable Microsoft Viva Engage	Bring people together across the organization to connect with leaders, coworkers, and communities; crowdsource answers and ideas; share their work and experience; and find belonging at work.
Enable Microsoft Viva Goals	Enable Microsoft Viva Goals	Align teams with your organization's strategic priorities, driving results and a thriving business.
Enable Microsoft Viva Insights	Enable Microsoft Viva Insights	Viva Insights helps improve productivity and wellbeing through data-driven, privacy-protected insights and recommendations.
Enable Microsoft Viva Learning	Enable Microsoft Viva Learning	Bring enterprise learning into the flow of work by connecting content from your organization, learning management systems, non-Microsoft providers, and Microsoft.
Enable Microsoft Viva Topics	Enable Microsoft Viva Topics	Use AI to automatically organize content and expertise across your systems and teams into related topics, like projects, products, processes, and customers.
Enable Microsoft Viva Amplify	Enable Microsoft Viva Amplify	Centralize campaign management, publishing, and reporting to reach and engage employees.
Enable Microsoft Viva Glint	Enable Microsoft Viva Glint	Improve engagement and performance with recommended actions and data-driven insights across employee lifecycle and organization-wide surveys.
Enable Microsoft Viva Pulse	Enable Microsoft Viva Pulse	Empower managers to seek out and act on confidential feedback using smart templates, research-backed questions and analytics.
Microsoft 365 Apps setup guide	Microsoft 365 Apps setup guide	The Microsoft 365 Apps setup guide provides comprehensive guidance for setting up and deploying the latest versions of Office products like Word, Excel,

Guide - Setup Portal ↗	Guide - Admin Center ↗	Description
		<p>PowerPoint, and OneNote on your users' devices. You'll be walked through the activation process for your Microsoft 365 product key, as well as various deployment methods including easy self-install options and enterprise deployments with management tools. Additionally, the guide offers instructions on assessing your environment, determining your specific deployment requirements, and implementing the necessary support tools to ensure a successful installation.</p>
	Mobile apps setup guide ↗	<p>The Mobile apps setup guide provides instructions for the download and installation of Office apps on your Windows, iOS, and Android mobile devices. This guide provides you with step-by-step information to download and install Microsoft 365 and Office 365 apps on your phone and tablet devices.</p>
Microsoft Teams setup guide ↗	Microsoft Teams setup guide ↗	<p>The Microsoft Teams setup guide provides your organization with guidance to set up team workspaces that host real-time conversations through messaging, calls, and audio or video meetings for both team and private communication. Use the tools in this guide to configure Guest access, set who can create teams, and add team members from a .csv file, all without the need to open a PowerShell session. You'll also get best practices for determining your organization's network requirements and ensuring a successful Teams deployment.</p>
Plan and implement your Microsoft Teams Phone deployment ↗	Plan and implement your Microsoft Teams Phone deployment ↗	<p>This guide will help you transition from your existing voice solution to Microsoft Teams Phone. You'll be guided through discovery and planning phases, or you can go straight to deployment. You'll be able to configure a calling plan, Operator Connect, Teams Phone Mobile, Direct Routing, caller ID, and other features.</p>
Plan and deploy Teams Premium features ↗	Plan and deploy Teams Premium features ↗	<p>Microsoft Teams Premium helps make every meeting more intelligent, engaging, and protected. This guide will help you to plan for and deploy one or more Teams Premium features and take advantage of your Teams Premium licenses.</p>
SharePoint setup guide ↗	SharePoint setup guide ↗	<p>The SharePoint setup guide helps you set up your SharePoint document storage and content management, create sites, configure external sharing, migrate data and configure advanced settings, and drive user engagement and communication within your organization. You'll follow steps for configuring your content-sharing</p>

Guide - Setup Portal	Guide - Admin Center	Description
		permission policies, choose your migration sync tools, and enable the security settings for your SharePoint environment.
Surface Hub and Microsoft Teams Rooms setup guide ↗	Surface Hub and Microsoft Teams Rooms setup guide ↗	The Surface Hub and Microsoft Teams Rooms setup guide will customize your experience based on your environment. If you're hosted in Exchange Online and using Microsoft Teams, the guide will automatically create your device account with the correct settings.
OneDrive setup guide ↗	OneDrive setup guide ↗	Use the OneDrive setup guide to get started with OneDrive file storage, sharing, collaboration, and syncing capabilities. OneDrive provides a central location where users can sync their Microsoft 365 Apps files, configure external sharing, migrate user data, and configure advanced security and device access settings. The OneDrive setup guide can be deployed using a OneDrive subscription or a standalone OneDrive plan.
Viva Engage deployment advisor ↗	Viva Engage deployment advisor ↗	Connect and engage across your organization with Viva Engage. The Viva Engage deployment advisor prepares your Viva Engage network by adding domains, defining admins, and combining Viva Engage networks. You'll get guidance to deploy Viva Engage and then customize the look, configure security and compliance, and refine the settings.

Advanced guides

[+] Expand table

Guide - Setup Portal	Guide - Admin Center	Description
In-place upgrade with Configuration Manager guide ↗		Use the In-place upgrade with Configuration Manager guide when upgrading Windows 7 and Windows 8.1 devices to the latest version of Windows 10. You'll use the script provided to check the prerequisites and automatically configure an in-place upgrade.
Deploy Office to your users guide ↗		Deploy Office apps from the cloud with the ability to customize your installation by using the Office Deployment Tool. The Deploy Office to your users guide helps you create a customized Office configuration with advanced settings, or you can use a pre-built recommended configuration.

Guide - Setup Portal ↗ Center ↗	Guide - Admin Admin Center ↗	Description
		Whether your users are conducting a self-install or you're deploying to your users individually or in bulk, this advanced guide provides you with step-by-step instructions to give users an Office installation tailored to your organization.
Deploy Office to remote users guide ↗		<p>Now that working remotely is the norm, users need to receive your organization's Office settings when they're not connected to your internal network or when using their own devices.</p> <p>Use the Deploy Office to remote users guide to create a customized Office installation and then send users a generated PowerShell script that will seamlessly install Office with your configuration.</p>
Deploy and update Microsoft 365 Apps with Configuration Manager advisor ↗		<p>For organizations using Configuration Manager, you can use the Deploy and update Microsoft 365 Apps with Configuration Manager advisor to generate a script that will automatically configure your Microsoft 365 Apps deployment using best practices recommended by FastTrack engineers. Use this guide to build your deployment groups, customize your Office apps and features, configure dynamic or lean installations, and then run the script to create the applications, automatic deployment rules, and device collections you need to target your deployment.</p>
Intune Configuration Manager co-management setup guide ↗		<p>Use the Intune Configuration Manager co-management setup guide to set up existing Configuration Manager client devices and new internet-based devices that your org wants to co-manage with both Microsoft Intune and Configuration Manager. Co-management allows you to manage Windows 10 devices and adds new functionality to your org's devices, while receiving the benefits of both solutions.</p>
SDS Rollover setup guide ↗		<p>The SDS Rollover setup guide provides the steps to help your organization sync student information data to Microsoft Entra ID and Office 365. This guide streamlines the term lifecycle management process by creating Office 365 Groups for Exchange Online and SharePoint Online, class teams for Microsoft Teams and OneNote, as well as Intune for Education, and rostering and single sign-on integration for third-party apps. You'll perform end-of-year closeout, tenant cleanup and archive, new school year preparation, and new school year launch. Then you can create new profiles using the sync deployment method that suits your organization.</p>
Windows 365	Windows 365 Enterprise	<p>The Windows 365 Enterprise deployment checklist provides customers with information for provisioning and hosting Cloud PCs. With the deployment checklist, you can determine</p>

Guide - Setup Portal	Guide - Admin Center	Description
Enterprise checklist ↗	deployment checklist ↗	if Microsoft Entra join, Azure virtual network, or Microsoft-hosted networks path fits your organization. You can review resources that will assist with the required configuration for deployment features, health checks, updates, and maintenance for image configuration.

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Microsoft 365 inter-tenant collaboration

Article • 07/11/2024

Suppose that two organizations, Fabrikam and Contoso, each have a Microsoft 365 for business tenant. They want to work together on several projects; some of which run for a limited time and some of which are ongoing. How can Fabrikam and Contoso enable their people and teams to collaborate more effectively across their different Microsoft 365 tenants in a secure manner? Microsoft 365, with Microsoft Entra B2B collaboration, provides several options. This article describes several key scenarios that Fabrikam and Contoso can consider.

Microsoft 365 inter-tenant collaboration options include using a central location for files and conversations, sharing calendars, using IM, audio/video calls for communication, and securing access to resources and applications. Use the following tables to select solutions and learn more.

Exchange Online collaboration options

[] Expand table

Sharing goal	Administrative action	How-to information
Share calendars with another Microsoft 365 organization	Administrators can set up different levels of calendar access in Exchange Online to allow businesses to collaborate with other businesses and to let users share the schedules (free/busy information) with others.	<ul style="list-style-type: none">• Sharing• Organization relationships• Create an organization relationship• Modify an organization relationship• Remove an organization relationship• Share calendars with external users ↗
Control how users share their calendars with people outside your organization	Administrators apply sharing policies to users mailboxes to control who it can be shared with and the level of access granted	<ul style="list-style-type: none">• Sharing policies• Create a sharing policy• Apply a sharing policy to mailboxes

Sharing goal	Administrative action	How-to information
Configure secure email channels and control mail flow with partner organizations	Administrators create connectors to apply security to mail exchanges with a partner organization or service provider. The connectors enforce encryption via transport layer security (TLS) and allowing restrictions on domain names or IP address ranges your partners send email from.	<ul style="list-style-type: none"> • Modify, disable, or remove a sharing policy • How Exchange Online uses TLS to secure email connections • Configure mail flow using connectors • Remote domains • Set up connector for secure mail flow with a partner organization • Mail flow best practices (overview)

SharePoint and OneDrive for Business collaboration options

[\[\] Expand table](#)

Sharing goals	Administrative action	How-to information
Share sites and documents with external users	Administrators configure sharing at the tenant, or site collection level for Microsoft account authenticated, work or school account authenticated or guest accounts	<ul style="list-style-type: none"> • Manage external sharing for your SharePoint environment • Restrict sharing of SharePoint and OneDrive content by domain • Use SharePoint as a business-to-business (B2B) extranet solution
Tracking and controlling external sharing for end users	OneDrive for Business file owners and SharePoint end users configure site and document sharing and establish notifications to track sharing	<ul style="list-style-type: none"> • Configure notifications for external sharing for OneDrive for Business • Share SharePoint files or folders

Skype for Business collaboration options

[+] Expand table

Sharing goal	Administrative action	How-to information
Skype for Business Online - IM, calls, and presence with other Skype for Business users	Administrators can enable their Skype for Business Online users to IM, make audio/video calls, and see presence with users in another Microsoft 365 tenant.	Allow users to contact external Skype for Business users
Skype for Business Online - IM, calls, and presence with Skype (consumer) users	Administrators can enable their Skype for Business Online users to IM, make calls, and see presence with Skype (consumer) users.	Let Skype for Business users add Skype contacts

Microsoft Entra B2B Collaboration options

[+] Expand table

Sharing goal	Administrative action	How-to information
Microsoft Entra B2B collaboration - Content sharing by adding external users to a group in an organization's directory	A Microsoft Entra DC admin, Security Admin, User Admin, or Cloud Application Admin for one Microsoft 365 tenant can invite people in another Microsoft 365 tenant to join their directory, add those external users to a group, and grant access to content, such as SharePoint sites and libraries for the group.	<ul style="list-style-type: none">What is Microsoft Entra B2B collaboration preview?Microsoft Entra B2B: New updates make cross-business collab easyExternal sharing and Microsoft Entra B2B collaborationMicrosoft Entra B2B collaboration API and customizationMicrosoft Entra ID and Identity Show: Microsoft Entra B2B Collaboration (Business to Business)

Microsoft 365 collaboration options

[+] Expand table

Sharing goal	Administrative action	How-to information
Microsoft 365 Groups - Email, calendar, OneNote, and shared files in a central place	Groups are supported in Business Essentials, Business Premium, Education, and the Enterprise E1, E3, and E5 plans. People in one Microsoft 365 tenant can create a group and invite people in another Microsoft 365 tenant as guest users. Applies to Dynamics CRM as well.	<ul style="list-style-type: none">• Learn about Microsoft 365 groups• Guest access in Microsoft 365 Groups• Deploy Microsoft 365 Groups

Viva Engage collaboration options

[+] Expand table

Sharing goal	Administrative action	How-to information
Viva Engage - Collaboration through an enterprise social medium	Unless the ability to create external groups is disabled by a Viva Engage admin, users can create external groups to collaborate in Viva Engage through conversations, the ability to like and follow posts, share files, and chat online.	Create and manage external groups in Viva Engage

Teams collaboration options

[+] Expand table

Sharing goal	Administrative action	How-to information
Collaborate in Teams with users external to the organization	A User Admin for the inviting Microsoft 365 tenant needs to enable external collaboration in Teams. Team owners are able to invite anyone with an email address to collaborate in Teams. Admins can also manage and edit Guests already present in their tenant.	<ul style="list-style-type: none">• Authorize Guest Access• Turn Guest Access On or Off in Teams• Use PowerShell to control Guest Access• Guest Access Checklist

Sharing goal	Administrative action	How-to information
		<ul style="list-style-type: none"> • View Guest Users • Edit guest user information
Team owners can invite and manage how guests collaborate within their teams.	Team owners have extra controls on what the guests can do within their teams.	<ul style="list-style-type: none"> • Add Guests • Add a guest to a team • Manage Guest Access in Teams • See who's on a Team or in a Channel

Power BI collaboration options

[\[\] Expand table](#)

Sharing goal	Administrative action	How-to information
Power BI enables external guest users to consume content shared to them through links. This enables users in the organization to distribute content in a secure way across organizations.	The Power BI Admin can control whether users can invite external users to view content within the organization.	Distribute Power BI content to external guest users with Microsoft Entra B2B

Points to be aware of about Microsoft 365 inter-tenant collaboration

Sharing of user accounts, licenses, subscriptions, and storage

Each organization maintains its own user accounts, identities, security groups, subscriptions, licenses, and storage. People use the collaboration features in Microsoft

365 together with sharing policies and security settings to provide access to needed information while maintaining control of company assets.

- **User accounts:** Accounts can't be shared or duplicated between the tenants or partitions in the on-premises Active Directory Domain Services.
- **Licenses & subscriptions:** In Microsoft 365, licenses from licensing plans (also called SKUs or Microsoft 365 plans) give users access to the Microsoft 365 services that are defined for those plans.
- **Storage:** In Microsoft 365 licensing plans, software boundaries and limits for SharePoint are managed separately from mailbox storage limits. Mailbox storage limits are set up and managed by using Exchange Online. In both scenarios, storage can't be shared across tenants.

Can we share domain namespaces across Microsoft 365 tenants?

No. Organization domain names, such as fabrikam.com or tailspintoys.com, can only be associated and used with a single Microsoft 365 tenant. Each tenant must have its own namespace. UPN, SMTP, and SIP namespaces can't be shared across tenants.

What about hybrid components and Microsoft 365 inter-tenant collaboration?

On-premises hybrid components, such as an Exchange organization and Microsoft Entra Connect, can't be split across multiple tenants.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Cross-tenant mailbox migration

Article • 02/01/2024

During mergers or divestitures, you might need the ability to move your users' Exchange Online mailboxes into a new tenant. Cross-tenant mailbox migration allows tenant administrators to use well-known interfaces like Exchange Online PowerShell and MRS to transition users to their new organization.

Administrators can use the **New-MigrationBatch** cmdlet, available through the *Move Mailboxes* management role, to execute cross-tenant moves.

Users migrating must be present in the target tenant Exchange Online system as a *MailUser*, marked with specific attributes to enable the cross-tenant moves. The system fails to move users that aren't properly set up in the target tenant.

After the moves are complete, the source user mailbox is converted to a *MailUser*, and the *targetAddress* (shown as *ExternalEmailAddress* in Exchange) is stamped with the routing address to the destination tenant. This process leaves the legacy *MailUser* in the source tenant and allows for coexistence and mail routing. When business processes allow, the source tenant can remove the source *MailUser* or convert them to a mail contact.

Cross-tenant Exchange mailbox migrations are supported for tenants in hybrid or cloud only, or a combination of the two.

This article describes the process for cross-tenant mailbox moves and provides guidance on how to prepare source and target tenants for the Exchange Online mailbox content moves.

ⓘ Important

Mailboxes that are on any type of hold aren't migrated, and the move for those mailboxes is blocked.

When a mailbox is migrated cross-tenant with this feature, only user-visible content in the mailbox (email, contacts, calendar, tasks, and notes) is migrated to the target (destination tenant). After a successful migration, the source mailbox is deleted. This deletion means that after migration, under no circumstances is the source mailbox available, discoverable, or accessible in the source tenant.

Licensing

ⓘ Important

As of Nov. 2022, **Cross Tenant User Data Migration** is available as an add-on to the following Microsoft 365 subscription plans for Enterprise Agreement customers, and is required for cross-tenant migrations. User licenses are per migration (one-time fee) and can be assigned either on the source or target user object. This license also covers [OneDrive for Business migration](#). Contact your Microsoft account team for details.

The Cross Tenant User Data Migration add-on is available as a separate purchase for Microsoft 365 Business Basic, Standard, and Premium; Microsoft 365 F1/F3/E3/E5/; Office 365 F3/E1/E3/E5; Exchange Online; SharePoint Online; and OneDrive for Business.

Warning

You must have purchased, or verified that you can purchase, cross-tenant user data migration licenses prior to the next steps. Migrations fail if this step hasn't been completed. Microsoft doesn't offer exceptions for this licensing requirement.

If you do not have the proper license assigned to the user being migrated, the migration fails, and you receive an error that is similar to the following:

code

```
Error: CrossTenantMigrationWithoutLicensePermanentException: No license was found for the source recipient, '65c3c3ea-2b9a-44d0-a685-9bfe300f8c87', or the target recipient, '65c3c3ea-2b9a-44d0-a685-9bfe300f8c87'. A Cross-tenant User Data Migration license is required to move a mailbox between tenants.
```

Preparing source and target tenants

Prerequisites for source and target tenants

Before starting, ensure that you have the necessary permissions to configure the Move Mailbox application in Azure, EXO Migration Endpoint, and the EXO Organization Relationship.

Additionally, at least one mail-enabled security group in the source tenant is required. These groups are used to scope the list of mailboxes that can move from source tenant (or sometimes referred to as resource) to the target tenant. This scoping allows the source tenant administrator to restrict or scope the specific set of mailboxes that need to be moved, preventing unintended users from being migrated.

If you are migrating more than 10,000 users, we recommend creating multiple groups to contain the user list for best performance. While nested groups are supported, they are not recommended.

You also need to communicate with your trusted partner company (with whom you'll be moving mailboxes) to obtain their Microsoft 365 tenant ID. This tenant ID is used in the **Organization Relationship DomainName** field.

To obtain the tenant ID of a subscription, sign in to the [Microsoft 365 admin center](#) and go to

https://aad.portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Properties. Select the **copy** icon for the **Tenant ID** property to copy it to the clipboard.

All users in both the source and target organizations must be licensed with the appropriate Exchange Online subscriptions. Also, ensure that you apply Cross Tenant User Data Migration licenses to all users who will be migrated to the target side.

Configuration steps to enable your tenants for cross-tenant mailbox migrations

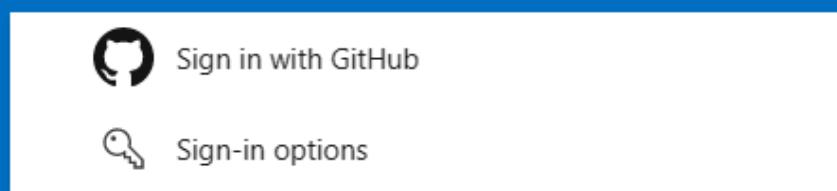
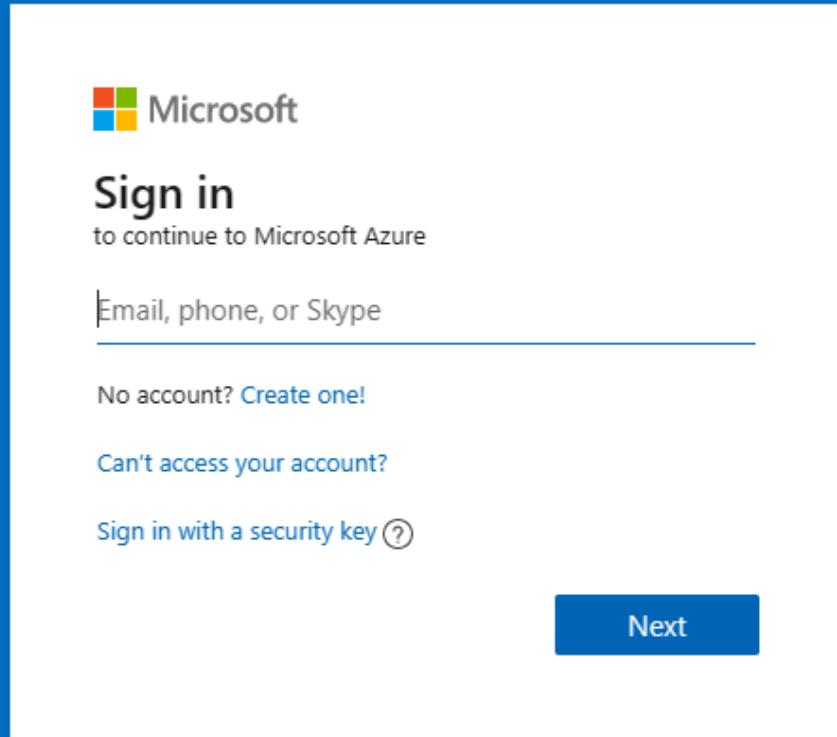
Note

You must configure the target (destination) first. To complete these steps, you aren't required to have or know the tenant administrator credentials for both the source and target tenant. Steps can be performed individually for each tenant by different administrators.

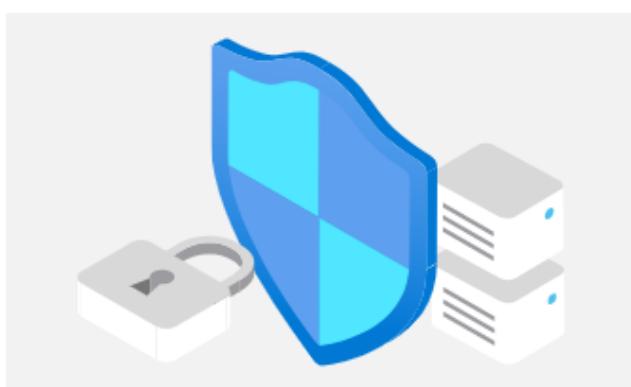
Prepare the target (destination) tenant by creating the migration application and secret

1. Sign in to your Microsoft Entra admin center (<https://portal.azure.com>) with your target tenant administrator credentials.

Microsoft Azure



2. Under Manage Microsoft Entra ID, select View.



Manage Azure Active Directory

Manage access, set smart policies, and enhance security with Azure Active Directory.

[View](#)

[Learn more](#)

3. In the navigation pane, select App registrations.

4. Select New registration.

The screenshot shows the Azure Active Directory App registrations page for the tenant 'contoso.com'. The top navigation bar includes the tenant name, 'App registrations', and links for 'New registration', 'Endpoints', 'Troubleshooting', 'Refresh', and 'Download'. The main content area displays a table of registered applications.

5. On the Register an application page, under Supported account types, select Accounts in any organizational directory (Any Microsoft Entra directory - Multi-tenant). Then, under Redirect URI (optional), select Web, and then type `https://office.com`. Then, select Register.

The screenshot shows the 'Register an application' dialog box. It includes fields for Name (MyCrossTenantMailboxMigrationApp), Supported account types (Accounts in any organizational directory (Any Azure AD directory - Multitenant) selected), and Redirect URI (optional) (Web selected, https://office.com entered).

On the top-right corner of the page, see the notification dialog box that states the app was successfully created.

6. Go back to the Home page, go to Microsoft Entra ID, and then select App registrations.
7. Under Owned applications, find the app you created, and then select it.
8. Under Essentials, copy the Application (client) ID. You'll need this information later to create a URL for the target tenant.
9. In the navigation pane, select API permissions to view permissions assigned to your app.
10. By default, User.Read permissions are assigned to the app you created, but these permissions aren't required for mailbox migrations. You can remove those permissions.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for test_test_msftofetesttenant-AdvancedEncryption

API / Permissions name	Type	Description	Admin consent requ...	Status	...	
Microsoft Graph (1)		User.Read	Delegated	Sign in and read user profile	No	 Remove permission

11. To add permission for mailbox migration, select **Add a permission**.
12. In the **Request API permissions** window, select **APIs my organization uses**, search for **Office 365 Exchange Online**, and then select it.

Request API permissions

Select an API

Microsoft APIs **APIs my organization uses** My APIs

Apps in your directory that expose APIs are shown below

 office 365 exchange online

Name
Office 365 Exchange Online

13. Select **Application permissions**.
14. Under **Select permissions**, expand **Mailbox** and select **Mailbox.Migration**, and then select **Add permissions** at the bottom on the screen.

Request API permissions

X

[All APIs](#)

O365 Office 365 Exchange Online
<https://ps.outlook.com>

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Start typing a permission to filter these results

Permission

Admin consent required

Other permissions

Calendars

Contacts

Exchange

Mailbox (1)



Mailbox.Migration ⓘ

Move mailboxes between organizations

Yes

MailboxSettings

Mail

[Add permissions](#)

[Discard](#)

15. Now select **Certificates & secrets** in the navigation pane for your application.

16. Under **Client secrets**, select **New client secret**.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

Description	Expires	Value	Secret ID
-------------	---------	-------	-----------

No client secrets have been created for this application.

17. In the **Add a client secret** window, type a description, and then configure your expiration settings.

Note

The password is used when creating your migration endpoint. It's extremely important that you copy this password to your clipboard and/or to a secure/secret

password safe location. The secret creation stage is the only time during which you can see this password! If you do somehow lose it or need to reset it, you can sign back into the Azure portal, go to **App registrations**, find your migration app, select **Secrets & certificates**, and then create a new secret for your app.

Now that you've successfully created the migration application and secret, the next step is to consent to the application.

Grant consent to the application

1. In the Microsoft Entra ID landing page, select **Enterprise applications** in the navigation pane; then find your migration app you created, select it, and then select **API Permissions**.
2. Select **Grant admin consent for [your tenant]**. A new browser window opens.
3. Select **Accept**.
4. Go back to your portal window and select **Refresh** to confirm your acceptance.
5. Formulate the URL to send to your trusted partner (source tenant administrator) so that they can also accept the application to enable mailbox migration.

Here's an example of the URL to provide to them:

```
https://login.microsoftonline.com/contoso.onmicrosoft.com/adminconsent?client_id=[application_id_of_the_app_you_just_created]&redirect_uri=https://office.com
```

Note

You'll need the application ID of the mailbox migration app you just created. You'll need to replace contoso.onmicrosoft.com in the above example with your source tenant's correct onmicrosoft.com name. You'll also need to replace [application_id_of_the_app_you_just_created] with the application ID of the mailbox migration app you just created.

Prepare the target tenant by creating the Exchange Online migration endpoint and organization relationship

1. [Connect to Exchange Online PowerShell](#) in the target Exchange Online tenant.
2. Create a new migration endpoint for Cross-tenant mailbox moves.

Note

You'll need the application ID of the mailbox migration app you just created and the password (secret) you configured in [Prepare the target \(destination\) tenant by creating the migration application and secret](#). Depending on the Microsoft 365 cloud instance you use, your endpoint may be different. See the [Microsoft 365 endpoints](#) page; select the correct instance for your tenant; then review the Exchange Online *Optimize/Required* address, and replace as appropriate.

PowerShell

```
# Enable customization if tenant is dehydrated
$dehydrated=Get-OrganizationConfig | select isdehydrated
if ($dehydrated.isdehydrated -eq $true) {Enable-OrganizationCustomization}
$AppId = "[Guid copied from the migrations app]"
$Credential = New-Object -TypeName System.Management.Automation.PSCredential
-ArgumentList $AppId, (ConvertTo-SecureString -String "[this is your secret
password you saved in the
previous steps]" -AsPlainText -Force)
New-MigrationEndpoint -RemoteServer outlook.office.com -RemoteTenant
"contoso.onmicrosoft.com" -Credentials $Credential -ExchangeRemoteMove:$true
-Name "[the name of your migration endpoint]" -ApplicationId $AppId
```

3. Create a new organization relationship object or edit your existing organization relationship object to your source tenant.

PowerShell

```
$sourceTenantId="[tenant id of your trusted partner, where the source
mailboxes are]"
$orgrels=Get-OrganizationRelationship
$existingOrgRel = $orgrels | ?{$_._DomainNames -like $sourceTenantId}
If ($null -ne $existingOrgRel)
{
    Set-OrganizationRelationship $existingOrgRel.Name -Enabled:$true -
MailboxMoveEnabled:$true -MailboxMoveCapability Inbound
}
If ($null -eq $existingOrgRel)
{
    New-OrganizationRelationship "[name of the new organization
relationship]" -Enabled:$true -MailboxMoveEnabled:$true -
MailboxMoveCapability Inbound -DomainNames $sourceTenantId
}
```

Prepare the source (current mailbox location) tenant by accepting the migration application and configuring the organization relationship

1. Using your browser, go to the URL link provided by your trusted partner to consent to the mailbox migration application. The URL should look like this:

```
https://login.microsoftonline.com/contoso.onmicrosoft.com/adminconsent?client_id=[application_id_of_the_app_you_just_created]&redirect_uri=https://office.com
```

⚠ Note

You'll need the application ID of the mailbox migration app you just created. You will need to replace `contoso.onmicrosoft.com` in the previous example with your source tenant's `onmicrosoft.com` URL. You'll also need to replace `[application_id_of_the_app_you_just_created]` with the application ID of the mailbox migration app you just created.

2. Accept the application when the pop-up appears. You can also sign in to your Microsoft Entra admin center and find the application under **Enterprise applications**.
3. [Connect to Exchange Online PowerShell](#) on the source Exchange Online tenant.
4. Create a new organization relationship object or edit your existing organization relationship object to your target (destination) tenant in Exchange Online PowerShell:

PowerShell

```
# Enable customization if tenant is dehydrated
$dehydrated=Get-OrganizationConfig | select isdehydrated
if ($dehydrated.isdehydrated -eq $true) {Enable-OrganizationCustomization}
$targetTenantId="[tenant id of your trusted partner, where the mailboxes are being moved to]"
$appId="[application id of the mailbox migration app you consented to]"
$scope="[name of the mail enabled security group that contains the list of users who are allowed to migrate]"
New-DistributionGroup -Type Security -Name $scope
$orgrels=Get-OrganizationRelationship
$existingOrgRel = $orgrels | ?{$_._DomainNames -like $targetTenantId}
If ($null -ne $existingOrgRel)
{
    Set-OrganizationRelationship $existingOrgRel.Name -Enabled:$true -MailboxMoveEnabled:$true -MailboxMoveCapability RemoteOutbound -OAuthApplicationId $appId -MailboxMovePublishedScopes $scope
}
If ($null -eq $existingOrgRel)
{
    New-OrganizationRelationship "[name of your organization relationship]" -Enabled:$true -MailboxMoveEnabled:$true -MailboxMoveCapability RemoteOutbound -DomainNames $targetTenantId -OAuthApplicationId $appId -MailboxMovePublishedScopes $scope
}
```

⚠ Note

The tenant ID that you enter as the \$sourceTenantId and \$targetTenantId is the GUID and not the tenant domain name. For an example of a tenant ID and information about finding your tenant ID, see [Find your Microsoft 365 tenant ID](#).

Prepare target user objects for migration

Users migrating must be present in the target tenant and Exchange Online system (as a MailUser) marked with specific attributes to enable the Cross-tenant moves. The system will fail to move users that aren't properly set up in the target tenant. The [Prerequisites for target user objects](#) section details the MailUser object requirements for the target tenant.

Prerequisites for target user objects

Ensure the following objects and attributes are set in the target organization:

Tip

Microsoft is developing a feature to provide a secure automated method to set many of the attributes (specified below, in this section). This feature, named Cross-Tenant Identity Mapping, is currently looking for customers willing to participate in a small private preview. For more information about this pre-release feature and how it can simplify your Cross-tenant migration processes, see [Cross-Tenant Identity Mapping](#).

For any mailbox moving from a source organization, you must provision a MailUser object in the Target organization:

1. The Target MailUser must have these attributes from the source mailbox or assigned with the new User object:
 - a. ExchangeGUID (direct flow from source to target): The mailbox GUID must match. The move process won't proceed if this attribute isn't present on target object.
 - b. ArchiveGUID (direct flow from source to target): The archive GUID must match. The move process won't proceed if this attribute isn't present on the target object. (This attribute is only required if the source mailbox is Archive enabled).
 - c. LegacyExchangeDN (flow as proxyAddress, "x500:<LegacyExchangeDN>"): The LegacyExchangeDN must be present on target MailUser as x500: proxyAddress. **In addition, you also need to copy all x500 addresses from the source mailbox to the target mail user.** The move processes won't proceed if these x500 addresses aren't present on the target object. Also, this step is important for enabling reply ability for emails that are sent before migration. The sender/recipient address in each email item and the auto-complete cache in Microsoft Outlook and in Microsoft Outlook Web

App (OWA) use the value of the LegacyExchangeDN attribute. If a user can't be located using the LegacyExchangeDN value, the delivery of email messages may fail with a 5.1.1 NDR.

- d. UserPrincipalName: UPN will align to the user's NEW identity or target company (for example, user@northwindtraders.onmicrosoft.com).
- e. Primary SMTPAddress: Primary SMTP address will align to the user's NEW company (for example, user@northwindtraders.com).
- f. TargetAddress/ExternalEmailAddress: MailUser will reference the user's current mailbox hosted in source tenant (for example user@contoso.onmicrosoft.com). When this value is being assigned, verify that you have/are also assigning PrimarySMTPAddress; else, this value will set the PrimarySMTPAddress, which will cause move failures.
- g. You can't add legacy smtp proxy addresses from source mailbox to target MailUser. For example, you can't maintain contoso.com on the MEU in northwindtraders.onmicrosoft.com tenant objects. Domains are associated with one Microsoft Entra ID or Exchange Online tenant only.

Example **target** MailUser object:

[Expand table](#)

Attribute	Value
Alias	LaraN
RecipientType	MailUser
RecipientTypeDetails	MailUser
UserPrincipalName	LaraN@northwindtraders.onmicrosoft.com
PrimarySmtpAddress	Lara.Newton@northwindtraders.com
ExternalEmailAddress	SMTP:LaraN@contoso.onmicrosoft.com
ExchangeGUID	1ec059c7-8396-4d0b-af4e-d6bd4c12a8d8
LegacyExchangeDN	/o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=74e5385fce4b46d19006876949855035-Lara
EmailAddresses	x500:/o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=d11ec1a2cacd4f81858c81907273f1f9-Lara smtp:LaraN@northwindtraders.onmicrosoft.com

Attribute	Value
	SMTP:Lara.Newton@northwindtraders.com
	X500:/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=f161af74128f460fba5c0c23984b3d6c-Lara

Example **source** Mailbox object:

[Expand table](#)

Attribute	Value
Alias	LaraN
RecipientType	UserMailbox
RecipientTypeDetails	UserMailbox
UserPrincipalName	LaraN@contoso.onmicrosoft.com
PrimarySmtpAddress	Lara.Newton@contoso.com
ExchangeGUID	1ec059c7-8396-4d0b-af4e-d6bd4c12a8d8
LegacyExchangeDN	/o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=d11ec1a2cacd4f81858c81907273f1f9-Lara
EmailAddresses	smtp:LaraN@contoso.onmicrosoft.com
	SMTP:Lara.Newton@contoso.com
	X500:/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=f161af74128f460fba5c0c23984b3d6c-Lara

2. Other attributes may be included in Exchange hybrid write-back already. If not, they should be included.

- a. `msExchBlockedSendersHash` – Writes back online blocked sender data from clients to on-premises Active Directory.
- b. `msExchSafeRecipientsHash` – Writes back online safe recipients data from clients to on-premises Active Directory.
- c. `msExchSafeSendersHash` – Writes back online safe sender data from clients to on-premises Active Directory.

Users in the target organization must be licensed with appropriate Exchange Online subscriptions applicable for the organization. You may apply a license in advance of a mailbox move but ONLY once the target MailUser is properly set up with ExchangeGUID and proxy addresses. Applying a license before the ExchangeGUID is applied will result in

a new mailbox provisioned in target organization. You must also apply a Cross Tenant User Data Migration license; else, you may see a transient error reading **needs approval**, which will report a warning in the move report that a license hasn't been applied to the target user.

 **Note**

When you apply a license on a Mailbox or MailUser object, all SMTP type proxyAddresses are scrubbed to ensure only verified domains are included in the Exchange EmailAddresses array.

3. You must ensure that the target MailUser has no previous ExchangeGUID that doesn't match the Source ExchangeGUID. This mismatch might occur if the target MEU was previously licensed for Exchange Online and provisioned a mailbox. If the target MailUser was previously licensed for or had an ExchangeGUID that doesn't match the Source ExchangeGUID, you need to perform a cleanup of the cloud MEU. For these cloud MEUs, you can run `Set-User <identity> -PermanentlyClearPreviousMailboxInfo`.

 **Caution**

This process is irreversible. If the object has a softDeleted mailbox, it can't be restored after this point. Once cleared, however, you can synchronize the correct ExchangeGUID to the target object, and MRS will connect the source mailbox to the newly created target mailbox. (Reference EHLO blog on the new parameter.)

Find objects that were previously mailboxes using the following command:

PowerShell

```
Get-User <identity> | select Name, *recipient* | Format-Table -AutoSize
```

Here's an example:

PowerShell

```
Get-User John@northwindtraders.com |select name, *recipient*| Format-Table -AutoSize
```

Name	PreviousRecipientTypeDetails	RecipientType	RecipientTypeDetails
John	UserMailbox	MailUser	MailUser

Clear the soft-deleted mailbox using the following command:

PowerShell

```
Set-User <identity> -PermanentlyClearPreviousMailboxInfo
```

Here's an example:

PowerShell

```
Set-User John@northwindtraders.com -PermanentlyClearPreviousMailboxInfo -Confirm
```

Are you sure you want to perform this action?

Delete all existing information about user "John@northwindtraders.com"? This operation will clear existing values from Previous home MDB and Previous Mailbox GUID of the user. After deletion, reconnecting to the previous mailbox that existed [in](#) the cloud will not be possible and any content it had will be unrecoverable PERMANENTLY.

Do you want to [continue](#)?

```
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (default is "Y"): Y
```

How do I know this worked?

You can verify Cross-tenant mailbox migration configuration by running the [Test-MigrationServerAvailability](#) cmdlet against the Cross-tenant migration endpoint that you created on your target tenant. Run the following cmdlet from target tenant:

PowerShell

```
Test-MigrationServerAvailability -EndPoint "[the name of your migration endpoint]" -TestMailbox "[Primary SMTP of MailUser object in target tenant]"
```

① Note

Additionally, you may want to take advantage of the [Cross-tenant mailbox migration validation script](#), which will allow you to validate the organizations being correctly setup between them, and the objects you are planning to migrate from one tenant to another. The script will help identify any discrepancies that may be present on all objects at once, and as a result, it will reduce the time spent on the initial phase.

Move mailboxes back to the original source

If a mailbox is required to move back to the original source tenant, the same set of steps and scripts must be run in both new source and new target tenants, with some variance.

Do not run the sample scripts provided to create the OrganizationRelationship.

Update the following values in the existing OrganizationRelationship created in each tenant:

- MailboxMovesCapability should have Inbound, RemoteOutbound as the capabilities in both source and target tenants.
- In the new source tenant, update the OAuthApplicationId value with the value from the newly created application in the new source tenant.
- In the new new source tenant, update the MailboxMovePublishedScopes value with the newly created security group in the new source tenant.

Perform mailbox migrations

Cross-tenant Exchange mailbox migrations are initiated from the target tenant as migration batches. This process is similar to the way on-boarding migration batches work when migrating from Exchange on-premises to Microsoft 365.

Create Migration batches

Here's an example command for initiating a batch migration:

PowerShell

```
New-MigrationBatch -Name T2Tbatch -SourceEndpoint target_source_7977 -CSVData ([System.IO.File]::ReadAllBytes('users.csv')) -Autostart -TargetDeliveryDomain northwindtraders.onmicrosoft.com

Identity          Status   Type           TotalCount
-----            -----   -----
T2Tbatch          Syncing  ExchangeRemoteMove 1
```

⚠ Note

The email address in the CSV file must be the one specified in the target tenant (for example, userA@northwindtraders.onmicrosoft.com), not the one in the source tenant.

[For more information on the cmdlet click here](#) [For some example CSV file info click here](#)

A minimal example of a CSV file is:

CSV

```
EmailAddress
userA@northwindtraders.onmicrosoft.com
userB@northwindtraders.onmicrosoft.com
userC@northwindtraders.onmicrosoft.com
```

Migration batch submission is also supported from the new [Exchange admin center](#) when selecting the cross-tenant option.

Update on-premises MailUsers

Once the mailbox moves from source to target, you should ensure that the on-premises mail users, in both the source and target, are updated with the new targetAddress. In the examples, the targetDeliveryDomain used in the move is [northwindtraders.onmicrosoft.com](#). Update the mail users with this targetAddress.

Remove endpoints and organization relationships after migration

Use the [Remove-MigrationEndpoint](#) cmdlet to remove existing migration endpoints for source or destination servers after the migration is complete.

Use the [Remove-OrganizationRelationship](#) cmdlet to remove existing organization relationships for source or destination servers after the migration is complete.

Frequently asked questions

Do I need to update RemoteMailboxes in the source on-premises tenant after the move?

Source Exchange Organization

You should update the targetAddress (RemoteRoutingAddress/ExternalEmailAddress) of each source on-premises user when the source tenant mailbox moves to the target tenant. While mail routing can follow the referrals across multiple mail users with different targetAddresses, Free/Busy lookups for mail users **must** target the location of the mailbox user.

Target Exchange Organization

After migration is complete in a hybrid organization, run the following PowerShell command if you want your users to have remote mailboxes on-premises:

PowerShell

```
Get-MailUser -Identity <Migrate Mail User> | Enable-RemoteMailbox
```

Do Teams meetings migrate cross-tenant?

While Teams meetings are moved, the meeting URL isn't updated when items migrate cross-tenant. Since the URL will be invalid in the target tenant, you must remove and recreate Teams

meetings.

What content is migrated cross-tenant?

When a mailbox is migrated cross-tenant with this feature, only user-visible content in the mailbox, also known as Top of Information Store (email, contacts, calendar, tasks, and notes), and the Recoverable Items folders Deletions, Versions, and Purges are migrated.

Do items in the Outbox get migrated cross-tenant?

Items in the Outbox aren't migrated cross-tenant as this folder is a client-based folder specific to the Outlook client. Items in the Outbox are stored locally, and not synced to the cloud.

Does the Teams chat folder content migrate cross-tenant?

No, the Teams chat folder content doesn't migrate cross-tenant. However, once the mailbox has been migrated cross-tenant, the Teams chat folder content will be available for source tenant administrator to search and export, using a content search.

How can I see just moves that are cross-tenant moves, not my onboarding and off-boarding moves?

Use the *Flags* parameter:

PowerShell

```
Get-MoveRequest -Flags "CrossTenant"
```

Can you provide example scripts for copying attributes used in testing?

ⓘ Note

SAMPLE – AS IS, NO WARRANTY This script assumes a connection to both source mailbox (to get source values) and the target on-premises Active Directory Domain Services (to stamp the ADUser object).

PowerShell

```
# This will export users from the source tenant with the CustomAttribute1 = "Cross-Tenant-Project"  
# These are the 'target' users to be moved to the northwindtraders tenant
```

```

$outFileUsers = "$home\desktop\UsersToMigrate.txt"
$outFileUsersXML = "$home\desktop\UsersToMigrate.xml"
Get-Mailbox -Filter "CustomAttribute1 -like 'Cross-Tenant-Project'" -ResultSize
Unlimited | Select-Object -ExpandProperty Alias | Out-File $outFileUsers
$mailboxes = Get-Content $outFileUsers
$mailboxes | ForEach-Object {Get-Mailbox $_} | Select-Object
PrimarySMTPAddress, Alias, SamAccountName, FirstName, LastName, DisplayName, Name, Excha
ngeGuid, ArchiveGuid, LegacyExchangeDn, EmailAddresses | Export-Clixml
$outFileUsersXML

```

PowerShell

```

# Copy the file $outfile to the desktop of the target on-premises then run the
below to create MEU in Target
$symbols = '!@#$%^&*'.ToCharArray()
$characterList = @(([char]([char]'a'..[char]'z')), [char]([char]'A'..
[char]'Z'), [char]([char]'0'..[char]'9') + $symbols)

function GeneratePassword {
    param(
        [ValidateRange(12, 256)]
        [int]
        $length = 16
    )

    do {
        $password = -join (0..$length | ForEach-Object { $characterList | Get-
Random })
        [int]$hasLowerChar = $password -cmatch '[a-z]'
        [int]$hasUpperChar = $password -cmatch '[A-Z]'
        [int]$hasDigit = $password -match '[0-9]'
        [int]$hasSymbol = $password.IndexOfAny($symbols) -ne -1
    }

    until (($hasLowerChar + $hasUpperChar + $hasDigit + $hasSymbol) -ge 3)

    $password | ConvertTo-SecureString -AsPlainText
}

$mailboxes = Import-Clixml $home\desktop\UsersToMigrate.xml
foreach ($m in $mailboxes) {
    $organization = "@contoso.onmicrosoft.com"
    $mosi = $m.Alias + $organization
    $Password = GeneratePassword
    $x500 = "x500:" + $m.LegacyExchangeDn
    $tmpUser = New-MailUser -MicrosoftOnlineServicesID $mosi -PrimarySmtpAddress
$mosi -ExternalEmailAddress $m.PrimarySmtpAddress -FirstName $m.FirstName -
LastName $m.LastName -Name $m.Name -DisplayName $m.DisplayName -Alias $m.Alias -
Password $Password
    $tmpUser | Set-MailUser -EmailAddresses @{add = $x500 } -ExchangeGuid
$m.ExchangeGuid -ArchiveGuid $m.ArchiveGuid -CustomAttribute1 "Cross-Tenant-
Project"
    $tmpx500 = $m.EmailAddresses | Where-Object { $_ -match "x500" }
    $tmpx500 | ForEach-Object { Set-MailUser $m.Alias -EmailAddresses @{add =
"$_" } }
}

```

```
# Now synchronize the changes from On-Premises to Azure and Exchange Online in  
the target tenant  
# This action should create the target mail enabled users (MEUs) in the Target  
tenant  
Start-ADSyncSyncCycle
```

How do we access Outlook on Day 1 after the user mailbox is moved?

Since only one tenant can own a domain, the former primary SMTPAddress won't be associated to the user in the target tenant when the mailbox move completes; only those domains associated with the new tenant. Outlook uses the user's new UPN to authenticate to the service, and the Outlook profile expects to find the legacy primary SMTPAddress to match the mailbox in the target system. Since the legacy address isn't in the target system, the outlook profile won't connect to find the newly moved mailbox.

For this initial deployment, users will need to rebuild their profile with their new UPN, primary SMTP address and resync OST content.

① Note

Plan accordingly as you batch your users for completion. You need to account for network utilization and capacity when Outlook client profiles are created and subsequent OST and OAB files are downloaded to clients.

What Exchange RBAC roles do I need to be member of to set up or complete a cross-tenant move?

There's a matrix of roles based on assumption of delegated duties when executing a mailbox move. Currently, two roles are required:

- The first role is for a one-time setup task that establishes the authorization of moving content into or out of your tenant/organizational boundary. As moving data out of your organizational control is a critical concern for all companies, we opted for the highest assigned role of **Organization Administrator**. This role must alter or set up a new OrganizationRelationship that defines the `-MailboxMoveCapability` setting with the remote organization. Only the organization administrator can alter the `-MailboxMoveCapability` setting, while other attributes on the OrganizationRelationship can be managed by the Federated Sharing administrator.
- The role of executing the actual move commands can be delegated to a lower-level function. The role of **Move Mailboxes** is assigned to the capability of moving mailboxes in or out of the organization.

How do we target which SMTP address is selected for targetAddress (TargetDeliveryDomain) on the converted mailbox (to MailUser conversion)?

Exchange mailbox moves using MRS craft the targetAddress on the original source mailbox when converting to a MailUser by matching an email address (proxyAddress) on the target object. The process takes the `-TargetDeliveryDomain` value passed into the command, then checks for a matching proxy for that domain on the target side. When we find a match, the matching proxyAddress is used to set the ExternalEmailAddress (targetAddress) on the converted mailbox (now MailUser) object.

How does mail flow work after migration?

Cross-Tenant mail flow after migration works similar to Exchange Hybrid mail flow. Each migrated mailbox needs the source MailUser with the correct target address to forward incoming mail from source tenant to mailboxes in target tenant. Transport rules, security and compliance features will run as configured in each tenant that the mail flows through. So, for inbound mail, features like anti-spam, anti-malware, quarantine, transport rules and journaling rules will run in the source tenant first, then in the target tenant.

How do mailbox permissions transition?

Mailbox permissions include Send on Behalf of and Mailbox Access:

- Send On Behalf Of (AD:publicDelegates) stores the DN of recipients with access to a user's mailbox as a delegate. This value is stored in the Active Directory and currently doesn't move as part of the mailbox transition. If the source mailbox has publicDelegates set, you'll need to restamp the publicDelegates on the target Mailbox once the MEU to Mailbox conversion completes in the target environment by running `Set-Mailbox <principal> -GrantSendOnBehalfTo <delegate>`.
- Mailbox Permissions that are stored in the mailbox will move with the mailbox when both the principal and the delegate are moved to the target system. For example, the user *TestUser7* is granted *FullAccess* to the mailbox *TestUser_8* in the tenant *SourceCompany.onmicrosoft.com*. After the mailbox moves complete to *TargetCompany.onmicrosoft.com*, the same permissions are set up in the target directory. Examples using `_Get-MailboxPermission` for *TestUser_7* in both source and target tenants are shown below. Exchange cmdlets are prefixed with source and target accordingly.

Here's an example of the output of the mailbox permission before a move from the source side:

PowerShell

```
Get-MailboxPermission TestUser_7 | Format-Table -AutoSize User, AccessRights, IsInherited, Deny
```

User	AccessRights
IsInherited Deny	
-----	-----
NT AUTHORITY\SELF	{FullAccess, ReadPermission}
False False	
TestUser_8@contoso.onmicrosoft.com	{FullAccess}
False False	

Here's an example of the output of the mailbox permission after the move from the target side:

PowerShell

```
Get-MailboxPermission TestUser_7 | Format-Table -AutoSize User, AccessRights, IsInherited, Deny
```

User	AccessRights
IsInherited Deny	
-----	-----
NT AUTHORITY\SELF	{FullAccess, ReadPermission}
False False	
TestUser_8@northwindtraders.onmicrosoft.com	{FullAccess}
False False	

ⓘ Note

Cross-tenant mailbox and calendar permissions aren't supported. You must organize principals and delegates into consolidated move batches so that these connected mailboxes are transitioned at the same time from the source tenant.

What X500 proxy should be added to the target MailUser proxy addresses to enable migration?

The cross-tenant mailbox migration requires that the LegacyExchangeDN value of the source mailbox object be stamped as an x500 email address on the target MailUser object.

Example:

PowerShell

```
LegacyExchangeDN value on source mailbox is:  
/o=First Organization/ou=Exchange Administrative  
Group(FYDIBOHF23SPDLT)/cn=Recipients/cn=d11ec1a2cacd4f81858c81907273f1f9Lara
```

so, the x500 email address to be added to target MailUser object would be:
x500:/o=First Organization/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=d11ec1a2cacd4f81858c81907273f1f9-Lara

ⓘ Note

In addition to this X500 proxy, you will need to copy all X500 proxies from the mailbox in the source to the mailbox in the target. While rare, you could also run across an X400 proxy address on a mailbox, while not a requirement for the move to complete, it is recommended that you also stamp this address on the target mail user object.

Can the source and target tenants utilize the same domain name?

No, the source tenant and target tenant domain names must be unique, for example, a source domain of contoso.com and the target domain of northwindtraders.com.

Will shared mailboxes move and still work?

Yes. However, we only keep the store permissions as described in this article:

- [Manage permissions for recipients in Exchange Online](#)

Do you have any recommendations for batches?

Don't exceed 2,000 mailboxes per batch. We strongly recommend submitting batches two weeks prior to the cut-over date as there's no impact on the end users during synchronization. If you need guidance for mailboxes quantities over 50,000, you can reach out to your CSAM or open a support request.

What if I use Service encryption with Microsoft Purview Customer Key?

The mailbox is decrypted prior to moving. Ensure Customer Key is configured in the target tenant if it's still required. For more information, see [here](#).

What is the estimated migration time?

To help you plan your migration, the table present [here](#) shows the guidelines about when to expect bulk mailbox migrations or individual migrations to complete. These estimates are

based on a data analysis of previous customer migrations. As every environment is unique, your exact migration velocity can vary.

Protecting documents in the source tenant consumable by users in the destination tenant.**

Cross-tenant migration only migrates mailbox data and nothing else. There are multiple other options, which are documented in the following blog post that may help:

[https://techcommunity.microsoft.com/t5/security-compliance-and-identity/mergers-and-spinoffs/ba-p/910455 ↗](https://techcommunity.microsoft.com/t5/security-compliance-and-identity/mergers-and-spinoffs/ba-p/910455)

Can I have the same labels in the destination tenant as you had in the source tenant, either as the only set of labels or an additional set of labels for the migrated users depending on alignment between the organizations.**

Because cross-tenant migrations don't export labels and there's no way to share labels between tenants, you can only achieve this objective by recreating the labels in the destination tenant.

Do you support moving Microsoft 365 Groups?

Currently the cross-tenant mailbox migrations feature doesn't support the migration of Microsoft 365 Groups.

Can a source tenant admin perform an eDiscovery search against a mailbox after the mailbox has been migrated to the new/target tenant?

No, after a cross-tenant mailbox migration, eDiscovery against the migrated user's mailbox in the source doesn't work. This eDiscovery failure is because there's no longer a mailbox in the source to search for as the mailbox has been migrated to the target tenant and now belongs to the target tenant. eDiscovery after mailbox migration can only be done in the target tenant (where the mailbox now exists). If a copy of the source mailbox needs to persist in the source tenant after migration, the administrator in the source tenant can copy the contents to an alternate mailbox pre-migration for future eDiscovery operations against the data.

At which point will the destination MailUser be converted to a destination mailbox and the source mailbox converted to a source MailUser?

These conversions happen automatically during the migration process. No manual steps are necessary.

At which step should I assign the Exchange Online license to destination MailUsers?

This license assignation can be done before the migration is complete, but you shouldn't assign a license prior to stamping the *ExchangeGUID* attribute; else, the conversion of MailUser object to mailbox will fail and a new mailbox will be created instead. To mitigate this risk, it's best to wait until the migration is complete and assign licenses during the 30-day grace period.

Can I use Microsoft Entra Connect to sync users to the new tenant if I'm keeping the on-premises Active Directory?

Yes. It's possible to have two instances of Microsoft Entra Connect synchronize to different tenants. However, there are some things you need to be aware of:

- Preprovisioning the user's accounts with the script provided in this article shouldn't be done. Instead, a selective OU sync of the users in scope for the migration can be performed to populate the target tenant. You'll receive a warning about the UPN not matching during Microsoft Entra Connect configuration.
- Depending on your current state of hybrid Exchange, you need to verify that the on-premises directory objects have the required attributes (such as *msExchMailboxGUID* and *proxyAddresses*) populated correctly before attempting to sync to another tenant; else you'll run into issues with double mailboxes and migration failures.
- You must take some extra steps to manage UPN transitioning, changing it on-premises once the migration has been completed for a user unless you're also moving the custom domain during a cut-over migration.

How should I handle mailboxes that are close to, or over quota.

Mailboxes nearing their quota prior to migration may end up over quota either before or during the actual migration. If this happens, these mailboxes will fail migration and will need to be remediated and restarted. To mitigate this, it is recommend the source tenant admin identify mailboxes at or near quota prior to migration and take the necessary steps to either reduce the mailbox size, provision a primary archive or in some cases enable auto expanding archives for the user's mailboxes.

 Note

Once enabling an archive or auto expanding archive for a user, ensure the correct archiving policies are applied to the user and the process is run to move the mailbox data to its new location and free up space.

Do auto-expanded archive mailboxes move?

Issue: Auto Expanded archives cannot be migrated. Yes, if the user in source has auto-expanding archives enabled and has additional auxiliary archives, cross-tenant mailbox migration will work. We support moving users that have no more than 12 auxiliary archive mailboxes. Additionally, users with large primary, large main archive, and large auxiliary archive mailboxes will require extra time to synchronize and should be submitted well in advance of the cut-over date. If the source mailbox is expanded during the mailbox migration process, the migration will fail as a new auxiliary archive will be created in the source, but not in the target. In this case, you'll need to remove the user from the batch and resubmit them.

Can I perform a cross cloud tenant to tenant migration?

Cross cloud tenant to tenant migration is not supported. An example scenario would be moving from Office 365 Worldwide to Office 365 Government Cloud.

Are voicemails migrated cross tenant?

Yes, voicemails are migrated cross tenant.

- Received voicemails in email as attachments are available in the target mailbox.
- Received voicemails are available in Teams if you call voicemail and listen to saved messages. (VMs received in source are available as saved messages)
- Received voicemails are not available in Teams client UI in target post migration.
- The voicemail greeting is also migrated to the target.

Are mailbox signatures migrated cross tenant?

Mailbox signatures are not migrated cross tenant and must be recreated.

Known issues

- Post-migration Teams functionality in the source tenant will be limited. After the mailbox is migrated to the target tenant, Teams in the source tenant no longer has access to the user's mailbox. If a user signs in to Teams with the source tenant credential, there's a loss of functionality such as the inability to update their profile picture, no calendar application, and an inability to search and join public teams.

- Cloud MailUsers with non-owned smtp proxyAddress block MRS moves. When creating target tenant MailUser objects, you must ensure that all SMTP proxy addresses belong to the target tenant organization. If an SMTP proxyAddress exists on the target mail user that doesn't belong to the local tenant, the conversion of the MailUser to a mailbox is prevented. This prevention is due to our assurance that mailbox objects can only send mail from domains for which the tenant is authoritative (domains claimed by the tenant).
- If you synchronize users from on-premises using Microsoft Entra Connect in the target tenant, then you can provision on-premises MailUser objects with ExternalEmailAddress pointing to the source tenant where the mailbox exists (LaraN@contoso.onmicrosoft.com), and you stamp the PrimarySMTPAddress as a domain that resides in the target tenant (Lara.Newton@northwindtraders.com). These values synchronize down to the tenant and an appropriate mail user is provisioned and is ready for migration. An example object is shown here.

PowerShell

```
Get-MailUser LaraN | select ExternalEmailAddress, EmailAddresses

ExternalEmailAddress           EmailAddresses
-----
SMTP:LaraN@contoso.onmicrosoft.com {SMTP:lara.newton@northwindtraders.com}
```

 **Note**

The *contoso.onmicrosoft.com* address is *not* present in the EmailAddresses/proxyAddresses array.

- MailUser objects with "external" primary SMTP addresses are modified/reset to "internal" company-claimed domains.

MailUser objects are pointers to non-local mailboxes. In the case for cross-tenant mailbox migrations, we use MailUser objects to represent either the source mailbox (from the target organization's perspective) or target mailbox (from the source organization's perspective). The MailUsers will have an ExternalEmailAddress (targetAddress) that points to the smtp address of the actual mailbox (ProxyTest@northwindtraders.onmicrosoft.com) and primarySMTP address that represents the displayed SMTP address of the mailbox user in the directory. Some organizations choose to display the primary SMTP address as an external SMTP address, not as an address owned/verified by the local tenant (for example, as northwindtraders.com rather than as contoso.com). However, once an Exchange service plan object is applied to the MailUser via licensing operations, the primary SMTP address is modified to show as a domain verified by the local organization (contoso.com). There are two potential reasons:

- When any Exchange service plan is applied to a MailUser, the Microsoft Entra ID process starts to enforce proxy scrubbing to ensure that the local organization isn't able to send out mail, spoof, or mail from another tenant. Any SMTP address on a recipient object with these service plans will be removed if the address isn't verified by the local organization. As is the case in the example, the northwindtraders.com domain isn't verified by the contoso.onmicrosoft.com tenant; therefore, the scrubbing removes that northwindtraders.com domain. If you wish to persist these external domains on MailUser, either before or after the migration, you need to alter your migration processes to strip licenses after the move completes or before the move to ensure that the users have the expected external branding applied. You'll need to ensure that the mailbox object is properly licensed to not affect mail service. An example script to remove the service plans on a MailUser in the contoso.onmicrosoft.com tenant is shown here.

 **Note**

The following script uses Microsoft Graph Powershell. For more information, see [Microsoft Graph PowerShell overview](#).

For information about how to use different methods to authenticate `Connect-Graph` in an unattended script, see the article [Authentication module cmdlets in Microsoft Graph PowerShell](#).

PowerShell

```
# Connect to Microsoft Graph
Connect-Graph -Scopes User.ReadWrite.All, Organization.Read.All

# Get licensing plans and include disabled plans
$EmsSku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'ENTERPRISEPREMIUM'
$user = Get-MgUser -UserId LaraN@contoso.onmicrosoft.com
$userLicense = Get-MgUserLicenseDetail -UserId $user.Id

$userDisabledPlans = $userLicense.ServicePlans |
    Where ProvisioningStatus -eq "Disabled" |
    Select -ExpandProperty ServicePlanId

$newDisabledPlans = $EmsSku.ServicePlans |
    Where ServicePlanName -in
('LOCKBOX_ENTERPRISE', 'EXCHANGE_S_ENTERPRISE', 'INFORMATION_BARRIERS', 'MIP_S_CLP2',
'MIP_S_CLP1', 'MYANALYTICS_P2', 'EXCHANGE_ANALYTICS', 'EQUIVIO_ANALYTICS', 'THREAT_INTELLIGENCE',
'PAM_ENTERPRISE', 'PREMIUM_ENCRYPTION') |
    Select -ExpandProperty ServicePlanId

$disabledPlans = $userDisabledPlans + $newDisabledPlans | Select -Unique

$addLicenses = @(
    @{SkuId = $EmsSku.SkuId
    DisabledPlans = $disabledPlans
    }
)
```

```

Set-MgUserLicense -UserId '38955658-c844-4f59-9430-6519430ac89b' -AddLicenses
$addLicenses -RemoveLicenses @()

Id                               DisplayName   Mail UserPrincipalName
UserType
--                               -----
38955658-c844-4f59-9430-6519430ac89b Bianca Pisani
BiancaP@contoso.onmicrosoft.com      Member

```

Results in the set of ServicePlans assigned are shown here:

```

PowerShell

$order = @(
    @{ Expression = 'ProvisioningStatus'; Ascending = $true }
)
Get-MgUserLicenseDetail -UserId '38955658-c844-4f59-9430-6519430ac89b' | Select-
Object -ExpandProperty ServicePlans | sort ProvisioningStatus $order

AppliesTo ProvisioningStatus ServicePlanId
ServicePlanName
----- ----- -----
-
User      Success          2e2ddb96-6af9-4b1d-a3f0-d6ecfd22edb2
ADALLOM_S_STANDALONE
User      Success          6c6042f5-6f01-4d67-b8c1-eb99d36eed3e STREAM_0365_E5
User      Success          e212cbc7-0961-4c40-9825-01117710dcbb FORMS_PLAN_E5
User      Success          07699545-9485-468e-95b6-2fca3738be01 FLOW_0365_P3
User      Success          9c0dab89-a30c-4117-86e7-97bda240acd2
POWERAPPS_0365_P3
User      Success          871d91ec-ec1a-452b-a83f-bd76c7d770ef WINDEFATP
User      Success          21b439ba-a0ca-424f-a6cc-52f954a5b111
WIN10_PRO_ENT_SUB
User      Success          57ff2da0-773e-42df-b2af-ffb7a2317929 TEAMS1
User      Success          8c7d2df8-86f0-4902-b2ed-a0458298f3b3 Deskless
User      Success          8e0c0a52-6a6c-4d40-8370-dd62790dc70
THREAT_INTELLIGENCE
User      Success          4a51bca5-1eff-43f5-878c-177680f191af
WHITEBOARD_PLAN3
User      Success          efb0351d-3b08-4503-993d-383af8de41e3 MIP_S_CLP2
User      Success          617b097b-4b93-4ede-83de-5f075bb5fb2f
PREMIUM_ENCRYPTION
User      Success          8c098270-9dd4-4350-9b30-ba4703f3b36b ADALLOM_S_0365
Company   Success          94065c59-bc8e-4e8b-89e5-5138d471eaff
MICROSOFT_SEARCH
User      Success          14ab5db5-e6c4-4b20-b4bc-13e36fd2227f ATA
User      Success          3fb82609-8c27-4f7b-bd51-30634711ee67 BPOS_S_TODO_3
User      Success          b1188c4c-1b36-4018-b48b-ee07604f6feb PAM_ENTERPRISE
User      Success          5136a095-5cf0-4aff-bec3-e84448b38ea5 MIP_S_CLP1
User      Success          33c4f319-9bdd-48d6-9c4d-410b750a4a5a MYANALYTICS_P2
User      Success          5689bec4-755d-4753-8b61-40975025187c RMS_S_PREMIUM2
User      Success          4828c8ec-dc2e-4779-b502-87ac9ce28ab7 MCOEV
User      Success          9f431833-0334-42de-a7dc-70aa40db46db
LOCKBOX_ENTERPRISE

```

User	Success	3e26ee1f-8a5f-4d52-aee2-b81ce45c8f40	MCOMEETADV
User	Success	43de0ff5-c92c-492b-9116-175376d08c38	
OFFICESUBSCRIPTION			
User	Success	0feaeb32-d00e-4d66-bd5a-43b5b83db82c	MCOSTANDARD
User	Success	70d33638-9c74-4d01-bfd3-562de28bd4ba	BI_AZURE_P2
Company	Success	f20fedf3-f3c3-43c3-8267-2bfdd51c0939	ATP_ENTERPRISE
User	Success	4de31727-a228-4ec3-a5bf-8e45b5ca48cc	
EQUIVIO_ANALYTICS			
User	Success	efb87545-963c-4e0d-99df-69c6916d9eb0	
EXCHANGE_S_ENTERPRISE			
User	Success	34c0d7a0-a70f-4668-9238-47f9fc208882	
EXCHANGE_ANALYTICS			
User	Success	8a256a2b-b617-496d-b51b-e76466e88db0	MFA_PREMIUM
User	Success	41781fb2-bc02-4b7c-bd55-b576c07bb09d	AAD_PREMIUM
User	Success	bea4c11e-220a-4e6d-8eb8-8ea15d019f90	
RMS_S_ENTERPRISE			
User	Success	eed0eb4f-6444-4f95-aba0-50c24d67f998	AAD_PREMIUM_P2
User	Success	6c57d4b6-3b23-47a5-9bc9-69f17b4947b3	RMS_S_PREMIUM
User	Success	5dbe027f-2339-4123-9542-606e4d348a72	
SHAREPOINTENTERPRISE			
User	Success	b737dad2-2f6c-4c65-90e3-ca563267e8b9	
PROJECTWORKMANAGEMENT			
User	Success	e95bec33-7c88-4a70-8e19-b10bd9d0c014	SHAREPOINTWAC
User	Success	7547a3fe-08ee-4ccb-b430-5077c5041653	
YAMMER_ENTERPRISE			
User	Success	a23b959c-7ce8-4e57-9140-b90eb88a9e97	SWAY
User	Success	c4801e8a-cb58-4c35-acab-f2dcc106f287	
INFORMATION_BARRIERS			
User	Success	b76fb638-6ba6-402a-b9f9-83d28acb3d86	
VIVA_LEARNING_SEEDED			
Company	Success	db4d623d-b514-490b-b7ef-8885eee514de	Nucleus
Company	Success	6f23d6a9-adbf-481c-8538-b4c095654487	
M365_LIGHTHOUSE_CUSTOMER_PLAN1			
User	Success	a82fbf69-b4d7-49f4-83a6-915b2cf354f4	
VIVAENGAGE_CORE			
User	Success	9a6eeb79-0b4b-4bf0-9808-39d99a2cd5a3	
Windows_Autopatch			
User	Success	cd31b152-6326-4d1b-ae1b-997b625182e6	MIP_S_Exchange
User	Success	a413a9ff-720c-4822-98ef-2f37c2a21f4c	
MICROSOFT_COMMUNICATION_COMPLIANCE			
User	Success	795f6fe0-cc4d-4773-b050-5dde4dc704c9	
UNIVERSAL_PRINT_01			
Company	Success	2b815d45-56e4-4e3a-b65c-66cb9175b560	
ContentExplorer_Standard			
User	Success	7bf960f6-2cd9-443a-8046-5dbff9558365	
WINDOWSUPDATEFORBUSINESS_DEPLOYMENTSERVICE			
User	Success	3ec18638-bd4c-4d3b-8905-479ed636b83e	
CustomerLockboxA_Enterprise			
User	Success	3efbd4ed-8958-4824-8389-1321f8730af8	
MESH_AVATARS_ADDITIONAL_FOR_TEAMS			
User	Success	99cd49a9-0e54-4e07-aea1-d8d9f5f704f5	
Defender_for_Iot_Enterprise			
User	Success	0898bdbb-73b0-471a-81e5-20f1fe4dd66e	
KAIZALA_STANDALONE			
User	Success	c948ea65-2053-4a5a-8a62-9eaaaf11b522	
PURVIEW_DISCOVERY			
User	Success	a1ace008-72f3-4ea0-8dac-33b3a23a2472	CLIPCHAMP
User	Success	f6de4823-28fa-440b-b886-4783fa86ddba	

M365_AUDIT_PLATFORM		
User Success	0d0c0d31-fae7-41f2-b909-eaf4d7f26dba	
Bing_Chat_Enterprise		
User Success	dcf9d2f4-772e-4434-b757-77a453cfbc02	
MESH_AVATARS_FOR_TEAMS		
User Success	c4b8c31a-fb44-4c65-9837-a21f55fcabda	MICROSOFT_LOOP
User Success	a6520331-d7d4-4276-95f5-15c0933bc757	
GRAPH_CONNECTORS_SEARCH_INDEX		
User Success	e26c2 <color>fcc-ab91</color> -4a61-b35c-03cdc8dddff66	
INFO_GOVERNANCE		
User Success	46129a58-a698-46f0-aa5b-17f6586297d9	
DATA_INVESTIGATIONS		
User Success	9d0c4ee5-e4a1-4625-ab39-d82b619b1a34	
INSIDER_RISK_MANAGEMENT		
User Success	65cc641f-cccd-4643-97e0-a17e3045e541	
RECORDS_MANAGEMENT		
User Success	d2d51368-76c9-4317-ada2-a12c004c432f	
ML_CLASSIFICATION		
User Success	bf6f5520-59e3-4f82-974b-7dbbc4fd27c7	SAFEDOCS
User Success	2f442157-a11c-46b9-ae5b-6e39ff4e5849	
M365_ADVANCED_AUDITING		
User Success	41fcdd7d-4733-4863-9cf4-c65b83ce2df4	
COMMUNICATIONS_COMPLIANCE		
User Success	6db1f1db-2b46-403f-be40-e39395f08dbb	CUSTOMER_KEY
User Success	6dc145d6-95dd-4191-b9c3-185575ee6f6b	
COMMUNICATIONS_DLP		
User Success	199a5c09-e0ca-4e37-8f7c-b05d533e1ea2	
MICROSOFTBOOKINGS		
User Success	ded3d325-1bdc-453e-8432-5bac26d7a014	
POWER_VIRTUAL_AGENTS_0365_P3		
Company Success	d9fa6af4-e046-4c89-9226-729a0786685d	
Content_Explorer		
User Success	afa73018-811e-46e9-988f-f75d2b1b8430	CDS_0365_P3
User Success	b21a6b06-1988-436e-a07b-51ec6d9f52ad	
PROJECT_0365_P3		
User Success	64bfac92-2b17-4482-b5e5-a0304429de3e	
MICROSOFTENDPOINTDLP		
User Success	bf28f719-7844-4079-9c78-c1307898e192	MTP
User Success	28b0fa46-c39a-4188-89e2-58e979a6b014	
DYN365_CDS_0365_P3		
User Success	d587c7a3-bda9-4f99-8776-9bcf59c84f75	INSIDER_RISK
User Success	531ee2f8-b1cb-453b-9c21-d2180d014ca5	EXCEL_PREMIUM
User PendingProvisioning	f0ff6ac6-297d-49 <color>cd-be34</color> -6dfef97f0c28	
MESH_IMMERSIVE_FOR_TEAMS		
User PendingInput	c1ec4a95-1f05-45b3-a911-aa3fa01094f5	INTUNE_A
Company PendingActivation	882e1d05-acd1-4ccb-8708-6ee03664b117	INTUNE_0365

The user's PrimarySMTPAddress is no longer scrubbed. The northwindtraders.com domain isn't owned by the contoso.onmicrosoft.com tenant and will persist as the primary SMTP address shown in the directory.

Here's an example:

PowerShell

```
Get-Recipient ProxyTest | Format-Table -AutoSize UserPrincipalName,
PrimarySmtpAddress, ExternalEmailAddress, ExternalDirectoryObjectId
UserPrincipalName           PrimarySmtpAddress
ExternalEmailAddress         ExternalDirectoryObjectId
-----
-----
ProxyTest@contoso.com       ProxyTest@contoso.com
SMTP:ProxyTest@contoso.com   e2513482-1d5b-4066-936a-cbc7f8f6f817
```

When `msExchRemoteRecipientType` is set to 8 (DeprovisionMailbox), for on-premises MailUsers that are migrated to the target tenant, the proxy scrubbing logic in Azure removes non-owned domains and reset the primarySMTP to an owned domain. With the `msExchRemoteRecipientType` in the on-premises MailUser being cleared, the proxy scrub logic no longer applies.

Below is the full set of current service plans that include Exchange Online:

[\[+\] Expand table](#)

Name
eDiscovery (Premium) Storage (500 GB)
Customer Lockbox
Data Loss Prevention
Exchange Enterprise CAL Services (EOP, DLP)
Exchange Essentials
Exchange Foundation
Exchange Online (P1)
Exchange Online (Plan 1)
Exchange Online (Plan 2)
Exchange Online Archiving for Exchange Online
Exchange Online Archiving for Exchange Server
Exchange Online Inactive User Add-on
Exchange Online Kiosk
Exchange Online Multi-Geo
Exchange Online Plan 1
Exchange Online POP

Name
Exchange Online Protection
Graph Connectors Search with Index
Information Barriers
Information Protection for Office 365 - Premium
Information Protection for Office 365 - Standard
Insights by MyAnalytics
Microsoft Information Governance
Microsoft Purview Audit (Premium)
Microsoft Bookings
Microsoft Business Center
Microsoft Data Investigations
Microsoft MyAnalytics (Full)
Microsoft Communications Compliance
Microsoft Communications DLP
Microsoft Customer Key
Microsoft 365 Advanced Auditing
Microsoft Records Management
Office 365 eDiscovery (Premium)
Office 365 Advanced eDiscovery
Microsoft Defender for Office 365 (Plan 1)
Microsoft Defender for Office 365 (Plan 2)
Office 365 Privileged Access Management
Premium Encryption in Office 365

Migration Failures

- MailboxNotInCrossTenantMigrationScopeException

Ensure the migration scope is set up correctly on the source tenant and that MailboxMovesPublishedScopes is set in the organization relationship with the target

tenant.

Verify that the mailbox to be migrated has been added to the security group in the source tenant.

After adding user to correct security group, resume the migration batch.

- AuxArchiveNotFoundInTargetRecipientException

This failure is because the user was not in the migration scope when batch was started and the user has AuxArchive on the source.

Add user to the correct security group on source target.

Remove the migration user from the batch.

Remove users with the following command:

PowerShell

```
Get-MigrationUser -Identity LaraN@contoso.onmicrosoft.com -  
IncludeAssociatedUsers | Remove-MigrationUser
```

Add user to new batch.

- MailboxIsNotInExpectedDBException

This failure is due to internal Microsoft maintenance.

Remove the migration user from the batch.

Remove users with the following command:

PowerShell

```
Get-MigrationUser -Identity LaraN@contoso.onmicrosoft.com -  
IncludeAssociatedUsers | Remove-MigrationUser
```

Add user to new batch.

- NotAcceptedDomainException

There is an invalid proxy address stamped on the target user. An example would be where a user in contoso.onmicrosoft.com had a proxy address of fabrikam.onmicrosoft.com, which is the source tenant.

Remove the invalid proxy address using the following command:

PowerShell

```
Set-MailUser LaraN@contoso.onmicrosoft.com -EmailAddress  
@{remove="smtp:LaraN@northwindtraders.onmicrosoft.com"}
```

Resume the migration batch.

- **SourceAuxArchiveIsProvisionedDuringCrossTenantMovePermanentException**

A new AuxArchive was provisioned during migration.

Remove the migration user from the batch.

Remove users with the following command:

PowerShell

```
Get-MigrationUser -Identity LaraN@contoso.onmicrosoft.com -  
IncludeAssociatedUsers | Remove-MigrationUser
```

Add user to new batch.

- **UserDuplicateInOtherBatchException**

User exists in another batch already.

Remove the migration user from the batch.

Remove users with the following command:

PowerShell

```
Get-MigrationUser -Identity LaraN@contoso.onmicrosoft.com -  
IncludeAssociatedUsers | Remove-MigrationUser
```

Add user to new batch.

- **MissingExchangeGuidException**

The target mailuser object is missing the correct ExchangeGuid value.

Update the ExchangeGuid with the following command:

PowerShell

```
Set-MailUser LaraN@contoso.onmicrosoft.com -ExchangeGuid 4e3188c6-39f5-4387-  
adc7-b355b6b852c8
```

Resume migration batch.

- **SourceMailboxAlreadyBeingMovedPermanentException**

The source mailbox already has an existing move request. Investigate and remove the existing move. It is possible that this is an internal Microsoft move and you will need to wait for the move to complete.

Remove the migration user from the batch.

Remove users with the following command:

PowerShell

```
Get-MigrationUser -Identity LaraN@contoso.onmicrosoft.com -  
IncludeAssociatedUsers | Remove-MigrationUser
```

Add user to new batch after the original move has been removed or completed.

- UserAlreadyHasDemotedArchiveException

The user had an archive mailbox previously that was disabled. Choose one of the two following options to resolve this issue.

Permanently delete the disabled archive mailbox, this is unreversible. Set-Mailbox - RemoveDisabledArchive LaraN@contoso.onmicrosoft.com

Re-enable the disabled archive mailbox with the following command:

PowerShell

```
Enable-Mailbox -Archive mailbox@contoso.onmicrosoft.com.
```

If you re-enable the disabled archive mailbox, you will need to update the archive guid on the target mailuser object.

Resume migration batch.

See also

- [Manage Microsoft 365 with PowerShell](#)
- [Get started with the Microsoft Graph PowerShell SDK](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Cross-Tenant Identity Mapping (preview)

Article • 03/07/2023

Cross-Tenant Identity Mapping is a feature that can be used during Cross-Tenant User Data Migrations from one Microsoft 365 organization to another. It provides a secure method of establishing one-to-one object relationships across organization boundaries, and automatically prepares the target objects for a successful migration.

ⓘ Note

Cross-Tenant Identity Mapping is in a private preview stage of development. As an unfinished project any information or availability is subject to change at any time. Support for private-preview customers will be handled via email. Cross-Tenant Identity Mapping is covered by the [preview terms of the Microsoft Universal License Terms for Online Services](#).

Benefits of using Cross-Tenant Identity Mapping

Cross-Tenant Identity Mapping removes the need to export large data sets from a source organization for the sole purpose of configuring Mail Enabled User objects in the target organization.

With Cross-Tenant Identity Mapping, data remains within the Microsoft security boundary and is securely copied directly from the source organization to the target organization using specially configured **Organization Relationships** serving as a unidirectional trust.

Using Cross-Tenant Identity Mapping reduces mistakes when configuring target objects for a migration by automatically configuring values such as *ExchangeGuid*, *ArchiveGuid*, and all necessary *X500 proxy addresses*.

Some additional benefits of using Cross-Tenant Identity Mapping:

- Reduces the number of manual processes where a mistake may result in failed migrations
- Automates identification of objects within scope to migrate from the source organization to the target organization

- Establishes a 1:1 map of a Mailbox User object in the source organization to a pre-existing Mail Enabled User object in the target organization
- Automates population of required attributes from the source organization Mailbox User to the target organization Mail Enabled User
- Provides a list of objects prepared and ready for [cross-tenant mailbox migration](#) based on the source organization users' primarySMTPAddress value

FAQ about Cross-Tenant Identity Mapping

We would like to provide information commonly asked so you may evaluate if you would like to participate in the private preview.

- The feature is only intended to be used with [Cross-tenant mailbox migration](#), and not with any third-party non-Microsoft migration solutions.
- Data processing (storage, compute, transfer, etc.) is currently within the European Union, and within the Exchange Online home region of the organizations participating in the migration.
 - For Multi-Geo enabled organizations, the organization's home geo for Exchange Online will be used.
- This feature can currently only be enabled in the worldwide Microsoft 365 offering. It doesn't work in GCC, GCC High, DoD, Office 365 by 21 Vianet, etc.
- Cross-Tenant Identity Mapping does **not** create the Mail Enabled User objects in the target tenant for you. These objects must still be created with a minimal attribute set. Once created, then Cross-Tenant Identity Mapping decorates their attributes correctly for a mailbox migration to proceed.
- Some familiarity with PowerShell is currently required as the feature is PowerShell-based
- The feature communicates over an encrypted connection to a REST endpoint.
- The feature currently requires the Global Administrator role for initial setup. This behavior may change in a future update.
- Organizational Relationships are used as a dual handshake approach to ensure both organizations have authorized this transaction type to take place.
- It works with cloud-only or hybrid organizations.
- Target organizations in a hybrid configuration require Microsoft supported on-premises object management tools to modify any Mail Enabled User objects synchronized from the on-premises directory.

What does participating in the private preview entail?

We're looking for customers willing to both try Cross-Tenant Identity Mapping and to provide feedback based on their experience. Did it make the migration easier for you compared to earlier migrations you've performed? Are there features you feel are missing? All constructive feedback is welcomed.

How to participate

The Cross-Tenant User Content Migration feature and licenses are currently only available to Enterprise Agreement customers. If you are an Enterprise Agreement customer who will be purchasing Cross-Tenant User Content Migration licenses, and you would like to evaluate Cross-Tenant Identity Mapping to improve your migration experience, then please email CTIMPreview@service.microsoft.com and provide some basic information about the migration you are performing. The team will respond to you within a couple business days with some additional questions. For more information on licensing, please see [Cross-Tenant User Content Migration Licensing](#) and contact your Microsoft account team.

Next steps

We recommend reviewing the current Cross-Tenant Mailbox Migration steps related to preparing target user objects for migration as this preparation is what Cross-Tenant Identity Mapping will automate.

- Review [Cross-Tenant Mailbox Migration](#)
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Plan for multitenant organizations in Microsoft 365

Article • 06/24/2024

ⓘ Note

Multitenant organizations is not available in Microsoft 365 China (operated by 21Vianet). If your organization manages multiple Microsoft 365 tenants, you can set up a multitenant organization in Microsoft 365 to facilitate collaboration and resource access between tenants. Creating a multitenant organization and synchronizing users between tenants provides a more seamless collaboration experience between the users in different tenants when [searching for each other](#), using Microsoft Teams and meetings, and collaborating on files.

The tenant that creates the multitenant organization is known as the *owner* while other tenants that join the multitenant organization are known as *members*. Once the global administrator in the owner tenant creates the multitenant organization, they can invite member tenants. A global administrator in each member tenant can then join the multitenant organization.

ⓘ Important

Microsoft recommends that you use roles with the fewest permissions. Using lower permissioned accounts helps improve security for your organization. Global Administrator is a highly privileged role that should be limited to emergency scenarios when you can't use an existing role.

While you configure Microsoft 365 multitenant organizations in the Microsoft 365 admin center, much of the supporting infrastructure is in Microsoft Entra ID. For details about how multitenant organizations work in Microsoft Entra ID, see [What is a multitenant organization in Microsoft Entra ID?](#) and [Topologies for cross-tenant synchronization](#).

User synchronization between tenants

Multitenant organizations synchronize users between tenants using Microsoft Entra B2B collaboration users. Users from your tenant are provisioned in the other tenants in the multitenant organization as B2B collaboration users, but with a user type of member

rather than guest. (See [What are the default user permissions in Microsoft Entra ID?](#) for the differences between these roles.) The member user type is required by Teams in multitenant organizations.

We recommend starting with a small set of users before rolling out to the entire organization. When you do the complete rollout, we highly recommend synchronizing all users across all tenants in your multitenant organization for the best user experience. However you can synchronize a subset of users if you need to, including different users to different tenants.

When you configure user synchronization in the Microsoft 365 admin center, the same users are synchronized to all tenants in the multitenant organization. Synchronizing different users to different tenants must be configured in Microsoft Entra ID.

Once user synchronization has been configured, you can adjust the synchronization settings, including user scope and attribute mapping, in Microsoft Entra ID. (While you can create multiple cross-tenant synchronization configurations for a single external tenant, we recommend that you only use one for ease of administration.) For more information, see [Configure cross-tenant synchronization](#).

Existing cross-tenant synchronization configurations

If you have existing cross-tenant synchronization configurations in Microsoft Entra ID, they continue to operate after you set up a multitenant organization in Microsoft 365. You can continue to use these configurations to synchronize users for your Microsoft 365 multitenant organization. (Note that the Microsoft 365 admin center won't recognize these configurations and the outbound sync status will show as not configured.)

If you already have B2B member users synchronized with tenants that are part of the MTO, those users will immediately become MTO members upon MTO formation.

You can synchronize users between tenants using the Microsoft 365 admin center. This will create new cross-tenant synchronization configurations in Microsoft Entra ID. Both the new and previously existing configurations will run and synchronize the users that you've specified.

We recommend that you only have a single configuration to synchronize users to a given tenant. If you want to synchronize the same users to every tenant, [configure synchronization in the Microsoft 365 admin center](#). If you want to synchronize different users to different tenants, [configure synchronization in Microsoft Entra ID](#).

Cross-tenant access settings in Microsoft Entra ID

When you create a new multitenant organization or join an existing one, the other organizations in the multitenant organization are added to the [Microsoft Entra cross-tenant access settings](#) in your tenant.

If you already have an organizational relationship configured in Microsoft Entra ID with a tenant that you're adding to a multitenant organization, the existing configuration is updated as follows:

- The inbound cross-tenant sync settings are updated to allow users to sync into your tenant.
- The outbound trust settings are updated so users from this tenant don't have to accept the consent prompt the first time they access the other tenant using cross-tenant synchronization, B2B collaboration, or B2B direct connect (shared channels).

We recommend that you check the B2B collaboration settings for pre-existing organizational relationships to ensure the appropriate users and apps are allowed.

The new Microsoft Teams desktop client

For the best experience in multitenant organizations, users need [the new Microsoft Teams desktop client](#). With the new Teams desktop client, users can:

- Receive real-time notifications from all the tenants in your multitenant organization
- Participate in chats, meetings, and calls across all of the tenants without dropping from a call or meeting to switch tenants.
- Set their status for each account and organization individually.
- User profile card shows organization name and email address

To control which users can use the new Teams desktop client, use the Teams update policies. For more information, see [Deploy the new Teams using policies](#)

Trusted organizations in external access

External access is required for chats and calls between tenants. External access for Teams and Skype for Business users in external organizations must be configured for each tenant in your multitenant organization and must allow the domains of all the tenants in your multitenant organization. Additionally, all the users that you synchronize between

tenants must be enabled for external access with Teams and Skype for Business users in external organizations. For details, see [Manage external meetings and chat with people and organizations using Microsoft identities](#).

Shared channels in multitenant organizations

Using [shared channels in Teams](#) with other tenants in a multitenant organization works the same as using shared channels with any other external organization. While the organizational relationship in Microsoft Entra ID is configured as part of multitenant organization configuration, you must still enable shared channels in Teams and configure the B2B direct connect settings in Microsoft Entra ID. For details, see [Collaborate with external participants in a shared channel](#).

License requirements

Use of the multitenant organization feature requires Microsoft Entra ID P1 licenses or above in all multitenant organization tenants. For additional details, see [Entra multitenant organization licensing requirements](#). If you plan on utilizing [Entra cross-tenant sync](#) via the Microsoft 365 admin center or Microsoft Entra ID, also see [Entra cross-tenant sync licensing requirements](#).

Limitations for multitenant organizations in Microsoft 365

The following are limitations of the multitenant organizations in Microsoft 365:

- A maximum of 100 tenants in the multitenant organization is supported.
- Teams on the web, Microsoft Teams Rooms (MTR), and VDI/AVD aren't supported.
- The ability to grant or revoke permission to receive notifications from other tenants and to switch between tenants isn't supported on mobile.
- *People in your organization* links may not work for users from another tenant if their account had originally been a guest and they had previously accessed SharePoint resources.
- It might take up to seven days for a user to appear in search once they've been synchronized. Contact Microsoft support if users aren't searchable after seven days.
- Support for a guest UserType of member in Power BI is currently in preview. For more information, see [Distribute Power BI content to external guest users with Microsoft Entra B2B](#).

If you want to add more than 100 tenants, contact Microsoft support.

For additional limitations, see [Limitations in multitenant organizations](#).

Set up or join a multitenant organization

To set up a new multitenant organization where your tenant is the owner, see [Set up a multitenant organization in Microsoft 365](#).

To join an existing multitenant organization as a member tenant, see [Join or leave a multitenant organization in Microsoft 365](#).

Related topics

[Configure cross-tenant synchronization using PowerShell or Microsoft Graph API](#)

[Synchronize users in multitenant organizations in Microsoft 365](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

Set up a multitenant org in Microsoft 365

Article • 06/24/2024

You can set up a multitenant organization or add tenants to an existing one in the Microsoft 365 admin center.

When each external tenant accepts the invitation to join the multitenant organization, the following settings are configured in Microsoft Entra ID:

- A cross-tenant synchronization configuration is added with the name *MTO_Sync_<TenantID>*, but no sync jobs are created yet. (If you already have a cross-tenant synchronization configuration, it remains unchanged.)
- An organization relationship is added to the [cross-tenant access settings](#) based on the [multitenant organization templates](#) for cross-tenant access and identity synchronization. (If an organizational relationship already exists, the existing one is used.)
- The multitenant organization template for identity synchronization is set to allow users to sync into this tenant.
- The multitenant org template for cross-tenant access will be set to automatically redeem user invitations, inbound as well as outbound.

Set up a new multitenant organization

ⓘ Important

Microsoft recommends that you use roles with the fewest permissions. Using lower permissioned accounts helps improve security for your organization. Global Administrator is a highly privileged role that should be limited to emergency scenarios when you can't use an existing role.

To set up a new multitenant org in Microsoft 365:

1. Sign in to the [Microsoft 365 admin center](#) as a global administrator.
2. Expand **Settings** and select **Org settings**.
3. On the **Organization profile** tab, select **Multitenant collaboration**.
4. Select **Get started**.
5. Select **Create a new multitenant organization**, and then select **Next**.
6. Type a name and description for the multitenant org.

7. Enter the tenant IDs of any tenants that you want to invite to this org.
8. Select **Next**.
9. Select the **Allow users to sync into this tenant from the other tenants in this multitenant organization** and **Suppress consent prompts for users from the other tenant when they access apps and resources in my tenant** check boxes.
10. Select **Create multitenant organization**.
11. Copy the instructions for joining the multitenant org and email them to a global administrator in each of the orgs you invited.
12. Select **Done**.

The next step after each external tenant accepts the invitation to join the multitenant organization is to synchronize your users with the other tenants. For details, see [Synchronize users in multitenant orgs in Microsoft 365](#).

Add a tenant to your multitenant organization

Important

Microsoft recommends that you use roles with the fewest permissions. Using lower permissioned accounts helps improve security for your organization. Global Administrator is a highly privileged role that should be limited to emergency scenarios when you can't use an existing role.

To add a tenant to your multitenant organization:

1. Sign in to the [Microsoft 365 admin center](#) as a global administrator.
2. Expand **Settings** and select **Org settings**.
3. On the **Organization profile** tab, select **Multitenant collaboration**.
4. Select **Add new tenants**.
5. Enter the tenant IDs of the tenants you want to add, and then select **Add tenant**.
6. Copy the instructions for joining the multitenant org and email them to a global administrator in each of the orgs you invited.
7. Select **Done**.

The next step after each external tenant accepts the invitation to join the multitenant organization is to synchronize your users with the other tenants. For details, see [Synchronize users in multitenant orgs in Microsoft 365](#).

Related topics

[Set up a multitenant organization using Microsoft Graph API](#)

[Plan for multitenant organizations in Microsoft 365](#)

[Join or leave a multitenant organization in Microsoft 365](#)

[Synchronize users in multitenant organizations in Microsoft 365](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Join or leave a multitenant organization in Microsoft 365

Article • 06/24/2024

To join a multitenant organization, a global administrator in the owner organization must first add your organization to the multitenant organization. Once they've done that, you can join the multitenant organization. You'll need the tenant ID of the owner organization in order to join.

Once you've joined, you can leave a multitenant organization at any time.

Related settings in Microsoft Entra ID

When you join an existing multitenant organization, the following settings are configured in Microsoft Entra ID:

- A cross-tenant synchronization configuration is added with the name *MTO_Sync_<TenantID>*, but no sync jobs are created yet. (If you already have a cross-tenant synchronization configuration, it remains unchanged.)
- An organization relationship is added to the [cross-tenant access settings](#) based on the [multitenant organization templates](#) for cross-tenant access and identity synchronization. (If an organizational relationship already exists, the existing one is used.)
- The multitenant organization template for identity synchronization is set to allow users to sync into this tenant.
- The multitenant org template for cross-tenant access will be set to automatically redeem user invitations, inbound as well as outbound.

When you leave a multitenant organization, the cross-tenant access settings and cross-tenant synchronization configurations in Microsoft Entra ID aren't affected.

Join an existing multitenant organization

Important

Microsoft recommends that you use roles with the fewest permissions. Using lower permissioned accounts helps improve security for your organization. Global

Administrator is a highly privileged role that should be limited to emergency scenarios when you can't use an existing role.

To join an existing multitenant organization in Microsoft 365:

1. Sign in to the [Microsoft 365 admin center](#) as a global administrator.
2. Expand **Settings** and select **Org settings**.
3. On the **Organization profile** tab, select **Multitenant collaboration**.
4. Select **Get started**.
5. Select **Join an existing multitenant organization**.
6. Enter the tenant ID of the owner organization.
7. Select the **Allow users to sync into this tenant from the other tenants in this multitenant organization** and **Suppress consent prompts for users from the other tenant when they access apps and resources in my tenant** check boxes.
8. Select **Next**.
9. Select **Done**.

It can take up to four hours for your tenant to be joined to the multitenant organization.

ⓘ Note

If you encounter an error when joining the multitenant organization, try again after two hours. If the error reoccurs, contact Microsoft support.

The next step after you join the multitenant organization is to synchronize your users with the other tenants. For details, see [Synchronize users in multitenant orgs in Microsoft 365](#).

Leave a multitenant organization

You can leave a multitenant organization as long as your tenant isn't the last owner tenant in the multitenant organization. You can also remove other member tenants.

ⓘ Important

Microsoft recommends that you use roles with the fewest permissions. Using lower permissioned accounts helps improve security for your organization. Global Administrator is a highly privileged role that should be limited to emergency scenarios when you can't use an existing role.

To remove a tenant from a multitenant organization in Microsoft 365:

1. Sign in to the [Microsoft 365 admin center](#) as a global administrator.
2. Expand **Settings** and select **Org settings**.
3. On the **Organization profile** tab, select **Multitenant collaboration**.
4. Select the check box next to the tenant you want to remove.
5. Select **Remove tenant**.
6. Read the details regarding tenant removal in the side panel, and then select **Remove tenant**.

Removing a tenant doesn't change any user synchronization configurations or cross-tenant access settings in Microsoft Entra ID. We recommend you review these settings and make any updates needed after the tenant is removed.

Remove synchronized users from other tenants

When you remove a tenant from a multitenant organization, you might want to stop synchronizing users between that tenant and the tenants that remain in the multitenant organization. This can be done by updating the cross-tenant synchronization configuration in Microsoft Entra ID and removing the security groups being synchronized, then restarting the synchronization with zero users.

Cross-tenant synchronization configurations for multitenant organizations that were created in the Microsoft 365 admin center are named *MTO_Sync_<TenantID>* in Microsoft Entra cross-tenant synchronization.

To remove the cross-synchronized users:

- For the tenant that is leaving the multitenant organization, update the synchronization configurations for each remaining tenant in the multitenant organization where you're synchronizing users.
- For each tenant that's remaining in the multitenant organization, update the synchronization configuration for the tenant that's leaving.

Important

Microsoft recommends that you use roles with the fewest permissions. Using lower permissioned accounts helps improve security for your organization. Global Administrator is a highly privileged role that should be limited to emergency scenarios when you can't use an existing role.

To remove your users from other tenants in a multitenant organization:

1. Sign in to the [Microsoft Entra admin center](#) as a Global administrator.
2. Expand **Identity**, and then expand **External Identities**.
3. Select **Cross-tenant synchronization**.
4. Select **Configurations**.
5. Select the link for the configuration you want to update.
6. Select **Users and groups**
7. Select the check boxes for the security groups that you want to remove, and then select **Remove**.
8. Select **Overview**.
9. Select **Restart provisioning**.

Once the users have been removed from the other tenants' directories, you can stop provisioning for the synchronization configurations or delete them.

Stop user sync and automatic invitation redemption

Once you remove a tenant from a multitenant organization, you might want to stop user sync and automatic invitation redemption with the tenants that remain in the multitenant organization.

To prevent user sync and automatic invitation redemption:

- For the tenant that is leaving the multitenant organization, update the cross-tenant access settings for each tenant that's remaining in the multitenant organization.
- For each tenant that's remaining in the multitenant organization, update the cross-tenant access settings for the tenant that's leaving.

Important

Microsoft recommends that you use roles with the fewest permissions. Using lower permissioned accounts helps improve security for your organization. Global Administrator is a highly privileged role that should be limited to emergency scenarios when you can't use an existing role.

To prevent user sync and automatic invitation redemption:

1. Sign in to the [Microsoft Entra admin center](#) as a Global administrator.
2. Expand **Identity**, and then expand **External Identities**.
3. Select **Cross-tenant access settings**.

4. On the **Organizational settings** tab, select the link for the **Inbound access** settings for the tenant you want to update.
 - a. On the **Trust settings** tab, clear the **Automatically redeem invitations with the tenant <organization>** check box.
 - b. On the **Cross-tenant sync** tab, clear the **Allow users sync into this tenant** check box.
 - c. Select **Save**.
5. Select the link for the **Outbound access** settings for the tenant you want to update.
 - a. On the **Trust settings** tab, clear the **Automatically redeem invitations with the tenant <organization>** check box.
 - b. Select **Save**.

For more information about cross-tenant access settings, see [Configure cross-tenant access settings for B2B collaboration](#).

Related topics

[Configure cross-tenant synchronization](#)

[Overview: Cross-tenant access with Microsoft Entra External ID](#)

[Plan for multitenant organizations in Microsoft 365](#)

[Set up a multitenant org in Microsoft 365](#)

[Synchronize users in multitenant organizations in Microsoft 365](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Synchronize users in multitenant organizations in Microsoft 365

Article • 06/24/2024

For users in your tenant to be able to collaborate with those in other tenants, you must synchronize your users to the other tenants.

There are two ways to set up user synchronization:

- Share your users with other tenants in a multitenant organization by using the Microsoft 365 admin center (covered in this article)
- [Configure user synchronization in Microsoft Entra ID](#)

Both methods use cross-tenant synchronization in Microsoft Entra ID.

If you want to synchronize the same users with all the other tenants in a multitenant organization, we recommend sharing users in the Microsoft 365 admin center. This creates the necessary configurations in Microsoft Entra ID for you.

If you want to synchronize different users to different tenants or use Entra groups to determine which users are in scope for provisioning, then you must configure cross-tenant synchronization directly in Microsoft Entra ID.

While you can create multiple cross-tenant synchronization configurations for a single external tenant, we recommend that you only use one for ease of administration.

If you already have B2B member users synchronized with tenants that are part of the MTO, those users will immediately become MTO members upon MTO formation.

ⓘ Note

It might take up to 24 hours for synced users to be available in Microsoft 365 services such as Teams and SharePoint.

For more information about cross-tenant synchronization, see [What is cross-tenant synchronization?](#)

If you have issues with user synchronization check the [provisioning logs in Microsoft Entra ID](#).

User property synchronization

When you set up user synchronization with another tenant in a multitenant organization, the following user properties are synchronized:

[+] [Expand table](#)

Property	Property
accountEnabled	physicalDeliveryOfficeName
alternativeSecurityIds	postalCode
city	preferredLanguage
country	showInAddressList
department	state
displayName	streetAddress
employeeId	surname
givenName	telephoneNumber
isSoftDeleted	userPrincipalName
jobTitle	UserType (member)
mailNickname	manager

You can change the properties that are synchronized after the synchronization has been configured. For more information, see [Configure cross-tenant synchronization](#).

Profile card experience

The [profile card](#) is a feature that allows users to view information about another user, such as email, phone number, and office location. It's available in most Microsoft 365 apps like Teams, Outlook, SharePoint and Viva Engage. Users in multitenant organizations can see information about users in other tenants that are part of the multitenant organization. What users can see depends on what data is being synchronized between the tenants. (Note that some properties [require additional configuration](#) to be displayed.)

The [new Teams desktop client](#) fetches some data directly from the other tenants in the multitenant organization to create a richer experience. In a multitenant organization, when a user looks at the profile card for a user in another tenant in Teams, the name, contact information, and job information is available in 1:1 chats and shared channels without the need for property synchronization to be configured. (These properties are

retrieved by Microsoft Entra cross-tenant access and Teams external access.) To see these properties elsewhere in Teams, such as channels, group chats, and chats with guest accounts, you need to include them as part of user synchronization.

In a multitenant organization, the profile picture is always available and is retrieved from the user's home tenant.

For the most consistent profile card experience, keep in mind the following:

- Don't change property values as they're synced, or users will see different values in different tenants.
- [LinkedIn account connections](#) configurations may vary across tenants.

Users synchronized to your tenant from other tenants

Users synchronized to your tenant from other tenants in your multitenant organization are synchronized as [Microsoft Entra members rather than guests](#).

As members, people from other tenants have a more seamless collaboration experience. This includes access to files using [people in your organization sharable links](#). (Consider using [sensitivity labels](#) if you need to limit who can access a file with a [people in your organization](#) link.)

If some people from the other tenant already have guest accounts in your directory, the synchronization process doesn't change their user type to member by default. You can change these users' user type to member by [updating the user properties in Microsoft Entra ID](#) or updating your cross-tenant synchronization configuration mappings in [Microsoft Entra ID](#) to support converting from guest to member at scale.

Set up initial user synchronization for a multitenant organization

Important

Microsoft recommends that you use roles with the fewest permissions. Using lower permissioned accounts helps improve security for your organization. Global Administrator is a highly privileged role that should be limited to emergency scenarios when you can't use an existing role.

To synchronize identities to other tenants in a multitenant organization:

1. Sign in to the [Microsoft 365 admin center](#) as a global administrator.
2. Expand **Settings** and select **Org settings**.
3. On the **Organization profile** tab, select **Multitenant collaboration**.
4. Select **Share users**.
5. Select **Select users to share**.
6. Select **Save**.
7. Select **Yes** to confirm.

This creates a cross-tenant synchronization configuration in Microsoft Entra ID for each tenant in your multitenant organization. The synchronization configurations are named *MTO_Sync_<TenantID>*.

Set up user synchronization with newly added tenants

If you add additional tenants to your multitenant organization, you need to set up user synchronization with those tenants.

Important

Microsoft recommends that you use roles with the fewest permissions. Using lower permissioned accounts helps improve security for your organization. Global Administrator is a highly privileged role that should be limited to emergency scenarios when you can't use an existing role.

To set up user synchronization with newly added tenants:

1. Sign in to the [Microsoft 365 admin center](#) as a global administrator.
2. Expand **Settings** and select **Org settings**.
3. On the **Organization profile** tab, select **Multitenant collaboration**.
4. Select **Share users**.
5. Select **Share current user scope**.
6. Select **Yes** to confirm.

Change which users are synchronized with other tenants

You can change which users are synchronized to other tenants in your multitenant organization.

ⓘ Important

Microsoft recommends that you use roles with the fewest permissions. Using lower permissioned accounts helps improve security for your organization. Global Administrator is a highly privileged role that should be limited to emergency scenarios when you can't use an existing role.

To change which users are synchronized to other tenants:

1. Sign in to the [Microsoft 365 admin center](#) as a global administrator.
2. Expand **Settings** and select **Org settings**.
3. On the **Organization profile** tab, select **Multitenant collaboration**.
4. Select **Share users**.
5. Select **Edit shared users**.
6. Update the users that you want to sync to other tenants and then select **Save**.
7. Select **Yes** to confirm.

This procedure updates the *MTO_Sync_<TenantID>* synchronization configurations in Microsoft Entra ID for each tenant in your multitenant organization.

Set up calendar sharing for tenants in your MTO

Calendar sharing allows users in each multitenant organization (MTO) tenant to view free/busy (time only) calendar availability information.

ⓘ Note

Calendar sharing via Multitenant collaboration portal is currently not available in Microsoft 365 GCC, GCC High, DoD, or Microsoft 365 China (operated by 21Vianet).

ⓘ Important

Microsoft recommends that you use roles with the fewest permissions. Using lower permissioned accounts helps improve security for your organization. Global

Administrator is a highly privileged role that should be limited to emergency scenarios when you can't use an existing role.

To manage free/busy calendar sharing for tenants in your MTO:

1. Sign in to the [Microsoft 365 admin center](#) as a global administrator.
2. Expand **Settings** and select **Org settings**.
3. On the **Organization profile** tab, select **Multitenant collaboration**.
4. Select **Manage settings**.
5. Select **Edit calendar settings** under **Calendar**.
6. Select tenants to enable free/busy calendar sharing.
7. Select **Save changes**.

The calendar sharing feature for MTO utilizes [Organization relationships in Exchange Online](#). The organization relationship will share all users calendar availability and must also be set up by the other tenants in your MTO for free/busy information to be shared.

Set up MTO user labels in Teams for tenants in your MTO

MTO group admins can now configure an optional label for each tenant that will be displayed alongside MTO synced user's display name in Teams. This allows MTO synced users to be distinguishable within the MTO in Teams interactions.

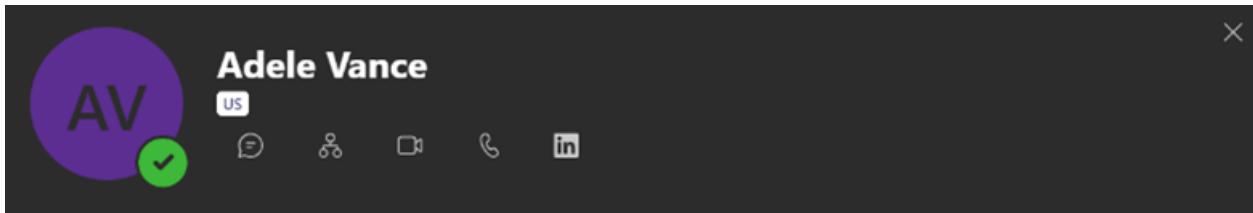


Fig 1: Teams people card shows MTO user label "US"

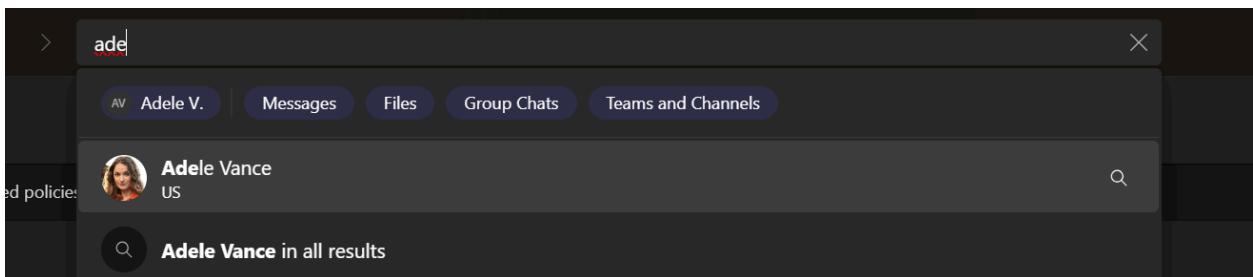


Fig 2: Teams search experience shows MTO user label "US"

Only MTO owners can manage the MTO user labels. Label changes may take some time to process and will only apply to active tenants.

ⓘ Important

Microsoft recommends that you use roles with the fewest permissions. Using lower permissioned accounts helps improve security for your organization. Global Administrator is a highly privileged role that should be limited to emergency scenarios when you can't use an existing role.

To manage MTO user labels for tenants in your MTO:

1. Sign in to the [Microsoft 365 admin center](#) as a global administrator.
2. Expand **Settings** and select **Org settings**.
3. On the **Organization profile** tab, select **Multitenant collaboration**.
4. Select **Manage settings**.
5. Select **Edit** under **Tenant label**.
6. Select either:
 - a. No label.
 - b. Use the multitenant organization name for all tenants.
 - c. Custom (assign a label for each tenant, which cannot be blank).
7. Select **Save changes**.

Related topics

[Troubleshooting tips for multitenant organizations](#)

[Known issues for provisioning in Microsoft Entra ID](#)

[Plan for multitenant organizations in Microsoft 365](#)

[Set up a multitenant org in Microsoft 365](#)

[Join or leave a multitenant organization in Microsoft 365](#)

[Scoping users or groups to be provisioned with scoping filters](#)

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Microsoft 365 multitenant Organization People Search

Article • 04/17/2024

The multitenant Organization (MTO) People Search is a collaboration feature that enables search and discovery of people across multiple tenants. A tenant admin can enable cross-tenant synchronization that allows users to be synced to another tenant and be discoverable in its global address list. Once enabled, users are able to search and discover synced user profiles from the other tenant and view their corresponding people cards.

Cross Tenant Synchronization

Key:
Sync'd user
Contoso user

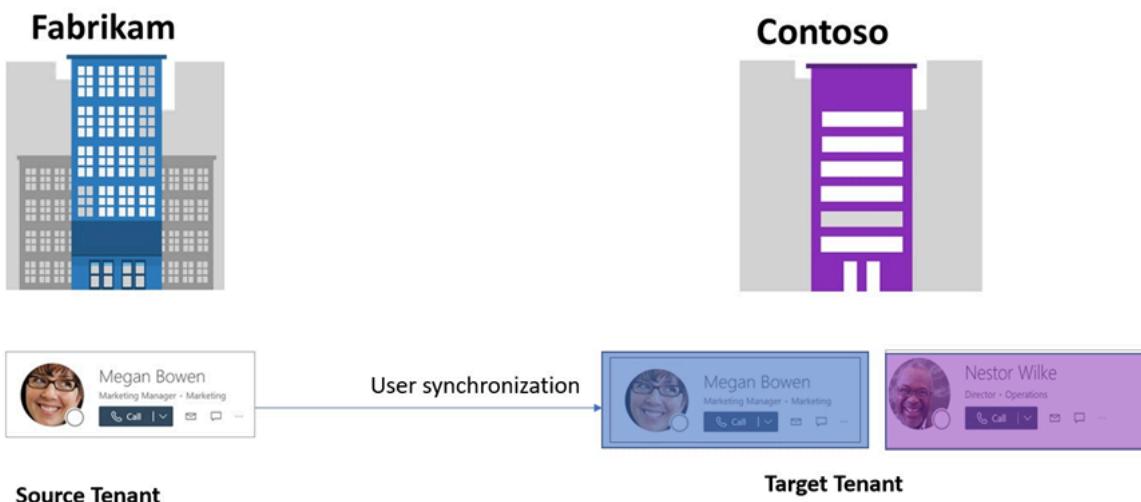


Fig 1: Microsoft Entra cross tenant synchronization illustration

Example scenario

Megan's user account has been synced from the *Fabrikam* tenant to the target tenant, *Contoso*. Nestor from *Contoso* would like to search and view Megan's people card in Teams. After Megan's account has been synced, Nestor can search and discover Megan's people card in any of the Microsoft 365 apps.

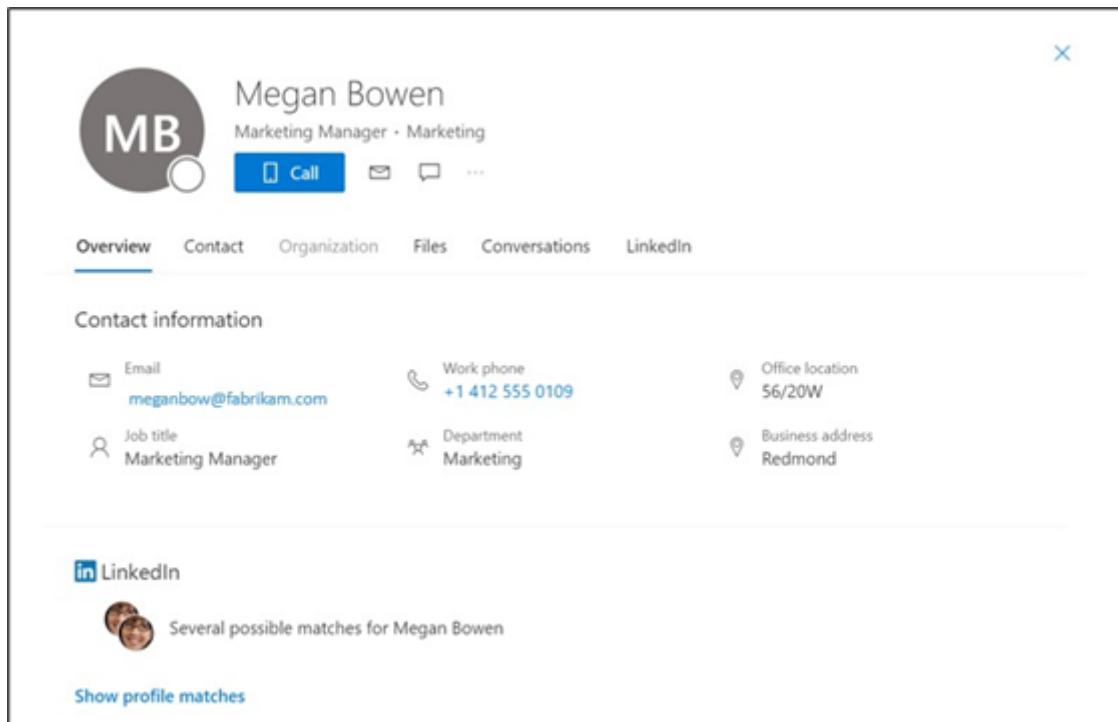


Fig 2: User can view a limited people card

Known limitations

- The Microsoft Teams audio and video call buttons will direct the call to the Megan's Contoso tenant Teams instance and not the Teams instance target tenant (Fabrikam).
- The current experience provides limited information on the people card (basic contact information, job title and office location).
- There's no external tag to differentiate synced users and internal users. For example, if there was a `megan@fabrikam` and `megan@Contoso` there's no (External) tag to show that `megan@fabrikam` is a different user.
- Converting an external guest into an external member or converting an external member into an external guest isn't currently supported by Teams.

Prerequisites

To test the MTO People Search feature, it's assumed that you already have the following settings:

- Two Microsoft Entra / Microsoft 365 tenants
- Both tenants have the **Microsoft Entra Cross-tenant Synchronization** feature enabled
- Provisioned users from home to target tenants

Use Cases

Multitenant organization people search is supported across a range of scenarios and Microsoft 365 applications. Some of the scenarios you can test and validate are described below:

1. Microsoft Outlook (OWA, desktop and mobile app)

- Nestor (nestor@contoso.com) searches for "Megan" on the centralized search bar in OWA and gets the results and can view Megan's people card with limited profile information.
- Nestor types in "Megan" in the *To* line of the email and can send an email to Megan after getting the results for megan@fabrikam.com.
- Nestor @mentions "Megan" in the body of the email and can get the result for megan@fabrikam.com.
- Nestor types in "Megan" in the *cc* line of the email and can get the result for megan@fabrikam.com.
- Nestor can hover and/or click on Megan's profile picture/initials to view Megan's limited people card.

2. Microsoft OneDrive/SharePoint

- Nestor (nestor@contoso.com) searches for "Megan" in the centralized search bar on SharePoint and can get the result for megan@fabrikam.com.
- Nestor can hover and/or click on Megan's profile picture/initials to view Megan's limited people card.
- Nestor can share and collaborate on Office documents with Megan.

3. Bing for Business

- Nestor (nestor@contoso.com) searches for "Megan" on the search bar and can view Megan's limited people card (megan@fabrikam.com).

Key terminology

- *Home tenant*: The tenant you want to search from. The direction of the search is *outbound*.
- *Resource tenant*: The tenant you want to search in. The direction of the search is *inbound*.

A tenant can be both home and resource tenant simultaneously.

- *Cross-Tenant synchronization* is a feature that enables multitenant organizations to grant users access to applications in other tenants within the organization. It achieves this by synchronizing internal member users from a home tenant into a resource tenant as external B2B users.
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Cross-tenant OneDrive migration

Article • 05/31/2024

ⓘ Note

Information in this article refers to **Cross-tenant OneDrive migration**. For mailbox migration, see [Cross-tenant mailbox migration](#).

Overview

During mergers or divestitures, you commonly need the ability to move users OneDrive accounts into a new Microsoft 365 tenant. With Cross-tenant OneDrive migration, tenant administrators can use familiar tools like *SharePoint Online PowerShell* to transition users into their new organization.

SharePoint administrators of two separate tenants can use the *Set-SPOCrossTenantRelationship* cmdlet to establish an organization relationship, and the *Start-SPOCrossTenantUserContentMove* command to begin cross-tenant OneDrive moves.

Up to 4,000 OneDrive accounts can be scheduled for migration in advance at a given time. Once scheduled, migrations occur without the user's data ever leaving the Microsoft 365 cloud and with minimal disruption, requiring only a few minutes where a user's OneDrive will be read-only. When migrations are complete, a redirect is placed in the location of the user's original OneDrive, so any links to files and folders can continue working in the new location.

ⓘ Important

Cross-Tenant moves are a one and done migration activity. The content will be moved from the Source to Target, leaving behind a redirect link on Source. Incremental and delta migration passes cannot be performed.

ⓘ Note

This feature is not supported for users of the Government Cloud, including GCC, Consumer, GCC High, or DoD.

Licensing

ⓘ Important

As of Nov. 2022, Cross Tenant User Data Migration is available as an add-on to the following Microsoft 365 subscription plans for Enterprise Agreement customers, and is required for cross-tenant migrations. User licenses are per migration (one-time fee) and can be assigned either on the source or target user object. This license also covers Cross-tenant mailbox migration. Contact your Microsoft account team for details.

The Cross Tenant User Data Migration add-on is available as a separate purchase for Microsoft 365 Business Basic, Standard, and Premium; Microsoft 365 F1/F3/E3/E5; Office 365 F3/E1/E3/E5; Exchange Online; SharePoint Online; and OneDrive for Business.

⚠ Warning

You must have purchased, or verified that you can purchase, cross tenant user data migration licenses prior to the next steps. Migrations fail if this step has not been completed. Microsoft does not offer exceptions for this licensing requirement.

Prerequisites and settings

- **Microsoft SharePoint Online Powershell.** Confirm you have the most recent version installed. [Download SharePoint Online Management Shell from the official Microsoft Download Center ↗](#).
- **Confirm that the source OneDrive tenant does not have Service encryption with Microsoft Purview Customer Key enabled.** If enabled on the source tenant, the migration will fail. [Learn more on Service encryption with Microsoft Purview Customer Key.](#)
- Source OneDrive accounts must be set to Read/Write. If set to Read only, they'll fail.

Pre-create target accounts

- Ensure all users and groups identified for migration have been pre-created on the target tenant.
- Assign the appropriate licenses to each user on the target tenant.

Important

OneDrive sites should **NOT** be created before **OR** during a migration.

OneDrive site creation should be restricted in the target tenant to prevent users from creating OneDrive sites. If a OneDrive site already exists for the user on the target tenant, the migration will fail. You can't overwrite an existing site.

If users continue to access resources in the source tenant, you should restrict OneDrive creation in the source tenant to prevent creating new OneDrive sites.

Note

To learn more about restricting OneDrive site creation, see [Disable OneDrive creation for some users](#)

Path size limits

Microsoft limits the number of characters in a path to not exceed 400 characters. This is the full path limit, not just the file name. In planning your migrations, review the length of OneDrive URL names in your target tenant. Failure often occurs when files or folder paths from the source, combined with the OneDrive URL on the target exceed the 400-character path limit.

A migration will detect if you have exceeded the character limit. Work with the site owner to update the file/folder directory structure to reduce file path lengths.

Any legal URL will be accepted when creating your Identity Map from Source to Target for your migrations. At this current time usernames/URLs that contain an apostrophe character (') in a username/URL will fail with an "invalid character" error when attempting the migration.

Tip

We recommend keeping your target OneDrive URL names short to avoid exceeding the character limit.

OneDrive account size limits

Each OneDrive account can have a maximum of 5 TB of content or 1 million items.

ⓘ Important

The 1 million item limit can be any "item", including files (including versions), folders, and list line entries if it is a list or library.

If you attempt to migrate any OneDrive site that exceeds the 5 TB quota, the transfer will fail.

Permissions

All users and groups included in the identity mapping file that you uploaded to the target tenant will maintain permissions in the target tenant related to the migrated OneDrive site.

Legal holds

OneDrive accounts with a Hold policy applied will be blocked from migration. To migrate these OneDrive accounts, remove the hold policy, migrate, then reapply the hold as needed on the target tenant.

Shared files

After a OneDrive account is migrated, anyone clicking on a shared link to the old location will be redirected to the new one, provided they still have access to the destination.

Those redirects remain until the source tenant is deprovisioned. The admin can also selectively remove redirects site-by-site.

How does it work?

- Step 1: [Connect to the source and the target tenants](#).
- Step 2: [Establish trust between the source and the target tenant](#)
- Step 3: [Verify trust has been established](#)
- Step 4: [Pre-create users and groups](#)

- Step 5: Prepare identity mapping
- Step 6: Start a Cross-tenant OneDrive migration
- Step 7: Post migration steps

Step 1: Connect to source and target tenants

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Step 1: Connect to the source and target tenants

Article • 08/08/2024

This article details Step 1 in a solution designed to complete a Cross-tenant OneDrive migration. To learn more, see [Cross-tenant OneDrive migration overview](#).

- Step 1: [Connect to the source and the target tenants](#)
- Step 2: [Establish trust between the source and the target tenant](#)
- Step 3: [Verify trust is established](#)
- Step 4: [Pre-create users and groups](#)
- Step 5: [Prepare identity mapping](#)
- Step 6: [Start a Cross-tenant OneDrive migration](#)
- Step 7: [Post migration steps](#)

Before you begin

- **Microsoft SharePoint Online Powershell.** Confirm you have the most recent version installed. If not, [Download SharePoint Online Management Shell from Official Microsoft Download Center](#).
- Be a SharePoint Online admin or Microsoft 365 Global admin on both the source and target tenants

Important

Microsoft recommends that you use roles with the fewest permissions. Using lower permissioned accounts helps improve security for your organization. Global Administrator is a highly privileged role that should be limited to emergency scenarios when you can't use an existing role.

Connect to both tenants

1. Sign in to the SharePoint Management Shell as a SharePoint Online admin or Microsoft 365 Global admin.
2. Run the following entering the **source** tenant URL:

```
PowerShell
```

```
Connect-SPOService -url https://<TenantName>-admin.sharepoint.com
```

3. When prompted, sign in to the **source** tenant using your Admin username and password.
4. Run the following entering the **target** tenant URL:

PowerShell

```
Connect-SPOService -url https://<TenantName>-admin.sharepoint.com
```

5. When prompted, sign in to the **target** tenant using your Admin username and password.

ⓘ Important

Microsoft 365 Multi-Geo customers: You must treat each geography as a separate tenant. Provide the correct geography-specific URLs throughout the migration process.

Step 2: Establish trust between the source and target tenants

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Step 2: Establishing trust between the source and target tenants

Article • 05/02/2024

This is Step 2 in a solution designed to complete a Cross-tenant OneDrive migration. To learn more, see [Cross-tenant OneDrive migration overview](#).

- Step 1: [Connect to the source and the target tenants](#)
- **Step 2: Establish trust between the source and the target tenant**
- Step 3: [Verify trust has been established](#)
- Step 4: [Precreate users and groups](#)
- Step 5: [Prepare identity mapping](#)
- Step 6: [Start a Cross-tenant OneDrive migration](#)
- Step 7: [Post migration steps](#)

After connecting to the source and target tenant, the next step in performing a cross-tenant OneDrive migration is establishing trust between the tenants.

To establish trust, each SharePoint tenant administrator must run specific commands on both source and target tenants. Once the trust has been requested, the administrator of the target tenant will receive an email informing them that another tenant is trying to establish a trust relationship.

ⓘ Note

The "trust" command is specific to SharePoint. It only grants permission for the SharePoint administrator on the source tenant to execute OneDrive Migration operations to the identified target tenant.

Granting trust *doesn't* give the administrator any visibility, permission, or ability to collaborate between the source tenant and the target tenant.

ⓘ Important

If you are Microsoft 365 Multi-Geo customer, you must establish trust between each geography involved in your migration project.

Before you begin

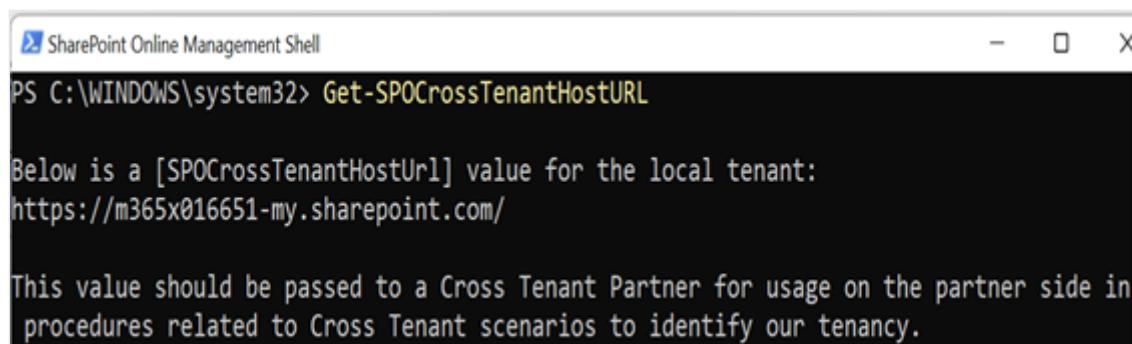
Before running the trust commands, obtain the cross-tenant host URLs for both the source and target tenants. You'll need these URLs when establishing the trust relationship between source-to-target and target-to-source.

To obtain the cross-tenant host URLs:

On both the source and target tenants, run:

```
PowerShell
Get-SPOCrossTenantHostURL
```

Example: Run command on Source tenant:



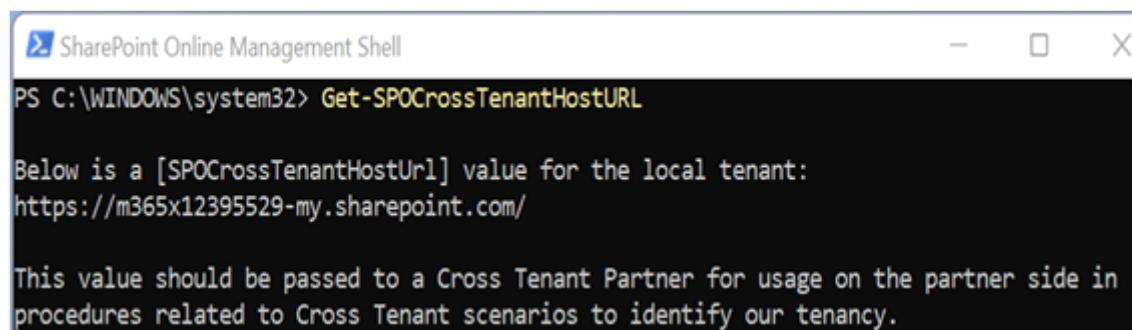
SharePoint Online Management Shell

```
PS C:\WINDOWS\system32> Get-SPOCrossTenantHostURL

Below is a [SPOCrossTenantHostUrl] value for the local tenant:
https://m365x016651-my.sharepoint.com/

This value should be passed to a Cross Tenant Partner for usage on the partner side in
procedures related to Cross Tenant scenarios to identify our tenancy.
```

Example: Run command on target tenant:



SharePoint Online Management Shell

```
PS C:\WINDOWS\system32> Get-SPOCrossTenantHostURL

Below is a [SPOCrossTenantHostUrl] value for the local tenant:
https://m365x12395529-my.sharepoint.com/

This value should be passed to a Cross Tenant Partner for usage on the partner side in
procedures related to Cross Tenant scenarios to identify our tenancy.
```

Run the trust commands

These commands send a request to the tenant with whom you want to establish trust.

1. On the source tenant, run this command to send a trust request to the target tenant:

```
PowerShell
Set-SPOCrossTenantRelationship -Scenario MnA -PartnerRole Target -
PartnerCrossTenantHostUrl <TARGETCrossTenantHostUrl>
```

2. On the target tenant, run this command to send a trust request to the source tenant:

```
PowerShell
```

```
Set-SPOCrossTenantRelationship -Scenario MnA -PartnerRole Source -  
PartnerCrossTenantHostUrl <SOURCECrossTenantHostUrl>
```

Parameter definitions

[+] Expand table

Parameter	Definition
PartnerRole	Roles of the partner tenant you're establishing trust with. Use <i>source</i> if partner tenant is the source of the OneDrive migrations, and <i>target</i> if the partner tenant is the Destination.
PartnerCrossTenantHostURL	The cross-tenant host URL of the partner tenant. The partner tenant can determine this for you by running: <i>Get-SPOCrossTenantHostURL</i> on each of the tenants.

Sample trust email

The following is an example of the email that is sent to global admins:

 SharePoint Online <no-reply@sharepointonline.com>
To: ○ ; @msftfotesttenantAdvEncryp.onmicrosoft.com;
○ ; @msftfotesttenantAdvEncryp.onmicrosoft.com;
○ ; @msftfotesttenantAdvEncryp.onmicrosoft.com;
○ ; @microsoft365demos.com; ○ ; @microsoft365demos.com;
○ ; migrationAdmin@msftfotesttenantadvencryp.onmicrosoft.com; ○ ; AdvEncryptAdminProd

SPO Tenant [https://a830edad9050849mnaus093022-my.sharepoint.com/] [setuporupdate] Organization Relation [Scenario=MnA, Role=Source] with us

Subject: SPO Tenant [https://a830edad9050849mnaus093022-my.sharepoint.com/] [setuporupdate] Organization Relation [Scenario=MnA, Role=Source] with us

Message: SPO Tenant [https://a830edad9050849mnaus093022-my.sharepoint.com/] [setuporupdate] Organization Relation [Scenario=MnA, Role=Source] with us

Step 3: Verify that trust has been established

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Step 3: Verifying trust

Article • 01/26/2024

This step is Step 3 in a solution designed to complete a Cross-tenant OneDrive migration. To learn more, see [Cross-tenant OneDrive migration overview](#).

- Step 1: [Connect to the source and the target tenants](#)
- Step 2: [Establish trust between the source and the target tenant](#)
- **Step 3: Verify trust has been established**
- Step 4: [Pre-create users and groups](#)
- Step 5: [Prepare identity mapping](#)
- Step 6: [Start a Cross-tenant OneDrive migration](#)
- Step 7: [Post migration steps](#)

Before proceeding with your migration, you need to verify the trust is complete. A status of *GoodToProceed* confirms that the trust is verified.

To verify trust has been established

1. On the **source tenant** run:

PowerShell

```
Verify-SPOCrossTenantRelationship -Scenario MnA -PartnerRole Target -  
PartnerCrossTenantHostUrl <TARGETCrossTenantHostUrl>
```

2. On the **target tenant** run:

PowerShell

```
Verify-SPOCrossTenantRelationship -Scenario MnA -PartnerRole Source -  
PartnerCrossTenantHostUrl <SOURCECrossTenantHostUrl>
```

Troubleshooting trust issues

When verifying trust, possible values

[+] Expand table

Value	Description
NotEstablished	Trust wasn't requested locally.
NotEstablishedByPartner	Partner hasn't requested the Trust.
DormantByPartner	Partner's requested trust is within the seven days waiting period after creation.
CouldNotContactPartner	Couldn't contact the partner to determine status.
GoodToProceed	Verified to proceed.

Step 4: Pre-create users and groups

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Step 4: Precreating users and groups

Article • 10/13/2023

This is Step 4 in a solution designed to complete a Cross-tenant OneDrive migration. To learn more, see [Cross-tenant OneDrive migration overview](#).

- Step 1: [Connect to the source and the target tenants](#)
- Step 2: [Establish trust between the source and the target tenant](#)
- Step 3: [Verify trust has been established](#)
- **Step 4: Pre-create users and groups**
- Step 5: [Prepare identity mapping](#)
- Step 6: [Start a Cross-tenant OneDrive migration](#)
- Step 7: [Post migration steps](#)

Identify users and groups to be migrated

To ensure that OneDrive permissions are retained as part of the migration, a mapping file needs to be created to align users from the source tenant to the target tenant.

1. Identify the full list of OneDrive sites that will be migrated from the source to the target tenant.
2. Prepare a complete list of users and groups that will be migrated to the target tenant.

Precreate users and groups on the target tenant

1. Precreate users and groups as needed in the target tenant's directory.
2. All users whose OneDrive accounts are migrating to the target tenant must have new user identities created for them in the target tenant.
3. All users whose OneDrive accounts are migrating to the target tenant must be assigned the appropriate OneDrive license.
4. Any users who remain in the source tenant but need access to resources migrating to the target tenant should have new guest identities created for them in the target tenant.
5. Precreated users must be added as members of any appropriate security groups or unified groups before the OneDrive migration begins.
6. If the user or group name already exists in the target tenant, create a user or group with a different name and make a note of it for the next step.

7. We recommend that OneDrive site creations are restricted in the target tenant to prevent users from creating OneDrive sites.

 **Note**

To learn more on restricting OneDrive site creation, see [Disable OneDrive creation for some users](#)

Step 5: Prepare the identity mapping file

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Step 5: Identity mapping

Article • 10/13/2023

This is Step 5 in a solution designed to complete a Cross-tenant OneDrive migration. To learn more, see [Cross-tenant OneDrive migration overview](#).

- Step 1: [Connect to the source and the target tenants](#)
- Step 2: [Establish trust between the source and the target tenant](#)
- Step 3: [Verify trust has been established](#)
- Step 4: [Pre-create users and groups](#)
- Step 5: [Prepare identity mapping](#)
- Step 6: [Start a Cross-tenant OneDrive migration](#)
- Step 7: [Post migration steps](#)

Create the identity mapping file

In this step of the cross-tenant migration process, you're going to create a single CSV (comma separated values) file that contains the mapping of the users and groups on the source tenant to their corresponding users and groups on the target tenant.

We recommend that you take the time to verify your mappings, ensuring they're accurate before starting any migrations to the target tenant.

There's a one-to-one relationship in the identity mapping file. You can't map the same user to multiple users in the target tenant. For example, if you have instances where the admin is the owner of multiple OneDrive accounts, the ownership must be changed to match the corresponding user you wish to migrate from Source to Target. If you don't, those account files won't migrate.

Example: In this example, the admin owns multiple OneDrive accounts.

Expand table

Source Tenant Owner	Target Tenant User
admin@source.com	new.userA@target.com
admin@source.com	new.userB@target.com
admin@source.com	new.userC@target.com

Cross-tenant migration supports this scenario:

Example:

[+] [Expand table](#)

Source Tenant Owner	Target Tenant User
userA@source.com	new.userA@target.com
userB@source.com	new.userB@target.com
userC@source.com	new.userC@target.com

Create the CSV file

There are six columns needed in your CSV file. The first three are your source values, each providing detail about where your data is currently located. The remaining three columns are the corresponding info on the target tenant. All six columns must be accounted for in the file. Create your file in Excel and save it as a .csv file.

Users and groups are included in the same file. Depending on whether it's a user or group, what you enter in the column is different. In each of the columns enter values as shown in the examples. **Do NOT include column headings.**

[+] [Expand table](#)

Column	User	Group
1	User	Group
2	SourceTenantCompanyID	SourceTenantCompanyID
3	SourceUserUpn	SourceGroupObjectID
4	TargetUserUpn	TargetGroupObjectID
5	TargetUserEmail	GroupName
6	UserType	GroupType

ⓘ Important

Do NOT include column headings in your CSV file. In the examples below we include them for illustrative purposes only.

Users. Enter your values as shown in this example for Users:

User	SourceTenantCompanyID	SourceUserUpn	TargetUserUpn	TargetUserEmail	UserType
------	-----------------------	---------------	---------------	-----------------	----------

Example: Mapping a member account (Source) to member account (Target)					
User	SourceTenantCompanyID	SourceUserUpn	TargetUserUpn	TargetUserEmail	UserType
User	03cb84b4-2f99-4b43-93fb-d4479e9b57af	user@source.com	John@target.com	John@target.com	RegularUser

Groups. Enter your values as shown in this example for Groups:

Group	SourceTenantCompanyID	SourceGroupObjectID	TargetGroupObject ID	GroupName	GroupType

Example:

Group	SourceTenantCompanyID	SourceGroupObjectID	TargetGroupObject ID	GroupName	GroupType
Group	03cb84b4-2f99-4b43-93fb-d4479e9b57af	94d00e94-a007-4b14-bf16-159b26ec2853	34a09691-899c-4613-895c-0e653061630d	34a09691-899c-4613-895c-0e653061630d	RegularGroup

Guest users. You can map guest accounts in the source tenant to member accounts in the target tenant. You can also map a guest account in the source to a guest account in the target if the guest has been previously created. Enter your values as shown in this example for guests:

Example: Mapping a Guest Account (Source) to Member Account (Target)					
User	SourceTenantCompanyID	SourceUserUpn	TargetUserUpn	TargetUserEmail	UserType
User	03cb84b4-2f99-4b43-93fb-d4479e9b99zz	user1_outlook.com#EXT#@source.onmicrosoft.com	john@target.com	john@target.com	GuestUser

Example: Mapping a Guest Account (Source) to Guest Account (Target)					
User	SourceTenantCompanyID	SourceUserUpn	TargetUserUpn	TargetUserEmail	UserType
User	03cb84b4-2f99-4b43-93fb-d4479e9b99zz	user1_outlook.com#EXT#@source.onmicrosoft.com	user1_outlook.com	user1@target.com	GuestUser

Multiple users and groups in a CSV file:

Example:

Group 9f724407-653e-46b3-be44-c2129e5ff698	94d00e94-a007-4b14-bf16-159b26ec2853	34a09691-899c-4613-895c-0e653061630d	34a09691-899c-4613-895c-0e653061630d	RegularGroup
Group 9f724407-653e-46b3-be44-c2129e5ff698	225adfea-d7ed-4c63-9c87-e2e8dc919c	34a09691-899c-4613-895c-0e653061630d	34a09691-899c-4613-895c-0e653061630d	RegularGroup
User 9f724407-653e-46b3-be44-c2129e5ff698	AdeleV@M365x016651.OnMicrosoft.com	Test-Adele@M365x946316.OnMicrosoft.com	Test-Adele@M365x946316.OnMicrosoft.com	RegularUser
User 9f724407-653e-46b3-be44-c2129e5ff698	AllanD@M365x016651.OnMicrosoft.com	Test-AllanD@M365x946316.OnMicrosoft.com	Test-AllanD@M365x946316.OnMicrosoft.com	RegularUser
User 9f724407-653e-46b3-be44-c2129e5ff698	DiegoS@M365x016651.OnMicrosoft.com	Test-Diego@M365x946316.OnMicrosoft.com	Test-Diego@M365x946316.OnMicrosoft.com	RegularUser
User 9f724407-653e-46b3-be44-c2129e5ff698	JoniS@M365x016651.OnMicrosoft.com	Test-Joni@M365x946316.OnMicrosoft.com	Test-Joni@M365x946316.OnMicrosoft.com	RegularUser
User 9f724407-653e-46b3-be44-c2129e5ff698	MeganB@M365x016651.OnMicrosoft.com	Test-Megan@M365x946316.OnMicrosoft.com	Test-Megan@M365x946316.OnMicrosoft.com	RegularUser
User 9f724407-653e-46b3-be44-c2129e5ff698	NestorW@M365x016651.OnMicrosoft.com	Test-NestorW@M365x946316.OnMicrosoft.com	Test-NestorW@M365x946316.OnMicrosoft.com	RegularUser

Obtain the source tenant company ID

To obtain Source Tenant Company ID:

1. Sign in as Admin to your [Azure portal](#)
2. Select or Search for Microsoft Entra ID.
3. Scroll down on the left-hand panel and select Properties.
4. Locate the Tenant ID Field. The required Tenant ID will be in that box.

Tenant properties

Name *	Contoso
Country or region	United States
Location	United States datacenters
Notification language	English
Tenant ID	9724407-653e-46b3-be44-c2129e5ff600
Technical contact	transformprov@microsoft.com
Global privacy contact	
Privacy statement URL	

To obtain source group object ID:

1. Sign in to source tenant as Admin to [Azure Groups](#).
2. Search for your required group(s).
3. Select the required Group instance and then **Copy to clipboard**. Paste this value in the sourceGroupId column of your mapping CSV file.
4. If you have multiple Groups to map, then repeat these steps for each group.

All Company

This is the default group for everyone in the network

Membership type	Assigned
Source	Cloud
Type	Microsoft 365
Object Id	94d00e94-a007-4b14-bf16-159b26ec2853
Creation date	8/5/2021, 11:25:51 AM
Email	allcompany@M365x016651.onmicrosoft.com

To obtain target group object ID:

1. Sign in to Target tenant as Admin to [Azure Groups](#)
2. Search for your required group(s).
3. Select the required group instance and then **Copy to clipboard**. Paste this value in the targetGroupId column of your mapping CSV file.
4. If you have multiple groups to map, then repeat the above process to obtain those specific targetGroupId's.
5. For the *GroupName*, use the same ID as the *TargetGroupId* you obtained.

The screenshot shows the 'All Company' group details in the SharePoint Admin Center. The group has the following properties:

- Membership type: Assigned
- Source: Cloud
- Type: Microsoft 365
- Object Id: 34a09691-899c-4613-895c-0e653061630d
- Creation date: 8/9/2021, 2:54:31 AM
- Email: allcompany@M365x946316.onmicrosoft.com

Upload the identity map

Once the identity mapping file has been prepared, the SharePoint Administrator on the target tenant uploads the file to SharePoint. This will allow identity mapping to occur automatically as part of the cross-tenant migration.

ⓘ Important

Before you run the `Add-SPOTenantIdentityMap -IdentityMapPath` command, save and close the `identitymap.csv` file on your Desktop/OneDrive/SharePoint. If the file remains open, you will receive the following error.

Add-SPOTenantIdentityMap: The process cannot access the file 'C:\Users\myuser\Test-Identity-Map.csv' because it is being used by another process.

1. To upload the identity Map on the target tenant, run the following command. For `-IdentityMapPath`, provide the full path and filename of the identity mapping CSV file.

PowerShell

```
Add-SPOTenantIdentityMap -IdentityMapPath <identitymap.csv>
```

ⓘ Important

If you make or need to make any changes to your Identity Map during the lifecycle of the migration you must run the `Add-SPOTenantIdentityMap -IdentityMapPath <identitymap.csv>` command **every time** a change is made to ensure those changes are applied to the migration.

Uploading any new identity map will overwrite the current one. Make sure that any revision or addition includes ALL users and groups for the full migration. Your identity map should always include everyone you're wanting to migrate.

To look at the mapping entries in the identity mapping file for a particular user, use the command `Get-SPOTenantIdentityMappingUser` with Field as `SourceUserKey` and Value as the UPN of the user you are moving.

Example:

PowerShell

```
get-spoTenantIdentityMappingUser -Field SourceUserKey -Value  
usera@Contoso.onmicrosoft.com
```

Verify cross-tenant compatibility status

Before starting any cross-tenant migrations, make sure that both SharePoint database schemas are up to date and compatible between source and target.

To perform this check, run the below cmdlet on your Source tenant.

PowerShell

```
Get-SPOCrossTenantCompatibilityStatus -PartnerCrossTenantHostURL [Target  
tenant hostname]  
  
Get-SPOCrossTenantCompatibilityStatus -PartnerCrossTenantHostURL  
https://m365x12395529-my.sharepoint.com
```

- If the tenant status shows as **Compatible** or **Warning**, you can then proceed with the next step of starting cross-tenant migrations.
- If the tenant status shows as **Incompatible**, your tenants will need to be patched/updated to ensure compatibility.

[] Expand table

Status	Can proceed with migration
Compatible	Yes
Warning	Yes
Incompatible	No

 **Note**

We recommend waiting a period of 48 hours. If your tenants are still reporting as *incompatible*, contact support.

We recommend performing the compatibility status check on a frequent basis and prior to starting ANY instances of cross tenant migrations. If the tenants are not compatible, this can result in cross-tenant migrations failing.

Step 6: Start a OneDrive cross-tenant migration

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Step 6: Start a OneDrive cross-tenant migration

Article • 08/08/2024

This is Step 6 in a solution designed to complete a Cross-tenant OneDrive migration. To learn more, see [Cross-tenant OneDrive migration overview](#).

- Step 1: [Connect to the source and the target tenants](#)
- Step 2: [Establish trust between the source and the target tenant](#)
- Step 3: [Verify trust has been established](#)
- Step 4: [Precreate users and groups](#)
- Step 5: [Prepare identity mapping](#)
- **Step 6: Start a Cross-tenant OneDrive migration**
- Step 7: [Post migration steps](#)

ⓘ Important

Microsoft recommends that you use roles with the fewest permissions. Using lower permissioned accounts helps improve security for your organization. Global Administrator is a highly privileged role that should be limited to emergency scenarios when you can't use an existing role.

Now you're ready to start your OneDrive migration. Before starting any cross-tenant migration, do the following steps.

1. Ensure you have verified the compatibility status. If you see a status of either **Compatible** or **Warning** on your source tenant, you can continue. Run:

PowerShell

```
Get-SPOCrossTenantCompatibilityStatus -PartnerCrossTenantHostUrl  
[Target tenant hostname]
```

2. To start the migration, a SharePoint Admin or Microsoft 365 Global Admin of the source tenant must run the following command:

PowerShell

```
Start-SPOCrossTenantUserContentMove -SourceUserPrincipalName <...> -  
TargetUserPrincipalName <...> -TargetCrossTenantHostUrl <...>
```

[+] Expand table

Parameters	Description
SourceUserPrincipalName	User principal name of the user who owns the OneDrive on the Source tenant.
TargetUserPrincipalName	User principal name of the user who owns the OneDrive on the Target tenant.
TargetCrossTenantHostUrl	The Cross-tenant Host URL of the target tenant. To find the TargetCrossTenantHostUrl, run <i>Get-SPOCrossTenantHostUrl</i> on the tenant.

Example:

Powershell

```
Start-SPOCrossTenantUserContentMove -SourceUserPrincipalName  
DiegoS@M365x016651.OnMicrosoft.com -TargetUserPrincipalName  
    Test-Diego@M365x946316.OnMicrosoft.com -TargetCrossTenantHostUrl  
https://m365x946316-my.sharepoint.com/
```

To Schedule a migration for a later time, you can use and append the above command with the one of the following parameters.

These commands can be useful when planning bulk batches of OneDrive migrations. You can queue/migrate up to 4,000 OneDrive migrations per batch. If your user count exceeds 4,000, create separate batches, and schedule them to run once the current batch is close to completion.

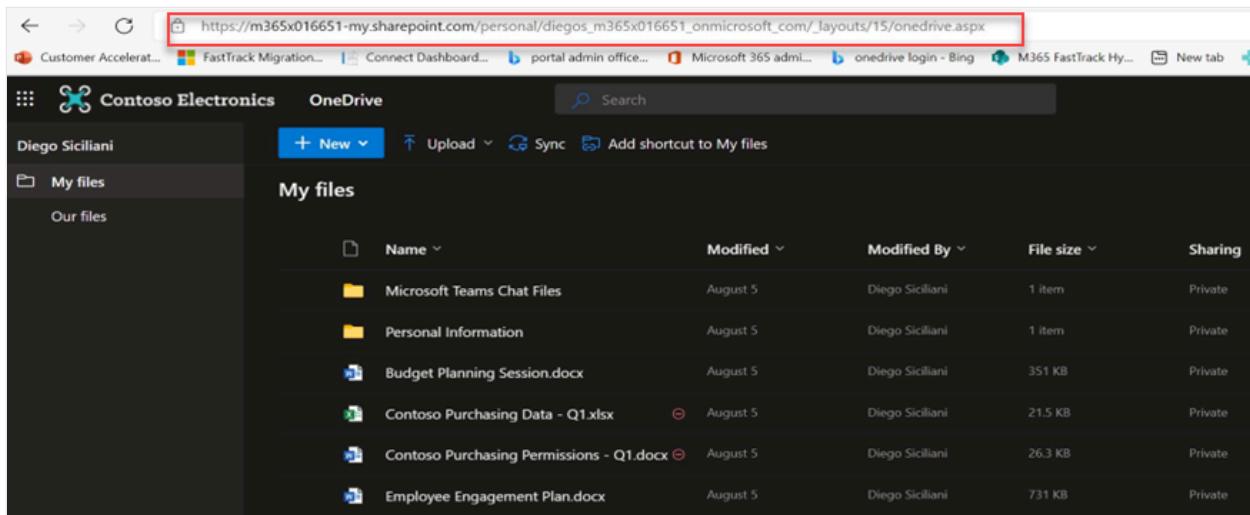
[+] Expand table

Parameter	Description
PreferredMoveBeginDate	The migration will likely begin at this specified time. Time must be specified in Coordinated Universal Time (UTC).
PreferredMoveEndDate	The migration will likely be completed by this specified time, on a best effort basis. Time must be specified in Coordinated Universal Time (UTC).

OneDrive status premigration

Before you start the migration, the users current source OneDrive status is similar to the example below. This example is from the users source tenant, showing their current files

and folders.



The screenshot shows a browser window with the URL https://m365x016651-my.sharepoint.com/personal/diegos_m365x016651_onmicrosoft_com/_layouts/15/onedrive.aspx. The page title is "Contoso Electronics - OneDrive". The left sidebar shows a navigation menu with "My files" selected. The main area is titled "My files" and displays a list of files. The columns are Name, Modified, Modified By, File size, and Sharing. The files listed are:

Name	Modified	Modified By	File size	Sharing
Microsoft Teams Chat Files	August 5	Diego Siciliani	1 item	Private
Personal Information	August 5	Diego Siciliani	1 item	Private
Budget Planning Session.docx	August 5	Diego Siciliani	351 KB	Private
Contoso Purchasing Data - Q1.xlsx	August 5	Diego Siciliani	21.5 KB	Private
Contoso Purchasing Permissions - Q1.docx	August 5	Diego Siciliani	26.3 KB	Private
Employee Engagement Plan.docx	August 5	Diego Siciliani	731 KB	Private

Cancelling a OneDrive migration

You can stop the cross-tenant migration of a user's OneDrive by using the following command, provided the migration doesn't have a status of *In Progress*, *Rescheduled* or *Success*.

PowerShell

```
Stop-SPOCrossTenantUserContentMove – SourceUserPrincipalName [UPN name of user who you wish to stop]
```

Example:

PowerShell

```
Stop-SPOCrossTenantUserContentMove – SourceUserPrincipalName  
DiegoS@M365x016651.OnMicrosoft.com
```

Determining current status of a migration

After starting your migration, you can check its status using the following command on either the source OR target tenant:

Source command format:

PowerShell

```
Get-SPOCrossTenantUserContentMoveState -PartnerCrossTenantHostURL [Target
```

URL]

Example:

Powershell

```
Get-SPOCrossTenantUserContentMoveState -PartnerCrossTenantHostURL  
https://m365x946316-my.sharepoint.com/
```

Target command:

PowerShell

```
Get-SPOCrossTenantUserContentMoveState -PartnerCrossTenantHostURL [Source  
URL]
```

Example:

PowerShell

```
Get-SPOCrossTenantUserContentMoveState -PartnerCrossTenantHostURL  
https://m365x016551-my.sharepoint.com/
```

To find the status of a specific user's migration, use the *SourceUserPrincipalName* parameter:

PowerShell

```
Get-SPOCrossTenantUserContentMoveState -PartnerCrossTenantHostURL  
<PartnerCrossTenantHostURL> -SourceUserPrincipalName <UPN>
```

Example:

PowerShell

```
Get-SPOUserAndContentMoveState -PartnerCrossTenantHostURL  
https://m365x946316-my.sharepoint.com -SourceUserPrincipalName  
DiegoS@m365x016651.onmicrosoft.com
```

To get the status of the move based on a particular user's UPN but with more information, use the *-Verbose* parameter.

Example:

PowerShell

```
Get-SPOCrossTenantUserContentMoveState -PartnerCrossTenantHostURL  
https://ttesttenant-my.sharepoint.com -SourceUserPrincipalName  
User3@stesttenant.onmicrosoft.com -Verbose
```

Migration States

[+] Expand table

Status	Description
NotStarted	The migration hasn't yet started.
Scheduled	The migration is now in the queue and is scheduled to run when a slot becomes available.
ReadytoTrigger	The Migration is in its preflight stage and will start the Migration shortly.
InProgress	The migration is in progress in one of the following states: - Validation - Backup - Restore - Cleanup
Success	The Migration completed successfully.
Rescheduled	The migration may not have completed and has been requeued for another pass.
Failed	The migration failed to complete.

Post-migration status checks

Target tenant: After the migration successfully completes, check the status of the user on the target tenant by logging into their new OneDrive account.

Source tenant: Since the user has successfully migrated to the target tenant, they no longer have an active OneDrive account on the source.

Step 7: Post migration steps

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Step 7: Post migration steps

Article • 10/13/2023

This is Step 7 in a solution designed to complete a Cross-tenant OneDrive migration. To learn more, see [Cross-tenant OneDrive migration overview](#).

- Step 1: [Connect to the source and the target tenants](#)
- Step 2: [Establish trust between the source and the target tenant](#)
- Step 3: [Verify trust has been established](#)
- Step 4: [Pre-create users and groups](#)
- Step 5: [Prepare identity mapping](#)
- Step 6: [Start a Cross-tenant OneDrive migration](#)
- Step 7: [Post migration steps](#)

Removing trust relationship

Important

Ensure you remove the Trust Relationship on both source and target tenants before your source tenant licenses expire. Once the licenses expire, the trust removal command will not work on source.

1. On the source tenant, run this command to remove the trust relationship between Source and Target tenant.

PowerShell

```
Remove-SPOCrossTenantRelationship -Scenario MnA -PartnerRole Target -  
PartnerCrossTenantHostUrl <TARGETCrossTenantHostUrl>
```

2. On the target tenant, run this command to remove the trust relationship between the target and source tenant.

PowerShell

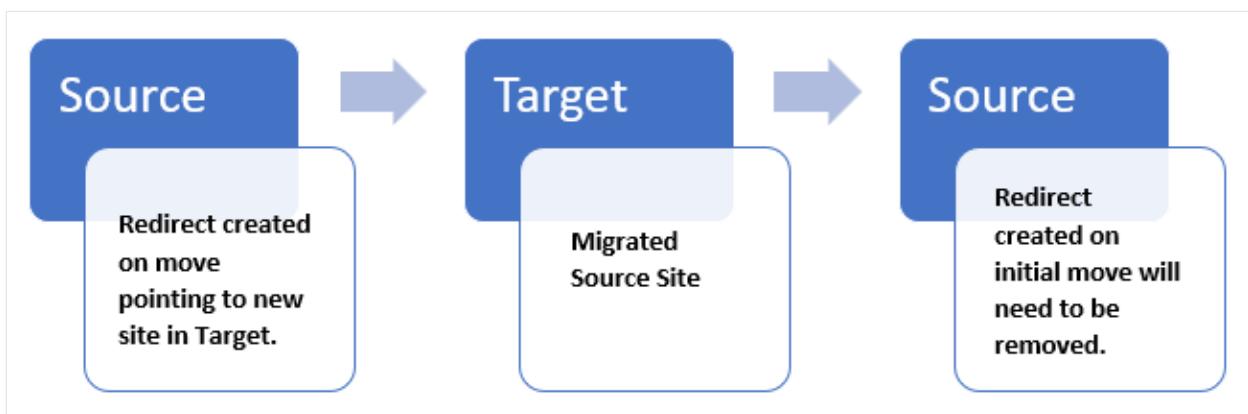
```
Remove-SPOCrossTenantRelationship -Scenario MnA -PartnerRole Target -  
PartnerCrossTenantHostUrl <TARGETCrossTenantHostUrl>
```

Parameter definitions

Parameter	Definition
PartnerRole	Roles of the partner tenant you're establishing trust with. Use <i>source</i> if partner tenant is the source of the OneDrive migrations, and <i>target</i> if the partner tenant is the destination.
PartnerCrossTenantHostURL	The cross-tenant host URL of the partner tenant. The partner tenant can determine this for you by running: <code>Get-SPOCrossTenantHostURL</code> on each of the tenants.

Removing redirect links post migration

After the migration from Source to Target is complete, a redirect link is placed on the source. If users attempt to log back into their Source account or site, the link automatically redirects them to their new Target site. Remove the redirect links on the source after your full migration has completed.



Occasionally, a user may need to be migrated back to the original source. Remove the redirect link on the Target if you migrate a user back to the source.

- To remove redirect links, use the **Remove-SPOSite** PowerShell command.
- To get a list of all redirect sites on a tenant, use the **Get-Sposite -Template RedirectSite#0** command.

Keep track of any user or site you migrate back to the source from the target. After successfully migrating these users or sites back to the source, confirm that the user/sites are accessible. Then you can remove the redirect link from Target using the **Remove-SPOSite** command.



Site URL's must be unique. When migrating a user or site back to the source, the redirect site created on the initial move will use the original URL. This will result in a conflict and cause the migration to fail if not removed. redirect link still being present on the tenant you are attempting to migrate to.

Other post migration steps

Once the migration is complete, OneDrive users must sign in using their new identity and resync their files to their devices on the target tenant.

OneDrive for Business

With their new credentials, have users sign in to OneDrive using the Microsoft 365 app launcher or a web browser.

Permissions on OneDrive content

Users with permission to access OneDrive content will continue to be able to access it, provided they were included in the identity mapping file

OneDrive Sync Client

The user must sign in to the **OneDrive Sync Client** and their new OneDrive location using their new identity. Once you've completed that step, the files and folders will begin resyncing to the device.

Sharing Links

The existing shared links for the migrated files will automatically redirect to the new target location.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Cross-tenant OneDrive migration FAQs

Article • 05/02/2024

Pre-migration FAQs

Question: Can a OneDrive account have any content in the **target tenant** before migration?

Answer: No. The tool doesn't support Merge functionality with existing content. The user being migrated must not have a pre-existing OneDrive on the target tenant.

Question: Can users be precreated on the target tenant?

Answer: Yes, all Users/Groups that are identified for migration should be precreated on the target tenant and appropriate licenses assigned prior to starting any migrations. Also:

- OneDrive site creation should be restricted in the target tenant to prevent users creating OneDrive sites.
- If a OneDrive site already exists for the user on the target tenant the migration fails.
- You can't overwrite an existing site.
- OneDrive sites should NOT be created Prior OR during a migration.

Question: Can my OneDrive accounts be in Read-only mode prior to starting any cross-tenant migrations?

Answer: No. Before starting any migration, you need to ensure that your Source OneDrive accounts are NOT set to Read-Only, otherwise the migration fails.

Question: Can anyone access the OneDrive while the migration process is running?

Answer: During the migration, the user's OneDrive is set to Read-only in Source.

Question: Can my OneDrive accounts be in **Read-only** mode prior to starting any cross-tenant migrations?

Answer: No, before starting any migrations, ensure that your source OneDrive accounts are NOT set to Read-only. Otherwise, the migration fails.

Question: Can anyone access their OneDrive account while the migration process is running?

Answer: No. During the migration, the user's OneDrive is set to Read-Only in source.

Question: Does the tool support GCC and GCC-High tenants?

Answer: We do NOT currently support government environments (GCC & GCC-High) but we plan to support them in the future.

Question: What is the current size limit for each OneDrive migration?

Answer: Each individual OneDrive site/account being migrated must have no more than 2 TB of storage, or 1 million items. The 1,000,000 item limit can be any "item", including files (including versions), folders, and list line entries if it's a list or library. **IMPORTANT:** If you attempt to migrate any OneDrive site that exceeds the 2-TB quota, the transfer fails.

Question: How long does the migration take?

Like most migrations, it's difficult to assign an exact length of time for how long a migration might take. Many things factor into the length of time it takes to migrate, including the number of users/sites, number of files/folders, when you're running your migrations, etc. However, you'll find our process is substantially faster than existing third party migration tools. Bulk migrations complete faster than using standard migration tools.

Question: Are OneDrive accounts with Legal hold supported for migrations?

OneDrive accounts currently under a Hold policy are blocked from migration. To migrate these OneDrive accounts, remove the hold policy, migrate, then reapply the hold as needed on the target tenant.

Question: Are OneDrive accounts with Customer Key Encryption supported for migration?

Answer: No. We do NOT support migration if the source tenant has Service encryption with Microsoft Purview Customer Key enabled.

Question: What do I need to consider for migrating users/sites between Multi-Geo tenants?

Answer: If you're a OneDrive Multi-Geo or MNC customer, you must treat each geography as a separate tenant and supply the correct geography-specific URLs throughout the process. You must also establish trust between each geography involved in your migration project.

Post-migration FAQs

Question: What should users do once their account is migrated to the new Target tenant?

Answer: Once the migration is complete, the user is directed to OneDrive on their new tenant (either via Microsoft 365 app launcher or web browser). Users should sign in to OneDrive using their new credentials.

Question: What happens to permissions on OneDrive content?

Answer: Users with permissions to OneDrive content will continue to have access to

their content upon completion on the new target tenant. If those users/groups were included as part of the Identity Map and mapped accordingly.

Question: What do I need to do to sync my content via OneDrive Sync Client?

Answer: After the migration is complete, the user needs to sign in to their OneDrive Sync client using their new identity and to the new OneDrive location. Once this step is done, files and folders begin resyncing to the device.

Question: What happens to sharing links?

Answer: After a user's OneDrive cross-tenant migration is completed, existing shared links for files that were migrated will automatically redirect to the new target location.

Question: How are shared files handled?

Answer: When a OneDrive account is migrated, we place a redirect at the old location; anyone clicking on a sharing link to the old location is redirected to the new one, provided they still have access on the destination. Those redirects remain until the original/source tenant is deprovisioned or is removed by the admin site-by-site.

Question: Will external Shared Files continue to work?

Answer: As part of the migration process, Admins must precreate the appropriate users on the destination tenant, including guest/external users, and provide the tool with an "Identity Map". The identify map tells us how to adjust file/site ownership and permissions.

Question: Will the shared file map to new internal users?

Answer: See the question above. The identity map informs how files are shared.

Question: If a file is shared in a Teams chat, will those files still be accessible after migration?

Answer: See the question above. The identity map informs how files are shared. If a user selects the link, it attempts to redirect to the new location. The file is accessible as long as the user has permissions to access the file on the destination.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Cross-tenant SharePoint migration (preview)

Article • 05/31/2024

ⓘ Note

Cross-Tenant SharePoint migration is currently in a private preview stage of development. As an unfinished project, any information or availability is subject to change at any time. Support for private-preview customers will be handled via email. Cross-Tenant SharePoint migration is covered by the preview terms of the [Microsoft Universal License Terms for Online Services](#).

SharePoint sites can now be moved from one tenant to another using the Cross-tenant SharePoint migration feature.

Using *SharePoint Online PowerShell*, SharePoint Admins can transition sites into their new tenants.

Up to 4,000 SharePoint accounts can be scheduled for migration in advance at a given time. Once scheduled, migrations occur without content ever leaving the Microsoft 365 cloud and with minimal disruption. When migrations are complete, a redirect is placed in the location of the user's original SharePoint site, so any links to files and folders can continue working in the new location.

ⓘ Important

Cross-Tenant moves are a one and done migration activity. The content will be **moved** from the Source to Target, leaving behind a redirect link on Source. **Incremental and delta migration passes cannot be performed.**

How to participate

The **Cross-Tenant User Content Migration** feature and licenses are currently only available to Enterprise Agreement customers.

If you're an Enterprise Agreement customer who will be purchasing Cross-Tenant User Content Migration licenses, and you would like to evaluate Cross-Tenant SharePoint migration to improve your migration experience, sign-up at:

- <https://aka.ms/ODSPSecurityPreviews>

Make sure to include all of the requested information, and indicate your interest in "SharePoint cross-tenant data migration (Mergers and Acquisition scenario)".

For more information on licensing:

- Contact your Microsoft account team
- [Learn more at Cross-Tenant User Content Migration Licensing.](#)

Prerequisites and settings

- **Microsoft SharePoint Online Powershell.** Confirm you have the most recent version installed. [Download SharePoint Online Management Shell from Official Microsoft Download Center](#)
- **Confirm that the source SharePoint tenant does not have Service encryption with Microsoft Purview Customer Key enabled.** If enabled on Source tenant, the migration will fail. [Learn more on Service encryption with Microsoft Purview Customer Key](#)
- Source SharePoint sites must be set to Read/Write. If set to Read only, the migration will fail.

Target SharePoint sites and Group-connected SharePoint sites

Important

- Don't create any target SharePoint sites before starting your migration. If the site already exists on the target tenant the migration will fail. **You can't overwrite or merge an existing site.**
- Target Microsoft 365 Groups for group-connected SharePoint site migrations **can't** be linked to existing SharePoint sites. Target Microsoft 365 groups must be pre-created in a specific way.

Before starting any migrations, make certain that your source SharePoint sites are set to Read/write mode. If they are set to read-only the migration will fail.

- Each individual SharePoint site being migrated must have no more than 5 TB of storage, or 1 million items. If during a migration of multiple sites a site with more than 5 TB is encountered, that site will eventually timeout and fail. Sites less 5 TB will continue until completion.
- The 1 million item limit can be any "item", including files (including versions), folders, and list line entries if it's a list or library.
- Ensure all users and groups identified for migration have been pre-created on the target tenant.
- Assign the appropriate licenses to each user on either the Source **or** the Target tenant. **The license does not need to be applied in both locations.**

Path size limits

Microsoft character path limit cannot exceed 400 characters. We recommend shortening your Target User and Site URL names to stay within the character limit.

Consider the length of User and Site ULR names in your Target tenant when planning your migrations. Longer user and site URL names may result in migrations failing.

Remember that the source's file or folder path name is combined with the new user or site name on the Target. Make sure that total doesn't exceed the 400-character path limit.

If your migration fails, rename the User or Site URL or work with the user to rename or move the affected files or folders higher up the directory structure to ensure it remains under the character threshold limit. Once resolved, you should be able to complete the migration.

Support SharePoint features

The following types of site can be migrated between geographic locations:

- Microsoft 365 group-connected sites, including those sites associated with Microsoft Teams
- Modern sites without a Microsoft 365 group association
- Classic SharePoint sites
- Communication sites

Important

This feature **does not** include migration of Teams content, channels or associated structure. If a Teams-connected SharePoint site is migrated, only the SharePoint site content will be migrated to the target.

Sharing Links

When the SharePoint site migration completes, the existing shared links for the files that were migrated will automatically redirect to the new geographic location.

Permissions

Users with permissions to site may continue to have access to the site after the migration is complete, provided those users/groups were accounted for in the Identity Mapping step.

SharePoint Workflows

Workflows (2010 or 2013) must be re-created and republished on the Target tenant.

Apps

If you're migrating a site with Apps, you must republish & potentially modify the App on the target tenant.

PowerApps/PowerAutomate

PowerApps & Automation Tasks must be re-created and reconnected to the Site on the target tenant.

Web Parts

Web parts that reference content in other SharePoint Sites and/or other Microsoft 365 services (such as email, calendars) may need to be modified or re-created on the target tenant.

Sensitivity labels

Labels associated with migrated files may not display correctly in M365 user experiences. In addition, any protection or policy associated with the original label won't be present after migration. To apply protection or policy, the recommendation is to remove labels from files before migration, and reapply new labels as appropriate after migration.

Sensitivity Labels with User-Defined Permissions

Sites containing Sensitivity labels with *user-defined permissions* can't be migrated using cross-tenant migration. This guidance refers to sensitivity labels where the setting **Let users assign permissions when they apply the label** is selected in the label definition. More information can be found here: [Enable sensitivity labels for files in SharePoint and OneDrive](#).

In order to migrate sites containing Sensitivity labels with *user-defined permissions*, the labels must first be removed from files within the sites. This action can be done either manually, or by using **Unlock-SPOSensitivityLabelEncryptedFile**.

Example:

```
Unlock-SPOSensitivityLabelEncryptedFile. -FileUrl  
"https://contoso.com/sites/Marketing/Shared Documents/Doc1.docx" -JustificationText  
"Need to decrypt this file".
```

Communicating with your users

When migrating SharePoint sites between tenants, it's important to communicate to your users what to expect.

- How will this migration impact them?
- Will they be able to continue to work during the migration?
- When will the migration start and how long will it last?
- What is the new URL in which to access their new site plus any other details about the new tenant
- Advise users to close their files and not make any edits during their migration window.
- Advise of any file permissions or sharing changes that may occur as part of the migration.

Scheduling SharePoint site migrations

You can schedule SharePoint site migrations in advance but consider the following recommendations:

- Start with a small number of sites to validate your workflows and communication strategies
- Once you're comfortable with the process, you can schedule large batches of migrations.
- You can schedule up to 4,000 migrations at a time per batch
- As the migrations begin, you can schedule more, with a maximum of 4,000 pending migrations in the queue at any given time.

Get started

- Step 1: [Connect to the source and the target tenants](#).
- Step 2: [Establish trust between the source and the target tenant](#)
- Step 3: [Verify trust has been established](#)
- Step 4: [Pre-create users and groups](#)
- Step 5: [Prepare identity mapping](#)
- Step 6: [Start a Cross-tenant SharePoint migration](#)
- Step 7: [Post migration steps](#)

Step 1: [Connect to source and target tenants](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Step 1: Connect to the source and target tenants (preview)

Article • 05/02/2024

ⓘ Note

Cross-Tenant SharePoint migration is currently in a private preview stage of development. As an unfinished project, any information or availability is subject to change at any time. Support for private-preview customers will be handled via email. Cross-Tenant SharePoint migration is covered by the preview terms of the [Microsoft Universal License Terms for Online Services](#).

This is Step 1 in a solution designed to complete a **Cross-tenant SharePoint migration**.

To learn more, see [Cross-tenant SharePoint migration overview](#).

- Step 1: [Connect to the source and the target tenants](#)
- Step 2: [Establish trust between the source and the target tenant](#)
- Step 3: [Verify trust has been established](#)
- Step 4: [Precreate users and groups](#)
- Step 5: [Prepare identity mapping](#)
- Step 6: [Start a Cross-tenant SharePoint migration](#)
- Step 7: [Post migration steps](#)

Before you begin

- **Microsoft SharePoint Powershell.** Confirm you have the most recent version installed. If not, [Download SharePoint Management Shell from Official Microsoft Download Center](#).
- Be a SharePoint admin or Microsoft 365 Global admin on both the source and target tenants

Connect to both tenants

1. Sign in to the SharePoint Management Shell as a SharePoint admin or Microsoft 365 Global admin.
2. Run the following entering the **source** tenant URL:

PowerShell

```
Connect-SPOService -url https://<TenantName>-admin.sharepoint.com
```

3. When prompted, sign in to the **source** tenant using your Admin username and password.
4. Run the following entering the **target** tenant URL:

PowerShell

```
Connect-SPOService -url https://<TenantName>-admin.sharepoint.com
```

5. When prompted, sign in to the **target** tenant using your Admin username and password.

ⓘ Important

Microsoft 365 Multi-Geo customers: You must treat each geography as a separate tenant. Provide the correct geography-specific URLs throughout the migration process.

Step 2: Establish trust between the source and target tenants

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Step 2: Establishing trust between the source and target tenants (preview)

Article • 10/13/2023

ⓘ Note

Cross-Tenant SharePoint migration is currently in a private preview stage of development. As an unfinished project, any information or availability is subject to change at any time. Support for private-preview customers will be handled via email. Cross-Tenant SharePoint migration is covered by the preview terms of the [Microsoft Universal License Terms for Online Services](#).

This is Step 2 in a solution designed to complete a Cross-tenant SharePoint migration.

To learn more, see [Cross-tenant SharePoint migration overview](#).

- Step 1: [Connect to the source and the target tenants](#)
- **Step 2: Establish trust between the source and the target tenant**
- Step 3: [Verify trust has been established](#)
- Step 4: [Precreate users and groups](#)
- Step 5: [Prepare identity mapping](#)
- Step 6: [Start a Cross-tenant SharePoint migration](#)
- Step 7: [Post migration steps](#)

After connecting to the source and target tenant, the next step in performing a cross-tenant SharePoint migration is establishing trust between the tenants.

To establish trust, each SharePoint tenant administrator must run specific commands on both source and target tenants. Once the trust has been requested, the administrator of the target tenant will receive an email informing them that another tenant is trying to establish a trust relationship.

ⓘ Note

The "trust" command is specific to SharePoint. It only grants permission for the SharePoint administrator on the source tenant to execute SharePoint Migration operations to the identified target tenant.

Granting trust *doesn't* give the administrator any visibility, permission, or ability to collaborate between the source tenant and the target tenant.

ⓘ Important

If you are Microsoft 365 Multi-Geo customer, you must establish trust between each geography involved in your migration project.

Before you begin

Before running the trust commands, obtain the cross-tenant host URLs for both the source and target tenants. You'll need these URLs when establishing the trust relationship between source-to-target and target-to-source.

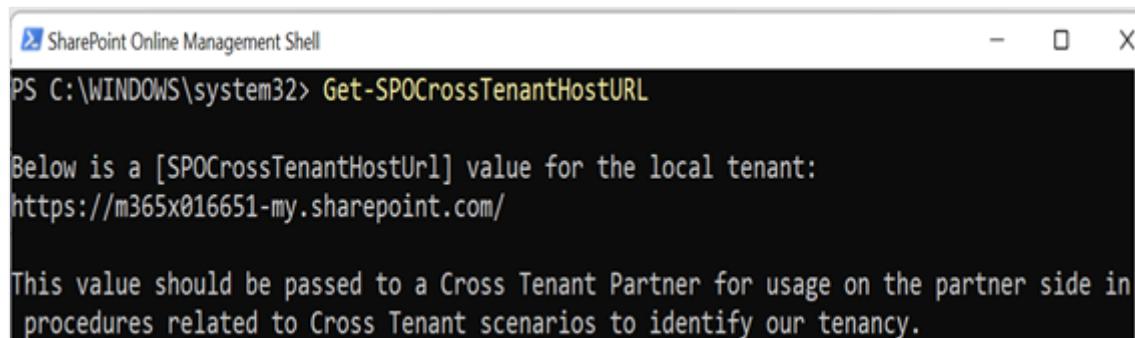
To obtain the cross-tenant host URLs:

On both the source and target tenants, run:

PowerShell

```
Get-SPOCrossTenantHostURL
```

Example: Run command on Source tenant:

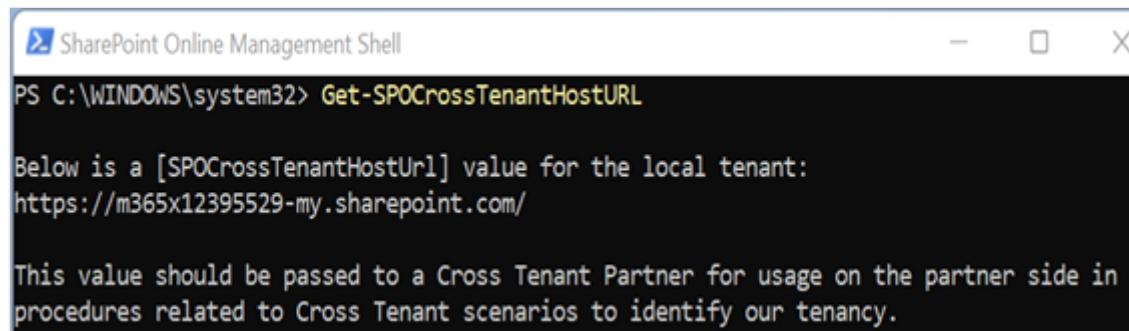


```
PS C:\WINDOWS\system32> Get-SPOCrossTenantHostURL

Below is a [SPOCrossTenantHostUrl] value for the local tenant:
https://m365x016651-my.sharepoint.com/

This value should be passed to a Cross Tenant Partner for usage on the partner side in
procedures related to Cross Tenant scenarios to identify our tenancy.
```

Example: Run command on target tenant:



```
PS C:\WINDOWS\system32> Get-SPOCrossTenantHostURL

Below is a [SPOCrossTenantHostUrl] value for the local tenant:
https://m365x12395529-my.sharepoint.com/

This value should be passed to a Cross Tenant Partner for usage on the partner side in
procedures related to Cross Tenant scenarios to identify our tenancy.
```

Run the trust commands

These commands send a request to the tenant with whom you want to establish trust.

1. On the source tenant, run this command to send a trust request to the target tenant:

```
PowerShell
```

```
Set-SPOCrossTenantRelationship -Scenario MnA -PartnerRole Target -  
PartnerCrossTenantHostUrl <TARGETCrossTenantHostUrl>
```

2. On the target tenant, run this command to send a trust request to the source tenant:

```
PowerShell
```

```
Set-SPOCrossTenantRelationship -Scenario MnA -PartnerRole Source -  
PartnerCrossTenantHostUrl <SOURCECrossTenantHostUrl>
```

Parameter definitions

[+] Expand table

Parameter	Definition
PartnerRole	Roles of the partner tenant you're establishing trust with. Use <i>source</i> if partner tenant is the source of the SharePoint migrations, and <i>target</i> if the partner tenant is the Destination.
PartnerCrossTenantHostURL	The cross-tenant host URL of the partner tenant. The partner tenant can determine this for you by running: <i>Get-SPOCrossTenantHostURL</i> on each of the tenants.

Sample trust email

The following is an example of the email that is sent to global admins:

 SharePoint Online <no-reply@sharepointonline.com>
To: ○ ; @msftfetesttenantAdvEncryp.onmicrosoft.com;
○ ; @msftfetesttenantAdvEncryp.onmicrosoft.com;
○ ; @msftfetesttenantAdvEncryp.onmicrosoft.com;
○ ; @microsoft365demos.com; ○ ; @microsoft365demos.com;
○ ; migrationAdmin@msftfetesttenantadvencryp.onmicrosoft.com; ○ ; AdvEncryptAdminProd
SPO Tenant [<https://a830edad9050849mnaus093022-my.sharepoint.com/>] [setuporupdate] Organization Relation [Scenario=MnA, Role=Source] with us

Subject: SPO Tenant [<https://a830edad9050849mnaus093022-my.sharepoint.com/>]
[setuporupdate] Organization Relation [Scenario=MnA, Role=Source] with us

Message: SPO Tenant [https://a830edad9050849mnaus093022-my.sharepoint.com/] [setuporupdate] Organization Relation [Scenario=MnA, Role=Source] with us

Step 3: Verify that trust has been established

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Step 3: Verifying trust (preview)

Article • 10/13/2023

ⓘ Note

Cross-Tenant SharePoint migration is currently in a private preview stage of development. As an unfinished project, any information or availability is subject to change at any time. Support for private-preview customers will be handled via email. Cross-Tenant SharePoint migration is covered by the preview terms of the [Microsoft Universal License Terms for Online Services](#).

This article is Step 3 in a solution designed to complete a [Cross-tenant SharePoint migration](#). To learn more, see [Cross-tenant SharePoint migration overview](#).

- Step 1: [Connect to the source and the target tenants](#)
- Step 2: [Establish trust between the source and the target tenant](#)
- **Step 3: Verify trust has been established**
- Step 4: [Pre-create users and groups](#)
- Step 5: [Prepare identity mapping](#)
- Step 6: [Start a Cross-tenant SharePoint migration](#)
- Step 7: [Post migration steps](#)

Before proceeding with your migration, you need to verify the trust is complete. A status of *GoodToProceed* confirms that the trust is verified.

To verify trust has been established

1. On the **source tenant** run:

PowerShell

```
Verify-SPOCrossTenantRelationship -Scenario MnA -PartnerRole Target -  
PartnerCrossTenantHostUrl <TARGETCrossTenantHostUrl>
```

2. On the **target tenant** run:

PowerShell

```
Verify-SPOCrossTenantRelationship -Scenario MnA -PartnerRole Source -  
PartnerCrossTenantHostUrl <SOURCECrossTenantHostUrl>
```

Troubleshooting trust issues

When verifying trust, possible values

[Expand table](#)

Value	Description
NotEstablished	Trust hasn't been requested locally.
NotEstablishedByPartner	Partner hasn't requested the Trust
DormantByPartner	Partner's requested trust is within the seven days waiting period after creation.
CouldNotContactPartner	Couldn't contact the partner to determine status.
GoodToProceed	Verified to proceed.

Step 4: Pre-create users and groups

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Step 4: Pre-creating users and groups (preview)

Article • 10/13/2023

ⓘ Note

Cross-Tenant SharePoint migration is currently in a private preview stage of development. As an unfinished project, any information or availability is subject to change at any time. Support for private-preview customers will be handled via email. Cross-Tenant SharePoint migration is covered by the preview terms of the [Microsoft Universal License Terms for Online Services](#).

This is Step 4 in a solution designed to complete a Cross-tenant SharePoint migration.

To learn more, see [Cross-tenant SharePoint migration overview](#).

- Step 1: [Connect to the source and the target tenants](#)
- Step 2: [Establish trust between the source and the target tenant](#)
- Step 3: [Verify trust has been established](#)
- **Step 4: Pre-create users and groups**
- Step 5: [Prepare identity mapping](#)
- Step 6: [Start a Cross-tenant SharePoint migration](#)
- Step 7: [Post migration steps](#)

Identify users and groups to be migrated

To ensure that SharePoint permissions are retained as part of the migration, a mapping file needs to be created to align users from the source tenant to the target tenant.

1. Identify the full list of SharePoint users and sites that will be migrated from the source to the target tenant.
2. Identify the list of Microsoft 365 Groups that are connected to any Group-connected SharePoint sites that will be migrating as part of your project.
3. Prepare a complete list of users, groups, and Microsoft 365 groups that will be migrated to the target tenant.

Pre-create users, groups, and Microsoft 365 groups on the target tenant

- Pre-create users and groups as needed in the target tenant's directory.
- All users who are migrating to the target tenant must have new user identities created for them in the target tenant.

 **Note**

Note: If these users are also having their OneDrive migrated, make sure that these new users don't attempt to sign-in to their new target OneDrive until their corresponding OneDrive migration is complete.

- All users whose SharePoint accounts are migrating to the target tenant must be assigned the appropriate SharePoint license.
- Any users who remain in the source tenant but need access to resources migrating to the target tenant should have new guest identities created for them in the target tenant.
- Pre-created users must be added as members of any appropriate security groups or unified groups before the SharePoint migration begins.
- If the user or group name already exists in the target tenant, create a user or group with a different name and make a note of it for the next step.
- We recommend that SharePoint site creations are restricted in the target tenant to prevent users from creating SharePoint sites.

 **Note**

To learn more on restricting SharePoint site creation, see [Disable SharePoint creation for some users](#)

Pre-create Microsoft 365 groups connect to SharePoint sites

Microsoft 365 groups connected to SharePoint sites must be pre-created using the [Exchange Online management shell](#)

These commands send a request to the tenant with whom you want to establish trust.

1. Sign in to the Exchange Online Management Shell as an Exchange Online Admin or Microsoft 365 Global admin. Enter the password for target tenant when prompted.

PowerShell

```
Connect-ExchangeOnline -UserPrincipalName <UserPrincipalName>
```

2. Create the appropriate Microsoft 365 groups, where *AccessType* matches the access type of the corresponding Microsoft 365 group on the source tenant.

PowerShell

```
New-UnifiedGroup -DisplayName <TargetGroupDisplayName> -Alias  
<TargetGroupAlias> -AccessType <Private|Public>
```

 **Important**

Microsoft 365 Groups connected to SharePoint sites **MUST** be pre-created using **this method**. Pre-creating Microsoft 365 groups using any other methods will cause SharePoint site migrations to fail.

Step 5: Prepare the identity mapping file

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Step 5: Identity mapping (preview)

Article • 10/13/2023

ⓘ Note

Cross-Tenant SharePoint migration is currently in a private preview stage of development. As an unfinished project, any information or availability is subject to change at any time. Support for private-preview customers will be handled via email. Cross-Tenant SharePoint migration is covered by the preview terms of the [Microsoft Universal License Terms for Online Services](#).

This is Step 5 in a solution designed to complete a Cross-tenant SharePoint migration.

To learn more, see [Cross-tenant SharePoint migration overview](#).

- Step 1: [Connect to the source and the target tenants](#)
- Step 2: [Establish trust between the source and the target tenant](#)
- Step 3: [Verify trust has been established](#)
- Step 4: [Pre-create users and groups](#)
- Step 5: **Prepare identity mapping**
- Step 6: [Start a Cross-tenant SharePoint migration](#)
- Step 7: [Post migration steps](#)\n

Create the identity mapping file

In this step of the cross-tenant migration process, you're going to create a single CSV (comma separated values) file that contains the mapping of the users and groups on the source tenant to their corresponding users and groups on the target tenant.

We recommend that you take the time to verify your mappings, ensuring they're accurate before starting any migrations to the target tenant.

There's a one-to-one relationship in the identity mapping file. You can't map the same user to multiple users in the target tenant. For example, if you have instances where the admin is the owner of multiple SharePoint accounts, the ownership must be changed to match the corresponding user you wish to migrate from Source to Target. If you don't, those account files won't migrate.

Example: In this example, the admin owns multiple SharePoint accounts.

[+] Expand table

Source Tenant Owner	Target Tenant User
admin@source.com	new.userA@target.com
admin@source.com	new.userB@target.com
admin@source.com	new.userC@target.com

Cross-tenant migration supports this scenario:

Example:

 Expand table

Source Tenant Owner	Target Tenant User
userA@source.com	new.userA@target.com
userB@source.com	new.userB@target.com
userC@source.com	new.userC@target.com

Create the CSV file

There are six columns needed in your CSV file. The first three are your source values, each providing detail about where your data is currently located. The remaining three columns are the corresponding info on the target tenant. All six columns must be accounted for in the file. Create your file in Excel and save it as a .csv file.

Users and groups are included in the same file. Depending on whether it's a user or group, what you enter in the column is different. In each of the columns enter values as shown in the examples. **Do NOT include column headings.**

 Expand table

Column	User	Group	Microsoft 365 Group
1	User	Group	Group
2	SourceTenantCompanyID	SourceTenantCompanyID	SourceTenantCompanyID
3	SourceUserUpn	SourceGroupObjectID	SourceGroupObjectID
4	TargetUserUpn	TargetGroupObjectID	TargetGroupObjectID
5	TargetUserEmail	GroupName	M365GroupAlias

Column	User	Group	Microsoft 365 Group
6	UserType	GroupType	GroupType

ⓘ Important

When creating your Identity Mapping for Group Connected sites, the Target site URL must align with the alias of the new Group created on the Target tenant.

Example:

- Source site: <https://contoso.sharepoint.com/teams/0365SourceGroup>
- New Target Group Alias = O365TargetGroup

In your Identity Mapping file the Target site needs to be:

<https://fabrikam.sharepoint.com/teams/0365TargetGroup>.

If the Target Alias and Target URL don't align, the migration will fail.

Do NOT include column headings in your CSV file. In the examples below we include them for illustrative purposes only.

Users. Enter your values as shown in this example for Users:

User	SourceTenantCompanyID	SourceUserUpn	TargetUserUpn	TargetUserEmail	UserType
------	-----------------------	---------------	---------------	-----------------	----------

Example: Mapping a member account (Source) to member account (Target)					
User	SourceTenantCompanyID	SourceUserUpn	TargetUserUpn	TargetUserEmail	UserType
User	03cb84b4-2f99-4b43-93fb-d4479e9b57af	user@source.com	John@target.com	John@target.com	RegularUser

Guest users. You can map guest accounts in the source tenant to member accounts in the target tenant. You can also map a guest account in the source to a guest account in the target if the guest has been previously created. Enter your values as shown in this example for guests:

Example: Mapping a Guest Account (Source) to Member Account (Target)					
User	SourceTenantCompanyID	SourceUserUpn	TargetUserUpn	TargetUserEmail	UserType
User	03cb84b4-2f99-4b43-93fb-d4479e9b99zz	user1_outlook.com#EXT#@source.onmicrosoft.com	john@target.com	john@target.com	GuestUser

Example: Mapping a Guest Account (Source) to Guest Account (Target)					
User	SourceTenantCompanyID	SourceUserUpn	TargetUserUpn	TargetUserEmail	UserType
User	03cb84b4-2f99-4b43-93fb-d4479e9b99zz	user1_outlook.com#EXT#@source.onmicrosoft.com	user1_outlook.com	user1@target.com	GuestUser

Groups. Enter your values as shown in this example for groups:

Group	SourceTenantCompanyID	SourceGroupObjectID	TargetGroupObject ID	GroupName	GroupType

Example:

Group	SourceTenantCompanyID	SourceGroupObjectID	TargetGroupObject ID	GroupName	GroupType
Group	03cb84b4-2f99-4b43-93fb-d4479e9b57af	94d00e94-a007-4b14-bf16-159b26ec2853	34a09691-899c-4613-895c-0e653061630d	34a09691-899c-4613-895c-0e653061630d	RegularGroup

Microsoft 365 Groups. Enter your values as shown in this example for Microsoft 365 groups:

A	B	C	D	E	F
1 Group	SourceTenantCompanyID	SourceGroupObjectID	TargetGroupObjectID	M365GroupAlias	GroupType
2 User	03cb84b4-2f99-4b43-93fb-d4479e9b57af	94d00e94-a007-4b14-bf16-159b26ec2853	34a09691-899c-4613-895c-0e653061630d	TargetGroupAlias12345	O365Group
3					

Multiple users and groups in a CSV file:

Example:

Group	9f724407-653e-46b3-be44-c2129e5ff698	94d00e94-a007-4b14-bf16-159b26ec2853	34a09691-899c-4613-895c-0e653061630d	34a09691-899c-4613-895c-0e653061630d	RegularGroup
Group	9f724407-653e-46b3-be44-c2129e5ff698	225adfea-d7ed-4c63-9c87-e2e8dc9b991c	34a09691-899c-4613-895c-0e653061630d	34a09691-899c-4613-895c-0e653061630d	RegularGroup
User	9f724407-653e-46b3-be44-c2129e5ff698	AdeleV@M365x016651.OnMicrosoft.com	Test-Adele@M365x946316.OnMicrosoft.com	Test-Adele@M365x946316.OnMicrosoft.com	RegularUser
User	9f724407-653e-46b3-be44-c2129e5ff698	AllanD@M365x016651.OnMicrosoft.com	Test-AllanD@M365x946316.OnMicrosoft.com	Test-AllanD@M365x946316.OnMicrosoft.com	RegularUser
User	9f724407-653e-46b3-be44-c2129e5ff698	DiegoS@M365x016651.OnMicrosoft.com	Test-Diego@M365x946316.OnMicrosoft.com	Test-Diego@M365x946316.OnMicrosoft.com	RegularUser
User	9f724407-653e-46b3-be44-c2129e5ff698	JoniS@M365x016651.OnMicrosoft.com	Test-Joni@M365x946316.OnMicrosoft.com	Test-Joni@M365x946316.OnMicrosoft.com	RegularUser
User	9f724407-653e-46b3-be44-c2129e5ff698	MeganB@M365x016651.OnMicrosoft.com	Test-Megan@M365x946316.OnMicrosoft.com	Test-Megan@M365x946316.OnMicrosoft.com	RegularUser
User	9f724407-653e-46b3-be44-c2129e5ff698	NestorW@M365x016651.OnMicrosoft.com	Test-NestorW@M365x946316.OnMicrosoft.com	Test-NestorW@M365x946316.OnMicrosoft.com	RegularUser

Obtain the source tenant company ID

To obtain Source Tenant Company ID:

1. Sign in as Admin to your [Azure portal](#)
2. Select or Search for **Microsoft Entra ID**.
3. Scroll down on the left-hand panel and select **Properties**.
4. Locate the **Tenant ID Field**. The required Tenant ID will be in that box.

The screenshot shows the 'Tenant properties' section of the Microsoft Entra ID Properties page. The 'Tenant ID' field is highlighted with a blue selection bar, containing the value '9f724407-653e-46b3-be44-c2129e5ff698'. Other fields visible include 'Name' (Contoso), 'Country or region' (United States), 'Location' (United States datacenters), 'Notification language' (English), 'Technical contact' (transformprov@microsoft.com), 'Global privacy contact' (empty), and 'Privacy statement URL' (empty).

To obtain source group object ID:

1. Sign in to source tenant as Admin to [Azure Groups](#).
2. Search for your required group(s).
3. Select the required Group instance and then **Copy to clipboard**. Paste this value in the `sourceGroupId` column of your mapping CSV file.
4. If you have multiple Groups to map, then repeat these steps for each group.

The screenshot shows the 'All Company' group details in the Azure Groups interface. The group name is 'All Company'. It is described as 'This is the default group for everyone in the network'. The group has the following properties:

Property	Value
Membership type	Assigned
Source	Cloud
Type	Microsoft 365
Object Id	94d00e94-a007-4b14-bf16-159b26ec2853
Creation date	8/5/2021, 11:25:51 AM
Email	allcompany@M365x016651.onmicrosoft.com

A 'Copy to clipboard' button is visible next to the Object Id field.

To obtain target group object ID:

1. Sign in to Target tenant as Admin to [Azure Groups](#)
2. Search for your required group(s).
3. Select the required group instance and then **Copy to clipboard**. Paste this value in the `targetGroupId` column of your mapping CSV file.
4. If you have multiple groups to map, then repeat the above process to obtain those specific `targetGroupId`'s.
5. For the `GroupName`, use the same ID as the `TargetGroupId` you obtained.

The screenshot shows the 'All Company' group details in the Azure Groups interface. The group name is 'All Company'. It is described as 'This is the default group for everyone in the network'. The group has the following properties:

Property	Value
Membership type	Assigned
Source	Cloud
Type	Microsoft 365
Object Id	34a09691-899c-4613-895c-0e653061630d
Creation date	8/9/2021, 2:54:31 AM
Email	allcompany@M365x946316.onmicrosoft.com

A 'Copy to clipboard' button is visible next to the Object Id field.

Upload the identity map

Once the identity mapping file has been prepared, the SharePoint Administrator on the target tenant uploads the file to SharePoint. This will allow identity mapping to occur

automatically as part of the cross-tenant migration.

ⓘ Important

Before you run the `Add-SPOTenantIdentityMap -IdentityMapPath` command, save and close the `identitymap.csv` file on your Desktop/SharePoint/SharePoint.

If the file remains open, you will receive the following error. `Add-SPOTenantIdentityMap: The process cannot access the file 'C:\Users\myuser\Test-Identity-Map.csv' because it is being used by another process.`

1. To upload the identity Map on the target tenant, run the following command. For `-IdentityMapPath`, provide the full path and filename of the identity mapping CSV file.

PowerShell

```
Add-SPOTenantIdentityMap -IdentityMapPath <identitymap.csv>
```

ⓘ Important

If you make or need to make any changes to your Identity Map during the lifecycle of the migration you must run the `Add-SPOTenantIdentityMap -IdentityMapPath <identitymap.csv>` command **every time** a change is made to ensure those changes are applied to the migration.

Uploading any new identity map will overwrite the current one. Make sure that any revision or addition includes ALL users and groups for the full migration. Your identity map should always include everyone you're wanting to migrate.

To look at the mapping entries in the identity mapping file for a particular user, use the command `Get-SPOTenantIdentityMappingUser` with Field as `SourceUserKey` and Value as the UPN of the user you are moving.

Example:

PowerShell

```
get-spoTenantIdentityMappingUser -Field SourceUserKey -Value  
usera@Contoso.onmicrosoft.com
```

Verify cross-tenant compatibility status

Before starting any cross-tenant migrations, make sure that both SharePoint database schemas are up to date and compatible between source and target.

To perform this check, run the below cmdlet on your Source tenant.

PowerShell

```
Get-SPOCrossTenantCompatibilityStatus -PartnerCrossTenantHostURL [Target  
tenant hostname]
```

```
Get-SPOCrossTenantCompatibilityStatus -PartnerCrossTenantHostURL  
https://m365x12395529-my.sharepoint.com
```

- If the tenant status shows as **Compatible** or **Warning**, you can then proceed with the next step of starting cross-tenant migrations.
- If the tenant status shows as **Incompatible**, your tenants will need to be patched/updated to ensure compatibility.

[+] Expand table

Status	Can proceed with migration
Compatible	Yes
Warning	Yes
Incompatible	No

ⓘ Important

We recommend waiting a period of **48 hours**. If your tenants are still reporting as *incompatible*, contact support.

We recommend performing the compatibility status check on a frequent basis and prior to starting ANY instances of cross tenant migrations. If the tenants are not compatible, this can result in cross-tenant migrations failing.

Step 6: Start a SharePoint cross-tenant migration

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Step 6: Start a SharePoint site cross-tenant migration (preview)

Article • 10/13/2023

ⓘ Note

Cross-Tenant SharePoint migration is currently in a private preview stage of development. As an unfinished project, any information or availability is subject to change at any time. Support for private-preview customers will be handled via email. Cross-Tenant SharePoint migration is covered by the preview terms of the [Microsoft Universal License Terms for Online Services](#).

This is Step 6 in a solution designed to complete a Cross-tenant SharePoint migration.

To learn more, see [Cross-tenant SharePoint migration overview](#).

- Step 1: [Connect to the source and the target tenants](#)
- Step 2: [Establish trust between the source and the target tenant](#)
- Step 3: [Verify trust has been established](#)
- Step 4: [Pre-create users and groups](#)
- Step 5: [Prepare identity mapping](#)
- **Step 6: [Start a Cross-tenant SharePoint migration](#)**
- Step 7: [Post migration steps](#)

Now you're ready to start your SharePoint migration. Before starting any cross-tenant migration, do the following steps.

Start a SharePoint Cross-tenant site migration

1. Make sure you've verified the compatibility status. If you see a status of either **Compatible** or **Warning** on your source tenant, you may continue. Run:

PowerShell

```
Get-SPOCrossTenantCompatibilityStatus -PartnerCrossTenantHostURL  
[Target tenant hostname]
```

2. To start the migration, a SharePoint Admin or Microsoft 365 Global Admin of the source tenant must run the following command:

PowerShell

```
Start-SPOCrossTenantSiteContentMove -SourceSiteUrl <...> -TargetSiteUrl <...>
> -TargetCrossTenantHostUrl <...>
```

[+] Expand table

Parameters	Description
SourceSiteUrl	Full URL of the SharePoint Site of the Source tenant, for example: <code>https://sourcetenant.sharepoint.com/sites/sitename.</code>
TargetSiteUrl	Full URL of the SharePoint Site of the Target tenant, for example: <code>https://targettenant.sharepoint.com/sites/newsitename.</code>
TargetCrossTenantHostUrl	The Cross-tenant host URL of the target tenant. The target tenant Admin can determine the TargetCrossTenantHostUrl by running <code>Get-SPOCrossTenantHostUrl</code> on their tenant.

Start a SharePoint Microsoft 365 Group connected site cross-tenant migration

1. Ensure to verify the compatibility status. If you see a status of either **Compatible** or **Warning** on your source tenant, you may continue. Run:

PowerShell

```
Get-SPOCrossTenantCompatibilityStatus -PartnerCrossTenantHostURL
[Target tenant hostname]
```

2. To start the migration, a SharePoint Admin or Microsoft 365 Global Admin of the source tenant must run the following command:

PowerShell

```
Start-SPOCrossTenantGroupContentMove -SourceGroupAlias <...> -
TargetGroupAlias <...> -TargetCrossTenantHostUrl <...>
```

[+] Expand table

Parameters	Description
SourceGroupAlias	Alias of the Microsoft 365 Group connected to the SharePoint Site on the Source tenant. For example: SourceGroup1
TargetGroupAlias	Alias of the Microsoft 365 that was created on the target tenant
TargetCrossTenantHostUrl	The Cross-tenant Host URL of the target tenant. The target tenant Admin can determine the TargetCrossTenantHostUrl by running <i>Get-SPOCrossTenantHostUrl</i> on their tenant

Schedule a migration for a later time

To schedule a migration for a later time, add one of the following parameters to the command.

For example:

PowerShell

```
Start-SPOCrossTenantGroupContentMove -SourceGroupAlias <...> -  
TargetGroupAlias <...> -TargetCrossTenantHostUrl <...> -PreferredMoveBeginDate  
<...>
```

These commands can be useful when planning bulk batches of site migrations. You can queue and migrate up to 4,000 migrations per batch. If your count exceeds 4,000, then separate batches can be created and scheduled to run once the current batch is close to completion.

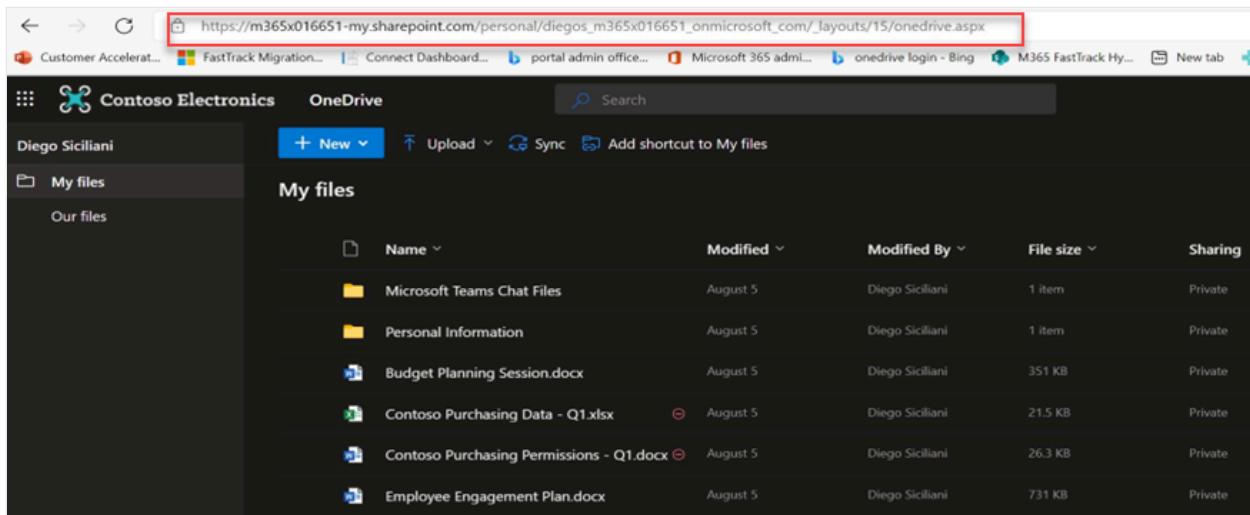
[\[+\] Expand table](#)

Parameter	Description
PreferredMoveBeginDate	The migration will likely begin at this specified time. Time must be specified in Coordinated Universal Time (UTC).
PreferredMoveEndDate	The migration will likely be completed by this specified time, on a best effort basis. Time must be specified in Coordinated Universal Time (UTC).

SharePoint status pre-migration

Before you begin the migration, the users current source SharePoint status will be similar to the following. This example is from the users source tenant, showing their

current files and folders.



The screenshot shows a web browser window with the URL https://m365x016651-my.sharepoint.com/personal/diegos_m365x016651_onmicrosoft_com/_layouts/15/onedrive.aspx. The page title is "Contoso Electronics - OneDrive". The left sidebar shows a navigation menu with "My files" selected. The main area is titled "My files" and displays a list of files with columns for Name, Modified, Modified By, File size, and Sharing. The files listed are:

Name	Modified	Modified By	File size	Sharing
Microsoft Teams Chat Files	August 5	Diego Siciliani	1 item	Private
Personal Information	August 5	Diego Siciliani	1 item	Private
Budget Planning Session.docx	August 5	Diego Siciliani	351 KB	Private
Contoso Purchasing Data - Q1.xlsx	August 5	Diego Siciliani	21.5 KB	Private
Contoso Purchasing Permissions - Q1.docx	August 5	Diego Siciliani	26.3 KB	Private
Employee Engagement Plan.docx	August 5	Diego Siciliani	731 KB	Private

Cancelling a SharePoint site migration

You can stop the cross-tenant migration of either a SharePoint site or SharePoint Microsoft 365 Group by using the following command, provided the migration doesn't have a status of *In Progress* or *Success*.

To cancel a SharePoint site migration:

PowerShell

```
Stop-SPOCrossTenantSiteContentMove – SourceSiteURL [URL of Site you wish to stop]
```

To cancel a SharePoint Microsoft 365 Group migration:

PowerShell

```
Stop-SPOCrossTenantGroupContentMove – SourceGroupAlias [Alias of Group connected to site you wish to stop]
```

Determining current status of a migration

After starting your migration, you can check its status using the following command on either the source OR target tenant:

Source command format:

PowerShell

```
Get-SPOCrossTenantUserContentMoveState -PartnerCrossTenantHostURL [Target URL]
```

Example:

Powershell

```
Get-SPOCrossTenantUserContentMoveState -PartnerCrossTenantHostURL  
https://m365x946316-my.sharepoint.com/
```

Target command:

PowerShell

```
Get-SPOCrossTenantUserContentMoveState -PartnerCrossTenantHostURL [Source URL]
```

Example:

PowerShell

```
Get-SPOCrossTenantUserContentMoveState -PartnerCrossTenantHostURL  
https://m365x016551-my.sharepoint.com/
```

To find the status of a specific user's migration, use the *SourceUserPrincipalName* parameter:

PowerShell

```
Get-SPOCrossTenantUserContentMoveState -PartnerCrossTenantHostURL  
<PartnerCrossTenantHostURL> -SourceUserPrincipalName <UPN>
```

Example:

PowerShell

```
Get-SPOUserAndContentMoveState -PartnerCrossTenantHostURL  
https://m365x946316-my.sharepoint.com -SourceUserPrincipalName  
DiegoS@m365x016651.onmicrosoft.com
```

To get the status of the move based on a particular user's UPN but with more information, use the *-Verbose* parameter.

Example:

PowerShell

```
Get-SPOCrossTenantUserContentMoveState -PartnerCrossTenantHostURL  
https://ttesttenant-my.sharepoint.com -SourceUserPrincipalName  
User3@stesttenant.onmicrosoft.com -Verbose
```

Migration States

[+] Expand table

Status	Description
NotStarted	The migration hasn't yet started.
Scheduled	The migration is now in the queue and is scheduled to run when a slot becomes available.
ReadytoTrigger	The Migration is in its pre-flight stage and will start the Migration shortly.
InProgress	The migration is in progress in one of the following states: - Validation - Backup - Restore - Cleanup
Success	The Migration has completed successfully.
Rescheduled	The migration may not have completed and has been requeued for another pass.
Failed	The migration failed to complete.

Post-migration status checks

Target tenant: After the migration has successfully completed, check the status of the user on the target tenant by logging into their new SharePoint account.

Source tenant: Once the user has successfully migrated to the target tenant, they no longer have an active SharePoint account on the source.

Step 7: Post migration steps

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Step 7: Post migration steps (preview)

Article • 10/13/2023

ⓘ Note

Cross-Tenant SharePoint migration is currently in a private preview stage of development. As an unfinished project, any information or availability is subject to change at any time. Support for private-preview customers will be handled via email. Cross-Tenant SharePoint migration is covered by the preview terms of the [Microsoft Universal License Terms for Online Services](#).

This is Step 7 in a solution designed to complete a Cross-tenant SharePoint migration. To learn more, see [Cross-tenant SharePoint migration overview](#).

- Step 1: [Connect to the source and the target tenants](#)
- Step 2: [Establish trust between the source and the target tenant](#)
- Step 3: [Verify trust has been established](#)
- Step 4: [Pre-create users and groups](#)
- Step 5: [Prepare identity mapping](#)
- Step 6: [Start a Cross-tenant SharePoint migration](#)
- Step 7: [Post migration steps](#)

Removing trust relationship

ⓘ Important

Make sure you remove the Trust Relationship on both source and target tenants before your source tenant licenses expire. Once the licenses expire, the trust removal command will not work on source.

1. On the source tenant, run this command to remove the trust relationship between Source and Target tenant.

PowerShell

```
Remove-SPOCrossTenantRelationship -Scenario MnA -PartnerRole Target -  
PartnerCrossTenantHostUrl <TARGETCrossTenantHostUrl>
```

2. On the target tenant, run this command to remove the trust relationship between the target and source tenant.

```
PowerShell
```

```
Remove-SPOCrossTenantRelationship -Scenario MnA -PartnerRole Target -  
PartnerCrossTenantHostUrl <TARGETCrossTenantHostUrl>
```

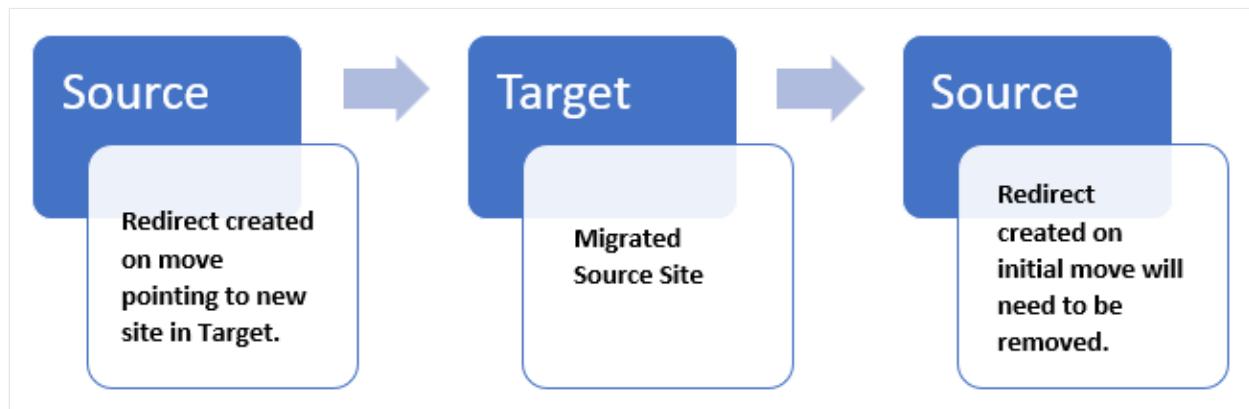
Parameter definitions

[+] Expand table

Parameter	Definition
PartnerRole	Roles of the partner tenant you're establishing trust with. Use <i>source</i> if partner tenant is the source of the SharePoint migrations, and <i>target</i> if the partner tenant is the destination.
PartnerCrossTenantHostURL	The cross-tenant host URL of the partner tenant. The partner tenant can determine this for you by running: <i>Get-SPOCrossTenantHostURL</i> on each of the tenants.

Removing redirect links post migration

After the migration from Source to Target is complete, a redirect link is placed on the source. If users attempt to log back into their Source account or site, the link automatically redirects them to their new Target site. Remove the redirect links on the source after your full migration has completed.



Occasionally, a user may need to be migrated back to the original source. Remove the redirect link on the Target if you migrate a user back to the source.

- To remove redirect links, use the **Remove-SPOSite** PowerShell command.

- To get a list of all redirect sites on a tenant, use the **Get-Sposite -Template RedirectSite#0** command.

Keep track of any user or site you migrate back to the source from the target. After successfully migrating these users or sites back to the source, confirm that the user/sites are accessible. Then you can remove the redirect link from Target using the **Remove-SPOSite** command.

Important

Site URL's must be unique. When migrating a user or site back to the source, the redirect site created on the initial move will use the original URL. This will result in a conflict and cause the migration to fail if not removed. redirect link still being present on the tenant you are attempting to migrate to.

Other post migration steps

Existing links and permissions should continue to work as expected once the migration is complete, based on the identity mapping files that were created.

SharePoint sites

The source SharePoint site is set to read-only while a migration is in progress. Once the migration is complete, users are directed to the site in the new target tenant whenever they navigate to the source site. Users must sign in using their target tenant credentials.

Permissions on SharePoint content

Users with permissions to SharePoint content will continue to have access to the content during the migration and after it is complete, provided that those users or groups were included as part of the identity mapping step.

Sharing Links

The existing shared links for the migrated files will automatically redirect to the new target location.

Note

Customers need to manually add the labels which they might have removed before migration.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Cross-tenant SharePoint migration FAQs (Preview)

Article • 10/13/2023

ⓘ Note

Cross-Tenant SharePoint migration is currently in a private preview stage of development. As an unfinished project, any information or availability is subject to change at any time. Support for private-preview customers will be handled via email. Cross-Tenant SharePoint migration is covered by the preview terms of the [Microsoft Universal License Terms for Online Services](#).

Premigration FAQs

Question: Can a SharePoint account have any content in the **target tenant** before migration?

Answer: No. The tool doesn't support Merge functionality with existing content. The user being migrated must not have a pre-existing SharePoint on the target tenant.

Question: Can users be precreated on the target tenant?

Answer: Yes, all Users/Groups that are identified for migration should be precreated on the target tenant and appropriate licenses assigned prior to starting any migrations. Also:

- SharePoint site creation should be restricted in the target tenant to prevent users creating SharePoint sites.
- If a SharePoint site already exists for the user on the target tenant the migration fails.
- You can't overwrite an existing site.
- SharePoint sites should NOT be created Prior OR during a migration.

Question: Can my SharePoint accounts be in Read-only mode prior to starting any cross-tenant migrations?

Answer: No. Before starting any migration, you need to ensure that your Source SharePoint accounts are NOT set to Read-Only, otherwise the migration fails.

Question: Can my SharePoint accounts be in **Read-only** mode prior to starting any cross-tenant migrations?

Answer: No, before starting any migrations, ensure that your source SharePoint accounts are NOT set to Read-only. Otherwise, the migration fails.

Question: Does the tool support GCC and GCC-High tenants?

Answer: We don't currently support government environments (GCC & GCC-High) but we plan to support them in the future.

Question: Are SharePoint accounts with Customer Key Encryption supported for migration?

Answer: No. We do NOT support migration if the source tenant has Service encryption with Microsoft Purview Customer Key enabled.

Question: What do I need to consider for migrating sites between Multi-Geo tenants?

Answer: If you're a SharePoint Multi-Geo or MNC customer, you must treat each geography as a separate tenant and supply the correct geography-specific URLs throughout the process. You must also establish trust between each geography involved in your migration project.

Post-migration FAQs

Question: What happens to permissions on SharePoint content?

Answer: Users with permissions to SharePoint content continues to have access to their content upon completion on the new target tenant. If those users/groups were included as part of the Identity Map and mapped accordingly.

Question: What happens to sharing links?

Answer: After the SharePoint cross-tenant migration, existing shared links for files that were migrated will automatically redirect to the new target location.

Question: How are shared files handled?

Anyone clicking on a sharing link to the old location will be redirected to the new location. The original/source tenant is deprovisioned or can be removed by the admin site-by-site basis.

Question: Will external Shared Files still work?

Answer: As part of the migration process, Admins must precreate the appropriate users on the destination tenant, including guest/external users, and provide the tool with an "Identity Map." The identify map tells us how to adjust file/site ownership and permissions.

Question: If a file is shared in a Teams chat, will those files still be accessible after migration?

Answer: See the question above. The identity map informs how files are shared. If a user selects on the link, it attempts to redirect to the new location. The file is accessible as long as the user has permissions to access the file on the destination.

Feedback

Was this page helpful?

 Yes

 No

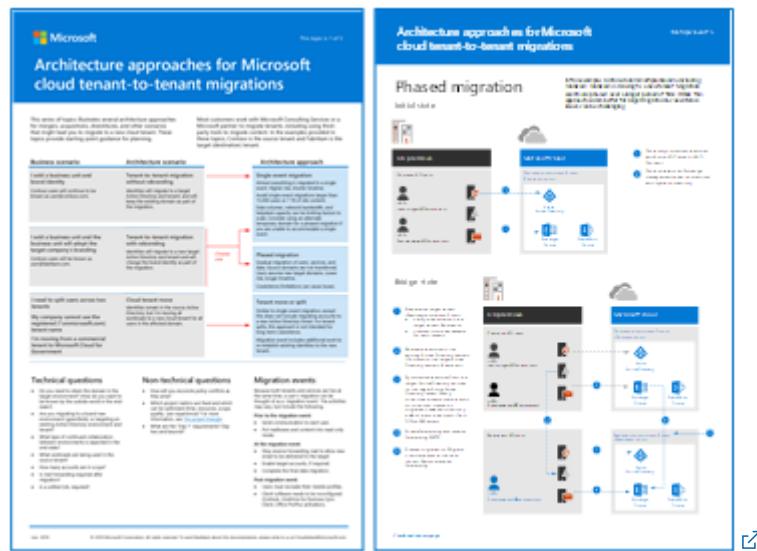
Provide product feedback ↗

Microsoft 365 tenant-to-tenant migrations

Article • 07/22/2024

There are several architecture approaches for mergers, acquisitions, divestitures, and other scenarios that might lead you to migrate an existing Microsoft 365 tenant to a new tenant. Most customers work with Microsoft Consulting Services or a Microsoft partner to migrate tenants, including using third-party tools to migrate content.

Use the [Tenant-to-tenant migration architecture model](#) to understand how to plan for Microsoft 365 tenant-to-tenant migrations and the steps of a migration.



You download this model in [PDF](#) format and print it on letter, legal, or tabloid (11 x 17 inches) size paper.

This model provides guidance and a starting-point for planning with sections on:

- Mapping of business scenarios to architecture approaches
- Design considerations

This model also contains detailed examples of:

- A single event migration flow
- A phased migration flow
- A tenant move or split flow

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Overview and Definitions

Article • 03/01/2024

Definitions

In order to promote clarity in the capability descriptions on data residency functionality in this document, refer to these terms.

Table 1: Definitions and Terms

 Expand table

Term	Definition
Macro Region Geography	Macro Region Geography 1 – EMEA, Macro Region Geography 2 – Asia Pacific, Macro Region Geography 3 - Americas
Macro Region Geography 1 - EMEA	Data centers in Austria, Finland, France, Ireland, Israel, Italy, Netherlands, Poland, Spain, Sweden
Macro Region Geography 2 - Asia Pacific	Data centers in Australia, Hong Kong Special Administrative Region, Japan, Malaysia, Singapore, South Korea
Macro Region Geography 3 - Americas	Data centers in Brazil, Chile, Mexico, United States
Local Region Geography	Australia, Brazil, Canada, France, Germany, India, Israel, Italy, Japan, Mexico, Norway, Poland, Qatar, South Africa, South Korea, Spain, Sweden, Switzerland, United Arab Emirates, United Kingdom
Future Local Region Geography	Future planned data center regions: Indonesia, Malaysia, Austria, Chile, New Zealand, Denmark, Greece, Taiwan, Saudi Arabia
Geography	<i>Local Region Geography, Future Local Region Geography, or Macro Region Geography</i>
Satellite Geography	If a customer subscribes to the Multi Geo service, then they can set policy at a user level to store customer data in other Geographies outside of the <i>Tenant Primary Provisioned Geography</i>
Microsoft Entra ID	Microsoft Entra ID
Tenant	A <i>Tenant</i> represents an organization in Microsoft Entra ID. It's a reserved Microsoft Entra service instance that an organization receives and owns when it signs up for a Microsoft cloud service such as Azure or Microsoft 365. Each Microsoft Entra ID <i>Tenant</i> is distinct and separate from other Microsoft Entra ID Tenants

Term	Definition
Default Geography	When a <i>Microsoft Entra ID Tenant</i> is created, a country/region is provided by the customer during the sign-up process. This country/region determines the default Geography for all Microsoft 365 services. In some cases, not all services are able to provision in this single <i>Default Geography</i> . See <i>Microsoft 365 Service provisioning mapping</i> below for a description.
Microsoft 365 Service provisioning mapping	All Microsoft 365 Services use the <i>Default Geography</i> to determine where a given <i>Tenant's</i> specified data will be provisioned and stored.
Microsoft 365 Service provisioning country mapping	Refer to data maps to learn where a given service provisions specified customer data, based on the <i>Tenant Default Geography</i> .
Primary Provisioned Geography	A given Microsoft 365 service uses the <i>Tenant Default Geography</i> combined with the <i>Microsoft 365 Service provisioning country mapping</i> to determine which <i>Geography</i> to provision customer data into.
Microsoft 365 admin center Data Location	To see the <i>Primary Provisioned Geography</i> for Exchange Online, SharePoint, OneDrive, and Microsoft Teams refer to Microsoft 365 admin center in Admin > Settings > Org Settings > Organization Profile > Data Location .
Microsoft 365 Multi-Geo Capabilities	Microsoft 365 Multi-Geo Capabilities allows a single <i>Tenant</i> to store customer data-at-rest across multiple geographies rather than be limited to the single <i>Primary Provisioned Geography</i> . See the Multi-Geo description for more detail.
Preferred Data Location (PDL)	Used for <i>Tenants</i> with a Multi-Geo subscription. A property set by the administrator that indicates where the user or shared resource's data should be stored at-rest. See the Multi-Geo description for more detail.
Advanced Data Residency (ADR)	A new Microsoft 365 add-on service that guarantees customer data residency for a defined set of services. See section 3
Privacy and Security Product Terms	<p>Privacy and Security Terms for Microsoft 365 services provides some customer data location related commitments. The document can be found here. The extract of the relevant section (on November 1, 2022) is:</p> <p>Office 365 Services. If Customer provisions its <i>Tenant</i> in Australia, Brazil, Canada, the European Union, France, Germany, India, Japan, Norway, Qatar, South Africa, South Korea, Sweden, Switzerland, the United Kingdom, the United Arab Emirates, or the United States, Microsoft stores the following Customer Data at rest only within that Geo: (1) Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments), (2) SharePoint site content and the files stored within that site, (3) files uploaded to OneDrive, and (4) Microsoft Teams chat messages (including private messages, channel messages, meeting messages and images used in chats), and for customers using Microsoft Stream (on SharePoint), meeting recordings, and (5) any stored content of interactions with Microsoft Copilot for Microsoft 365 to the extent not included in the preceding commitments.</p>
Workloads	Often used to refer to a Microsoft 365 service such as but not limited to Exchange Online, SharePoint, OneDrive, Microsoft Teams, etc.

Overview of Data Residency

Microsoft 365 Cloud services run on our data centers around the world and provide services to customers around the world. Customer data might be stored in multiple data centers. Data residency refers to the geographic location where customer data is stored at rest. Data residency is important for government, public sector, education and regulated commercial entities to help ensure protection of personal and/or sensitive information. In many countries/regions, customers are expected to comply with laws, regulations or industry standards that explicitly govern the location of data storage.

Microsoft makes decisions on where to persistently store customer data based on two factors:

1. The *Default Geography* of the *Tenant*
2. Available *Geographies* for a given service

Default Geography* of the Microsoft Entra ID *Tenant

When a customer creates a new Microsoft Entra ID *Tenant*, the customer enters a country/region during the creation process. This country/region is what defines the *Default Geography* for the *Tenant*. There are multiple paths to creating *Tenants*. They can be created through Microsoft Entra ID forms, they can be created when trying out new Microsoft 365 services (trials), etc. Once a *Tenant* is created, the *Default Geography* can't be changed.

Available Geographies for a given service

Microsoft 365 services aren't deployed to all Microsoft data centers globally. The larger services, like Exchange Online, SharePoint, OneDrive, and Microsoft Teams are universally deployed to all *Geographies*. Other services make decisions on where to deploy their services based on the number of customers, regional affiliations, and software architectures. When a customer first uses a service in this category, the provisioning logic uses the *Default Geography* and the supported *Geographies* to determine where to provision a given customer.

Over time, a particular service may deploy their software to additional *Geographies*, so the provisioning locations for new customers can change over time. This doesn't necessarily cause customer data to move to a new *Geography*.

You can use the Microsoft 365 admin center to understand where your data for a given service is stored. As a *Tenant* administrator you can find the actual data location by navigating to **Admin > Settings > Org Settings > Organization Profile > Data Location**. Currently the data location is available for Exchange Online, SharePoint, OneDrive, Microsoft Teams, Microsoft Copilot for Microsoft 365, Exchange Online Protection, Viva Connections and Viva Topics. In addition to this resource, see the [Data Maps page](#).

Some examples:

Example 1: For a *Tenant* with the sign-up country/region as "France" that has a new subscription that includes Exchange Online, SharePoint, OneDrive and Microsoft Teams, then the customer data for

those services will be provisioned into the French *Local Region Geography*. Why? Because those services are deployed into the French data centers and the *Tenant* has a France sign up country/region.

Example 2: For a *Tenant* with the sign-up country/region as "Belgium" that has a new subscription that includes Exchange Online, SharePoint, OneDrive and Microsoft Teams, then the customer data for those services will be provisioned into the *Macro Region Geography 1 – EMEA*. Why? Because there are no Microsoft 365 data centers in Belgium and the closest Geography is *Macro Region Geography 1 - EMEA*.

Example 3: For a *Tenant* with the sign-up country/region as "Japan" that has a new subscription that includes Microsoft Forms, then the customer data for Forms will be provisioned into the *Macro Region Geography 3 - Americas*. Why? Because Forms is only deployed in *Macro Region Geography 3 - Americas* and *Macro Region Geography 1 – EMEA* (EU *Tenants* only).

Example 4a: For a *Tenant* with the sign-up country/region as "Sweden" that has a new subscription that includes Microsoft Viva Engage, then the customer data for Viva Engage will be provisioned into the *Macro Region Geography 1 - EMEA*. Why? Because Viva Engage is deployed in *Macro Region Geography 1 - EMEA* and Swedish *Tenants* are best served out of that *Geography*.

Example 4b: For a *Tenant* with the sign-up country/region as "Sweden" that has a subscription that includes Microsoft Viva Engage from before Viva Engage was deployed to *Macro Regional Geography 1 - EMEA*, then the customer data for Viva Engage will be located in *Macro Region Geography 3 - Americas*. Why? Because, at that time, Viva Engage only had a single deployment for all customers in *Macro Region Geography 3 - Americas*.

Migrations/Moves

Once a Microsoft 365 service provisions a *Tenant* into a particular *Geography*, there are three ways that this data could move to another *Geography*:

1. The Microsoft 365 service decides to move the data to a new *Geography* for service operations reasons, if there are no other policies in place to prevent the move.
2. If a *Tenant* subscribes to the *Multi-Geo* service, then *Tenants* user's data for Exchange Online, SharePoint, OneDrive, Microsoft Teams and Microsoft Copilot for Microsoft 365 can be assigned to *Satellite Geographies*.
3. If a *Tenant* has sign up country/region as a *Local Region Geography* and has a subscription to the *Advanced Data Residency* service add-on, then the *Tenant* data for the included services will be migrated from the *Regional Geography* to the relevant *Local Region Geography*.

Durable commitments on data location

There are three methods for ensuring that the *Tenant* data location for a particular service doesn't change.

1. Product Terms: Exchange Online, SharePoint, OneDrive, Microsoft Teams and Microsoft Copilot for Microsoft 365 provisioned in Australia, Brazil, Canada, France, Germany, India, Japan, Qatar, South Korea, Norway, South Africa, Sweden, Switzerland, United Arab Emirates, United

Kingdom, European Union and the United States have a commitment for customer data residency expressed in the [Product Terms](#). For more information, see the [Product Terms Data Residency page](#).

2. *Multi Geo* subscription: allows customers to assign data location for Exchange Online, SharePoint, OneDrive, Microsoft Teams and Microsoft Copilot for Microsoft 365 to any supported *Geography*. For more information, see [Multi Geo Data Residency](#).
3. *Advanced Data Residency* subscription provides data residency commitments for an expanded set of Microsoft 365 services in any *Local Region Geography*. For more information, see the [Advanced Data Residency page](#).

Table 2: Available Data Residency by Workload

 [Expand table](#)

Service Name	Product Terms	Multi-Geo	ADR
Exchange Online	X ¹	X ²	X ³
SharePoint / OneDrive	X ¹	X ²	X ³
Microsoft Teams	X ¹	X ²	X ³
Microsoft Copilot for Microsoft 365	X ¹	X ²	X ³
Microsoft Defender for Office P1	-	-	X ³
Office for the Web	-	-	X ³
Viva Connections	-	-	X ³
Viva Topics	-	-	X ³
Microsoft Purview	-	-	X ³

1. Only available in the following countries/regions: Australia, Brazil, Canada, France, Germany, India, Japan, Qatar, South Korea, Norway, South Africa, Sweden, Switzerland, United Arab Emirates, United Kingdom, European Union and the United States.
2. Available in *Local Region Geography*, *Future Local Region Geography* (when the future data center is launched) and *Regional Geography countries/regions*
3. Only available for *Local Region Geography* and *Future Local Region Geography* (when the future data center is launched) countries/regions.

 **Note**

See the [Workload Data Residency Capabilities section](#) for more details on these topics.

Table 3: Available Data Residency by Country/Region

 [Expand table](#)

Country/Region	Exchange	SharePoint,	Teams	Copilot	MDO	Office	Viva	Viva	Purview
	Online	OneDrive		for Microsoft 365	P1	for the web	Connections	Topics	
Australia	P-M-A	P-M-A	P-M-A	P-M-A	A	A	A	A	A
Brazil	P-M-A	P-M-A	P-M-A	P-M-A	A	A	A	A	A
Canada	P-M-A	P-M-A	P-M-A	P-M-A	A	A	A	A	A
European Union	P-M	P-M	P-M	P-M	-	-	-	-	-
France	P-M-A	P-M-A	P-M-A	P-M-A	A	A	A	A	A
Germany	P-M-A	P-M-A	P-M-A	P-M-A	A	A	A	A	A
India	P-M-A	P-M-A	P-M-A	P-M-A	A	A	A	A	A
Israel	M-A	M-A	M-A	M-A	A	A	A	A	A
Italy	M-A	M-A	M-A	M-A	A	A	A	A	A
Japan	P-M-A	P-M-A	P-M-A	P-M-A	A	A	A	A	A
Mexico	M-A	M-A	M-A	M-A	A	A	A	A	A
Norway	P-M-A	P-M-A	P-M-A	P-M-A	A	A	A	A	A
Poland	M-A	M-A	M-A	M-A	A	A	A	A	A
Qatar	P-M-A	P-M-A	P-M-A	P-M-A	A	A	A	A	A
South Africa	P-M-A	P-M-A	P-M-A	P-M-A	A	A	A	A	A
South Korea	P-M-A	P-M-A	P-M-A	P-M-A	A	A	A	A	A
Spain	M-A	M-A	M-A	M-A	A	A	A	A	A
Sweden	P-M-A	P-M-A	P-M-A	P-M-A	A	A	A	A	A
Switzerland	P-M-A	P-M-A	P-M-A	P-M-A	A	A	A	A	A
United Arab Emirates	P-M-A	P-M-A	P-M-A	P-M-A	A	A	A	A	A
United Kingdom	P-M-A	P-M-A	P-M-A	P-M-A	A	A	A	A	A
United States	P-M	P-M	P-M	P-M	-	-	-	-	-

P: Product Terms Data Residency

M: Multi-Geo Data Residency

A: Advanced Data Residency

Country/Region specific Data Center city locations

The following Regional Geographies can store data at rest.

Table 4: Current Local Geographies and Region specific Datacenter locations

[\[+\] Expand table](#)

Country/Region	Datacenter Location
Australia	Sydney, Melbourne
Brazil	Rio, Campinas
Canada	Quebec City, Toronto
European Union	Austria (Vienna), Finland (Helsinki), France (Paris, Marseille), Ireland (Dublin), Italy (Milan), Netherlands (Amsterdam), Poland (Warsaw), Spain (Madrid), Sweden (Gävle, Sandviken, Staffanstorp)
France	Paris, Marseille
Germany	Frankfurt, Berlin
India	Chennai, Mumbai, Pune
Israel	Tel Aviv
Italy	Milan
Japan	Osaka, Tokyo
South Korea	Busan, Seoul
Spain	Madrid
Mexico	Queretaro
Norway	Oslo, Stavanger
Poland	Warsaw
Qatar	Doha
South Africa	Cape Town, Johannesburg
Sweden	Gävle, Sandviken, Staffanstorp
Switzerland	Geneva, Zurich
United Arab Emirates	Dubai, Abu Dhabi
United Kingdom	Durham, London, Cardiff
United States	Boydton, Cheyenne, Chicago, Des Moines, Quincy, San Antonio, Santa Clara, San Jose

FAQ

How does Microsoft define data?

▼ Select to expand

Review our [definitions for different types of customer data](#) on the Microsoft Trust Center. In the [Privacy & Security Terms](#), Microsoft makes contractual commitments regarding customer data/your *Tenant* and user data. We refer to customer data as the customer data that is committed to be stored at rest only within a *Tenant's* region according to the [Privacy & Security Terms](#).

Where are the exact addresses of the data centers?

▼ Select to expand

Microsoft doesn't disclose the exact addresses of its data centers. We established this policy to help secure our data center facilities. However, we do list city locations. See Table 5 in the [Country/Region-specific Data Center City Locations](#) on the Overview and Definitions page to learn more.

Does the location of your customer data have a direct impact on your end users' experience?

▼ Select to expand

The performance of Microsoft 365 isn't simply proportional to a *Tenant* user's distance to data center locations. Microsoft's continued investments in its global cloud network, global cloud infrastructure, and the Microsoft 365 services architecture help provide users with a singular, consistent experience independent of where customer data is stored at rest. If your users are experiencing performance issues, you should troubleshoot those in depth. Microsoft has published guidance for Microsoft 365 customers to plan for and optimize end-user performance on the [Office Support web site](#).

How does Microsoft help me comply with my national, regional, and industry-specific regulations?

▼ Select to expand

To help a *Tenant* comply with national, regional, and industry-specific requirements governing the collection and use of individuals' data, Microsoft 365 offers the most comprehensive set of compliance offerings of any global cloud productivity provider. Review [our compliance offerings](#) and more details in the [Microsoft Purview](#) section on the Microsoft Trust Center. Also, certain Microsoft 365 plans offer further compliance solutions to help a *Tenant* manage their data, comply with legal and regulatory requirements, and monitor actions taken on their data.

Who can access your data and according to what rules?

▼ Click to expand

Microsoft implements strong measures to help protect a *Tenant's* customer data from inappropriate access or use by unauthorized persons. This includes restricting access by Microsoft personnel and subcontractors, and carefully defining requirements for responding to government requests for

customer data. However, you can access your *Tenant's* customer data at any time and for any reason. More details are available on the [Microsoft Trust Center](#).

Does Microsoft access your data?

▼ Select to expand

Microsoft automates most Microsoft 365 operations while intentionally limiting its own access to customer data. This helps us manage Microsoft 365 at scale and address the risks of internal threats to customer data. By default, Microsoft engineers have no standing administrative privileges and no standing access to customer data in Microsoft 365. A Microsoft engineer may have limited and logged access to customer data for a limited amount of time, but only when necessary for normal service operations and only when approved by a member of senior management at Microsoft (and, for customers who are licensed for the Customer Lockbox feature, by the customer).

How does Microsoft secure your data?

▼ Select to expand

Microsoft has robust policies, controls, and systems built into Microsoft 365 to help keep your information safe. Review the [Microsoft 365 security section](#) on the Microsoft Trust Center to learn more.

Does Microsoft 365 encrypt your data?

▼ Select to expand

Microsoft 365 uses service-side technologies that encrypt customer data at rest and in transit. For customer data at rest, Microsoft 365 uses volume-level and file-level encryption. For customer data in transit, Microsoft 365 uses multiple encryption technologies for communications between data centers and between clients and servers, such as Transport Layer Security (TLS) and Internet Protocol Security (IPsec). Microsoft 365 also includes customer-managed encryption features.

Where can I find data residency information for Microsoft Azure?

▼ Select to expand

Review the [Products available by region](#) page to find data residency information for Microsoft Azure.

Why do I see my Microsoft 365 service requests for my data at rest connecting to servers in countries outside of my region?

▼ Click to expand

On occasion, a customer request may be handled by servers in a different region than the location where a *Tenant's* customer data is stored at rest. This may happen where network routing decisions choose a different server for the request processing, but in these cases such *Tenant's* customer data is not moved to a new at rest location.

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Overview of Product Terms Data Residency

Article • 03/01/2024

Microsoft Privacy and Security product terms included with Microsoft's Cloud product terms provides data residency commitment with the following scope:

1. Online Services: Exchange Online, SharePoint, OneDrive, Microsoft Teams (as of November 1, 2022) and Microsoft Copilot for Microsoft 365 (as of March 1, 2024).
2. Commitments period: The length of the customers contract with Microsoft. Typically, this is 1-3 years.
3. Country/regions included: Australia, Brazil, Canada, France, Germany, India, Japan, Norway, Qatar, South Africa, South Korea, Sweden, Switzerland, the United Kingdom, the United Arab Emirates, United States and the European Union.

The language at time of writing this article is:

- **Office 365 Services** If Customer provisions its tenant in Australia, Brazil, Canada, the European Union, France, Germany, India, Japan, Norway, Qatar, South Africa, South Korea, Sweden, Switzerland, the United Kingdom, the United Arab Emirates, or the United States, Microsoft stores the following Customer Data at rest only within that Geo: (1) Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments), (2) SharePoint site content and the files stored within that site, (3) files uploaded to OneDrive, (4) Microsoft Teams chat messages (including private messages, channel messages, meeting messages and images used in chats), and for customers using Microsoft Stream (on SharePoint), meeting recordings, and (5) any stored content of interactions with Copilot for Microsoft 365 to the extent not included in the preceding commitments.
- For current language, refer to the Privacy and Security Product Terms [webpage](#) and view the section titled "Location of Customer Data at Rest for Core Online Services."

For more data residency capabilities, refer to the [Multi-Geo service](#) and/or the [Advanced Data Residency service](#).

Product Terms Data Residency Migration

When Microsoft's data centers were launched in Australia, Brazil, Canada, the European Union, France, Germany, India, Japan, Norway, Qatar, South Africa, South Korea, Sweden, Switzerland, the United Kingdom, or the United Arab Emirates, it was possible for any

Tenant with the appropriate *Default Geography* to opt in to move their data into the applicable geography. This opt in period was open for six months after the Data Center was operational. Today, the *tenant* must have a valid subscription to the Advanced Data Residency add-on in order to migrate data into the country data centers.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Advanced Data Residency in Microsoft 365

Article • 04/08/2024

Overview of Advanced Data Residency

The Microsoft 365 Advanced Data Residency add-on (ADR) provides eligible customers with expanded coverage of Microsoft 365 workloads and Customer Data, committed data residency for local country/region datacenter regions, and prioritized tenant migration services. With Advanced Data Residency, enterprise customers can best address their data residency compliance and tenant location requirements.

The following workloads are included in ADR. For more information, see:

- [Exchange Online](#)
- [SharePoint and OneDrive](#)
- [Microsoft Teams](#)
- [Microsoft Copilot for Microsoft 365](#)
- [Microsoft Defender for Office P1 and Exchange Online Protection](#)
- [Office for the Web](#)
- [Viva Connections](#)
- [Viva Topics](#)
- [Microsoft Purview](#)
 - [Audit \(Standard\)](#)
 - [Audit \(Premium\)](#)
 - [Data Retention](#)
 - [Microsoft Purview Records Management](#)
 - [Sensitivity Labels](#)
 - [Data Loss Prevention](#)
 - [Office Message Encryption](#)
 - [Information Barriers](#)

Licensing and Purchase

Eligibility

The Advanced Data Residency ("ADR") add-on is intended for Microsoft 365 enterprise customers who have comprehensive data residency requirements. To be eligible to

purchase ADR, customers must meet the following prerequisites:

- The *Tenant Default Geography* must be one of the countries or regions included in the *Local Region Geography*: Australia, Brazil, Canada, France, Germany, India, Israel, Italy, Japan, Mexico, Poland, Qatar, South Korea, Norway, South Africa, Spain, Sweden, Switzerland, United Arab Emirates, and United Kingdom.
- Customers must have licenses for one or more of the following products:
 - Microsoft 365 F1, F3, E3, or E5 (including SKUs without Microsoft Teams)
 - Office 365 F3, E1, E3, or E5 (including SKUs without Microsoft Teams)
 - Exchange Online Plan 1 or Plan 2
 - OneDrive Plan 1 or Plan 2
 - SharePoint Plan 1 or Plan 2
 - Microsoft 365 Business Basic, Standard or Premium (including SKUs without Microsoft Teams)
 - Microsoft Teams Enterprise, EEA, or Essentials

Geographic availability is updated as available.

Customers must cover 100% of paid licenses in the tenant with ADR add-on license for tenant to receive data residency for ADR workloads. See the table for an example.

[Expand table](#)

ADR-related SKU	Available Licenses	Allocated Licenses	ADR Required Licenses
Office 365 E3	200	125	200
Microsoft 365 F1	1420	1100	1420
Exchange Online Plan 2	25	22	25
Totals	1645	1247	1645 ¹

If you have 1,645 licenses purchased for ADR, then you have a data residency commitment for your *Local Region Geography*. If you have fewer than 1,645 licenses, then you do NOT have a data residency commitment, and your tenant is subject to being moved out of the *Local Region Geography*.

Customers who purchase Multi-Geo licenses for their tenant don't have to also pay for ADR for the same licenses. You avoid 'double licensing' a single seat for two different data residency programs. For example, if a customer would normally require 15,000 ADR licenses to satisfy the program requirements, but they also have 4,000 Multi-Geo licenses, then they're only required to purchase 11,000 ADR licenses. The two programs combined would cover the normal ADR program requirement of 100% user coverage.

To find out how many ADR licenses, you need go to the Microsoft 365 admin center under **Billing > Your Products** within your tenant and add up the total Purchased Quantity for all ADR-eligible SKUs to get the proper total of ADR licenses required.

Tenants with a mix of Commercial and Education subscriptions

When a customer has a mix of commercial and education license types including both Commercial/Public Sector (for example, E3, E5) and Education (for example, A1, A3, etc.) licenses in their subscription, the following applies:

- Customers have rights to purchase full ADR add-on for only the paid portion of Microsoft 365 SKUs and aren't obligated to cover free subscription types. However, they must cover the paid education licenses with ADR (Microsoft 365 A3/A5, Office 365 A3/A5 student or faculty).
- ADR for Education products is only available to Volume Licensing / EES (Microsoft Enrollment for Education Solutions) customers; contact your Microsoft account representative for details on how to obtain an ADR Education related SKU.

Data Migration Management

If any customer tenant data covered by the Advanced Data Residency feature is not stored at rest within the customer's eligible *Local Region Geography*, then a data migration is needed to address customer data residency compliance and tenant location requirements fulfilled by ADR.

Starting Data Migration

After receiving the Advanced Data Residency licenses and applying them to the customer's tenant, the customer administrator must select the option to initiate the data migration process for ADR workloads that do not currently reside in their *Local Region Geography*. To initiate data migration for a tenant, the customer administrator should visit the "Data location" section in the Microsoft 365 admin center by navigating to **Settings > Org settings > Organization profile > Data location**. From here, the customer administrator can see the current location of the customer's data-at-rest and what *Local Region Geography* their customer data currently resides in or is eligible to be migrated to upon selection.

Microsoft 365 Admin Center Data Location

Org settings

Services Security & privacy Organization profile

Name	Description
Custom themes	Customize Microsoft 365 for your organization.
Custom tiles for Apps	Add tiles that open websites or SharePoint sites to Apps in the Microsoft 365 app.
Data location	See where Microsoft stores your data for each service you use.
Help desk information	Streamline user support by adding customized contact info to the Microsoft 365 help pane.
Keyboard shortcuts	Perform many common tasks using the keyboard. You can also see the full list of supported shortcuts by pressing [mark].
Organization information	Update your organization's contact info, such as your address, phone number, and technical contact.
Release preferences	Choose how your organization gets new features and service updates from Microsoft 365.
Send email notifications from your domain	Let Microsoft send notification messages from an email address within your organization instead of Microsoft's email address.
Support integration	Integrate your internal support tools with Microsoft 365.

Data location

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

Service	Geography
Copilot for Microsoft 365	European Union
Exchange Online	European Union
Exchange Online Protection	European Union
Microsoft Teams	European Union
OneDrive	European Union
SharePoint	European Union
Viva Connections	European Union
Viva Topics	European Union

Advanced Data Residency

Your tenant has a valid subscription to ADR. You must initiate a request to migrate specific data-at-rest to a Local Regional Geography by selecting the option below.

After you request a migration, no additional action is required while Microsoft moves the data-at-rest for your organization to a new geography. Data transfer and validation occur in the background with minimal impact to users.

By checking the box below, you acknowledge you have read and understand the [Migration Expectations](#), and specific data-at-rest for your organization will be stored at rest only within Italy, notwithstanding any contractual commitment that Microsoft may have made to store data-at-rest only in your current geography.

I want my organization's specific data-at-rest to migrate to and only be stored at rest in Italy.

Save

ⓘ Note

The data migration process described in the sections below will not initiate until the customer administrator completes this task.

The following screenshot is an example of the Microsoft 365 admin center Data location view that an ADR customer can expect to see before opting for migration to their *Local Region Geography*.

Before Migration Opt-in



Data location

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

Service	Geography
Copilot for Microsoft 365	European Union
Exchange Online	European Union
Exchange Online Protection	European Union
Microsoft Teams	European Union
OneDrive	European Union
SharePoint	European Union
Viva Connections	European Union
Viva Topics	European Union

Advanced Data Residency

Your tenant has a valid subscription to ADR. You must initiate a request to migrate specific data-at-rest to a Local Regional Geography by selecting the option below.

After you request a migration, no additional action is required while Microsoft moves the data-at-rest for your organization to a new geography. Data transfer and validation occur in the background with minimal impact to users.

By checking the box below, you acknowledge you have read and understand the [Migration Expectations](#), and specific data-at-rest for your organization will be stored at rest only within Italy, notwithstanding any contractual commitment that Microsoft may have made to store data-at-rest only in your current geography.

- I want my organization's specific data-at-rest to migrate to and only be stored at rest in Italy.

Save

Once a customer administrator chooses the option to initiate migration, they are provided with confirmation of their opt-in date and migration initiation as shown in the screenshot below.

After Migration Opt-in



Data location

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

Service	Geography
Copilot for Microsoft 365	European Union
Exchange Online	European Union
Exchange Online Protection	European Union
Microsoft Teams	European Union
OneDrive	European Union
SharePoint	European Union
Viva Connections	European Union
Viva Topics	European Union

Advanced Data Residency

Your organization requested a migration of eligible data-at-rest to Italy on August 25, 2023.

Migration for all eligible data-at-rest is underway. Microsoft will notify you via the message center in Microsoft 365 admin center as each individual workload migration completes.

[Learn more about expectations during a data migration.](#)

The "Data location" section in the Microsoft 365 admin center (referenced in the screenshots above) displays the most up-to-date location of each workload throughout the data migration process. Customer administrators can also view any Message center notifications related to their migration within the Microsoft 365 admin center by navigating to **Health > Message center**.

Migration Expectations

Microsoft adheres to the [Microsoft Online Services Service Level Agreement \(SLA\)](#) for service availability and uses reasonable efforts to complete an Advanced Data Residency add-on customer data migration within 12 months from the time the customer administrator selects the option to initiate migration. However, large, complex customers, and situations outside of Microsoft's control, may require more time for migration to complete.

Data moves are a back-end service operation with minimal impact to a customer's operations. For information related to specific workloads, customer administrators can

refer to the "Migration" sections in the following Workload Data Residency Capabilities pages: [Exchange Online](#), [SharePoint and OneDrive](#), [Microsoft Teams](#), [Microsoft Copilot for Microsoft 365](#), [Microsoft Defender for Office P1](#), [Office for the Web](#), [Viva Connections](#), [Viva Topics](#), [Microsoft Purview](#), and [Other Services](#).

During and After your Migration

No action is needed from the customer while Microsoft moves each ADR workload and associated customer tenant data to the customer's eligible *Local Region Geography*.

Customer administrators can visit the Message center or "Data location" section within the Microsoft 365 admin center throughout the migration process to review any migration notices and see when each workload service completes migration. From the Microsoft 365 admin center, customer administrators can access the Message center by navigating to **Health > Message center** and the "Data location" section by navigating to **Settings > Org settings > Organization profile > Data location**.

The following screenshots are examples of the Microsoft 365 admin center Data location view that an ADR customer can expect to see during and after their migration.

During Migration

X

Data location

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

Service	Geography
 Copilot for Microsoft 365	Italy
 Exchange Online	Italy
 Exchange Online Protection	Italy
 Microsoft Teams	Italy
 OneDrive	Italy
 SharePoint	European Union
 Viva Connections	European Union
 Viva Topics	European Union

Advanced Data Residency

Your organization requested a migration of eligible data-at-rest to Italy on August 25, 2023.

Migration for all eligible data-at-rest is underway. Microsoft will notify you via the message center in Microsoft 365 admin center as each individual workload migration completes.

[Learn more about expectations during a data migration.](#)

After Migration



Data location

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

Service	Geography
Copilot for Microsoft 365	Italy
Exchange Online	Italy
Exchange Online Protection	Italy
Microsoft Teams	Italy
OneDrive	Italy
SharePoint	Italy
Viva Connections	Italy
Viva Topics	Italy

Advanced Data Residency

Your organization requested a migration of eligible data at-rest to Italy on August 25, 2023. Migration is complete when each entitled Service indicates Geography of Italy. No additional action is required.

Effect on End Users and Workloads

Data moves are a back-end service operation with minimal, if any, effect on end users. Microsoft adheres to the [Microsoft Online Services Service Level Agreement \(SLA\)](#) for service availability and notifies customers of any service maintenance done via Message center in the Microsoft 365 admin center.

Features Affected

Given the complex nature of services included in an E3 or E5 license, the migration of customer data from one data center to another could cause minor disruption or temporary unavailability of certain services. For more information, customer administrators can refer to the "Migration" section of each workload page within [Workload Data Residency Capabilities](#).

Status Notification

Microsoft does not provide a granular status to indicate progress toward migration completion for individual customer scenarios.

Customer administrators can stay informed of migration updates through Message center notifications and by reviewing the "Data location" section within the Microsoft 365 admin center to see when a workload completes migration to their *Local Region Geography*. From the Microsoft 365 admin center, customer administrators can access the Message center by navigating to **Health > Message center** and the "Data location" section by navigating to **Settings > Org settings > Organization profile > Data location**.

For more information on Migration, customer administrators can refer to the following pages:

[Overview and Definitions - Microsoft 365 Enterprise](#)

[Where your Microsoft 365 customer data is stored - Microsoft 365 Enterprise](#)

Related articles

[Legacy Move Program](#)

[New datacenter geos for Microsoft Dynamics CRM Online](#)

[Azure services by region ↗](#)

[Teams experience in a Microsoft 365 Multi-Geo-enabled tenancy](#)

Feedback

Was this page helpful?

 Yes	 No
---	--

[Provide product feedback ↗](#)

Advanced Data Residency Commitments

Article • 03/01/2024

ⓘ Note

If you have purchased a Multi-Geo subscription, then Microsoft will store certain customer data at rest in more than one Geography based on your configuration even if you have purchased the Microsoft 365 Advanced Data Residency add-on ("ADR").

Microsoft makes commitments to store certain customer data at rest in the applicable *Local Region Geography* for [eligible customers](#) that purchase ADR. The commitments are specified as follows.

Exchange Online

The following customer data is stored at rest in the *Local Region Geography*:

- Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments stored in the related *Local Region Geography*).

SharePoint/OneDrive

The following customer data is stored at rest in the *Local Region Geography*:

- SharePoint site content and the files stored within that site and files uploaded to OneDrive

Microsoft Teams

The following customer data is stored at rest in the *Local Region Geography*:

- Microsoft Teams chat messages (including private messages, channel messages, meeting messages and images used in chats), and, for customers using Microsoft Stream (on SharePoint), meeting recordings

Microsoft Copilot for Microsoft 365

The following customer data is stored at rest in the *Local Region Geography*:

- Any stored content of interactions with Microsoft Copilot for Microsoft 365 to the extent not included in the preceding commitments.

Microsoft Defender for Office P1

The following customer data is stored at rest in the *Local Region Geography*:

- MDO P1 doesn't store any customer data within its service.
- Exchange Online Protection (EOP). The following customer data is stored at rest in the *Local Region Geography*: Service configuration data and policies, quarantined email and attachments, junk email, grading analysis, blocklists (url, tenant, user), spam domains, reports, and alerts

Office for the Web

The following customer data is stored at rest in the *Local Region Geography*:

- Office for the Web stores files on a storage host that has its applicable promises to *Local Region Geography*.

Viva Connections

The following customer data is stored in the *Local Region Geography*:

- Viva Connections Dashboard and Feed can have content sourced from SharePoint, Exchange Online and Microsoft Teams. All customer data sourced from these services covered by data residency commitments will be stored in the *Local Region Geography*. Refer to [Exchange Online](#), [SharePoint](#), and [Microsoft Teams](#) workload data residency pages for more details.

Viva Topics

The following customer data is stored at rest in the *Local Region Geography*:

- All the topics and customer data snippets discovered are stored within the relevant *Geographies* in Exchange Online Substrate (site or arbitration mailboxes, and Substrate). All topic customer data is partitioned based on which *Local Region Geography* the data came from within your tenant.
- Machine Learning ("ML") models are trained on public web data, and as such don't contain any customer data from your tenant. In the future, it's possible we'll use customer data to improve accuracy of the ML models, in which case the data

handling of ML models will follow the same policies as any other customer content (including data residency, retention, access control, sensitivity).

- Topic highlighting is computed dynamically when the SharePoint page is rendered by running a language model against the content of the page and linking it with the knowledge base of Topics. The Topics data is sourced from the Substrate in the *Local Region Geography*.
- The administration configuration data is stored within the *Local Region Geography*.

Purview Audit (Standard)

The following customer data is stored at rest in the *Local Region Geography*:

- Service configuration data, audited Activities, audit Records, and audit log query permissions

Purview Audit (Premium)

The following customer data is stored at rest in the *Local Region Geography*:

- In addition to the customer data stored as part of Purview Audit (Standard), configuration and Customer Data related to high-value crucial events

Data lifecycle management - Data Retention

The following customer data is stored at rest in the *Local Region Geography*:

- Retention policy settings and retention label definitions
- Customer Data stored in original locations for the following services:
 - Exchange email
 - SharePoint site
 - OneDrive accounts
 - Microsoft 365 Groups
 - Exchange public folders
 - Microsoft Teams chats and channel messages
- Customer Data copied and stored in Exchange Online hidden mailboxes
 - Teams channel messages
 - Teams chats
 - Teams private channel messages
 - SharePoint, OneDrive, Exchange Online and Microsoft Teams follow the data residency commitments for those services. Refer to [Exchange Online](#),

[SharePoint](#), and [Microsoft Teams](#) workload data residency pages for more details.

- Training classifiers
- Disposition data
- Mappings between retention labels and Data Loss Prevention (DLP) policies

Data lifecycle management - Records Management

The following customer data is stored at rest in the *Local Region Geography*:

- Record retention label definitions, file plan definitions, event-based retention policy settings, disposition review records and records of deletion

Information Protection - Sensitivity labels

The following customer data is stored at rest in the *Local Region Geography*:

- Label configuration
- Labels definition
- Label policies
- Custom help page
- Activity Explorer and Microsoft 365 unified audit logs
- Label change justification records

Information Protection - Data Loss Prevention (DLP)

The following customer data is stored at rest in the *Local Region Geography*:

- DLP admin configuration, DLP policies in Compliance Portal, DLP monitored activities, violation history, Activity Explorer and Microsoft 365 unified audit logs, quarantine storage, DLP Alerts and DLP Alert management dashboard

Information Protection - Office Message Encryption

The following customer data is stored at rest in the *Local Region Geography*:

- Encryption policies, admin settings and encrypted messages

Risk and compliance - information barriers

The following customer data is stored at rest in the *Local Region Geography*:

- Policy settings, risk indicators and admin settings
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Microsoft 365 Multi-Geo

Article • 05/08/2024

The Microsoft 365 Multi-Geo Capabilities add-on provides Enterprise Agreement customers with the ability to expand their Microsoft 365 presence to multiple geographic regions within a single existing Microsoft 365 *Tenant*. Multi-Geo enables customers to manage data-at-rest locations at a granular level for their users, SharePoint sites, Microsoft 365 Groups, and Microsoft Teams teams level. Multi-Geo is targeted to customers who have a need to store data in multiple geographies to satisfy their data residency requirements.

Starting June 1, 2023, CSP partners can purchase Multi-Geo Capabilities for their customers who are using Microsoft 365, Office 365, Exchange, OneDrive and SharePoint subscriptions. With Microsoft 365 Multi-Geo, CSP partners will be able to ensure their customers meet their data residency requirements.

Microsoft 365 Multi-Geo is designed to meet your data residency requirements while retaining single-tenant administration and full-fidelity collaboration experiences between users as necessary.

If a customer requires performance optimization functionalities for Microsoft 365, see [Network planning and performance tuning for Microsoft 365](#) or contact your support group.

Note

Exchange Online, SharePoint, OneDrive, and Microsoft Teams are available for Multi-Geo configuration. For more information about data residency commitments, see [Exchange Online](#), [SharePoint and OneDrive](#), and [Microsoft Teams](#) for more details.

For a video introduction to Microsoft 365 Multi-Geo, see [SharePoint and OneDrive Multi-Geo to control where your data resides](#).

Multi-Geo architecture

In a Multi-Geo environment, your Microsoft 365 *Tenant* consists of a central location (where your Microsoft 365 subscription was originally provisioned) and one or more satellite locations. In a Multi-Geo enabled *Tenant*, the information about geo locations, groups, and user information, is mastered in Microsoft Entra ID. Because your *Tenant*

information is mastered centrally and synchronized into each geo location, sharing and experiences involving anyone from your company contain global awareness.

Licensing

Microsoft 365 Multi-Geo is available as an add-on to the following Microsoft 365 subscription plans.

Enterprise Agreement customers must purchase a quantity of Multi-Geo licenses equal to or greater than 5% of their total eligible users. Similarly, CSP partners must purchase and assign a quantity of Multi-Geo licenses equal to or greater than 5% of their customers' total eligible Microsoft 365 users. For Enterprise customers, user subscription licenses must be on the same Enterprise Agreement as the Multi-Geo Services licenses. Contact your Microsoft account team for details.

- Microsoft 365 F1, F3, E3, or E5
- Office 365 F3, E1, E3, or E5
- Standalone Exchange Online Plan 1 or Plan 2
- Standalone OneDrive Plan 1 or Plan 2
- Standalone SharePoint Plan 1 or Plan 2

Note that Small Business products do not currently qualify for Multi-Geo, even if they contain elements of the above list.

Note that *Multi-Geo Capabilities in Microsoft 365* is a user-level add-on license. You need a license for each user that you want to host in a *Satellite Geography* location. You can add more licenses over time as you add users in *Satellite Geography* locations.

There are no Multi-Geo licenses specific to shared resources such as SharePoint Sites, Microsoft 365 Groups, or Microsoft Teams teams. If enough Multi-Geo user licenses have been acquired, then customers are eligible to use Multi-Geo with shared resources without limitation.

Microsoft 365 Multi-Geo availability

Microsoft 365 Multi-Geo is currently offered in these regions:

 Expand table

Microsoft 365 Region	PreferredDataLocation (PDL) Value
Macro Region Geography 2 - Asia-Pacific	APC

Microsoft 365 Region	PreferredDataLocation (PDL) Value
Australia	AUS
Brazil	BRA
Canada	CAN
Macro Region Geography 1 - EMEA	EUR
France	FRA
Germany	DEU
India	IND
Israel	ISR
Italy	ITA
Japan	JPN
Korea	KOR
Norway	NOR
Poland	POL
Qatar	QAT
South Africa	ZAF
Sweden	SWE
Switzerland	CHE
United Arab Emirates	ARE
United Kingdom	GBR
United States	NAM

To learn more about the definition of each region such as what countries or cities contain the datacenters, see [Overview and Definitions](#).

If you utilize Microsoft Purview eDiscovery Standard or Premium, see [Microsoft 365 Multi-Geo eDiscovery configuration](#) and [Set up compliance boundaries for eDiscovery investigations](#) for additional information on region usage and data storage as it relates to Microsoft Purview eDiscovery.

Getting started

Whether you're a CSP partner managing your customer's Microsoft 365 subscriptions or an Enterprise Agreement customer managing your own subscriptions, you can follow these steps to get started with Multi-Geo:

1. Ensure that you purchase Multi-Geo for at least 5% of the total eligible users in your Microsoft 365 subscription. Remember that you'll need a license for each user you want to host in a *Satellite Geography* location.
2. Before you can start using Microsoft 365 Multi-Geo, Microsoft needs to configure your *Tenant* for Multi-Geo support. This one-time automatic configuration process is triggered after you order the *Multi-Geo Capabilities in Microsoft 365* and the licenses show up in your *Tenant*. You'll receive workload-specific notifications in the [Microsoft 365 message center](#) once the *Tenant* has completed the configuration process for each workload, and then you may begin configuring and using your Microsoft 365 Multi-Geo capabilities. The time required to configure a *Tenant* for Multi-Geo support varies from *Tenant* to *Tenant*, but most *Tenants* finish within a month after receipt of the feature licenses. Larger or more complex *Tenants* may require more time to complete the configuration process.
3. Read [Plan your multi-geo environment](#).
4. Learn about [administering a multi-geo environment](#) and [how your users will experience the environment](#).
5. When you're ready to set up Microsoft 365 Multi-Geo, [configure your tenant for multi-geo](#).
6. [Set up search](#).

 **Note**

For more information on the Microsoft 365 services that support Multi-Geo, see the [EXO](#), [ODSP](#) and [Teams](#) workload data residency pages for more details.

See also

[Multi-Geo in Exchange Online and OneDrive](#)

[Multi-Geo Capabilities in OneDrive and SharePoint](#)

[Multi-Geo Capabilities in Exchange Online](#)

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Plan for Microsoft 365 Multi-Geo

Article • 12/11/2023

This guidance is for administrators of *Tenants* preparing their Microsoft 365 *Tenant* to meet their data residency requirements.

In a Multi-Geo configuration, your Microsoft 365 *Tenant* consists of a *Primary Provisioned Geography* location and multiple *Satellite Geography* locations. You retain a single *Tenant* that spans across multiple *Geography* locations retaining single-tenant administration and full-fidelity collaboration experiences across *Geographies*.

To help you understand the basic concepts of the Multi-Geo configuration, review terms in the Definitions section of the [Overview and Definitions page](#).

Enabling Multi-Geo requires four key steps:

1. Purchase the *Multi-Geo Capabilities in Microsoft 365* add-on SKU for your Microsoft 365 subscription.
2. Configure any workloads that require customer specific settings for Multi-Geo.
3. Set your users' Preferred Data Location (PDL) to the desired *Satellite Geography* location. A new user's OneDrive site, Exchange Online mailbox, and Teams chat store is provisioned in the *Geography* defined by their PDL value if the value is configured prior to assigning them a Microsoft 365 license. When an existing user's PDL value is set to a new value, then their existing Exchange Online mailbox and Teams chat store will automatically be migrated to the new geography.
4. Migrate your users' existing OneDrive sites from the *Primary Provisioned Geography* location to their *Satellite Geography* data location as needed. OneDrive sites don't migrate automatically like Exchange Online mailboxes or Teams chat stores.

See [Configure Microsoft 365 Multi-Geo](#) for details on each of these steps.

See the [Availability section](#) of the Microsoft 365 Multi-Geo Overview page for the *Geographies* that can be a *Satellite Geography*.

Best practices

We recommend that you create a test user in Microsoft 365 to do some initial testing. We'll walk through some testing and verification steps with this user before you proceed to onboard production users into Microsoft 365 Multi-Geo.

Once you've completed testing with the test user, select a pilot group – perhaps from your IT department – to be the first to use the Multi-Geo supporting workloads in *Satellite Geographies*.

Each user should have a *preferred data location* (PDL) set so that Microsoft 365 can determine in which *Geography* location to provision or relocate their data to. The user's preferred data location must match one of the available *Geographies*. While the PDL field isn't mandatory, we do recommend that a PDL value is set for all users. Users without a PDL value set will be provisioned in the *Primary Provisioned Geography*. If the PDL value isn't a valid value, then a user's data will be provisioned in the *Primary Provisioned Geography*.

Create a list of your users and include their user principal name (UPN) and the Preferred Data Location code. Include your test user and your initial pilot group to start with. You'll need this list for the configuration procedures.

If your users are synchronized from an on-premises Active Directory system to Microsoft Entra ID, then you must set the preferred data location as an Active Directory attribute and synchronize it by using Microsoft Entra Connect. You can't directly configure the preferred data location for synchronized users using [Microsoft Graph PowerShell](#). The steps to set up PDL in Active Directory and Synchronize it are covered in [Microsoft Entra Connect Sync: Configure preferred data location for Microsoft 365 resources](#).

The administration of a Multi-Geo *Tenant* can differ from a non-multi-geo *Tenant* in some scenarios. For example, many SharePoint and OneDrive settings and services are multi-geo aware. We recommend that you review [Administering a multi-geo environment](#) before you proceed with your configuration.

Read [User experience in a multi-geo environment](#) for details about your end users' experience in a Multi-Geo environment.

To get started configuring Microsoft 365 Multi-Geo, see [Configure Microsoft 365 Multi-Geo](#).

Once you've completed the configuration, remember to [migrate your users' OneDrive libraries](#) as needed to get your users working from their preferred data locations.

Related topics

[Microsoft 365 Multi-Geo eDiscovery configuration](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Service behavior a Multi-Geo enabled environment

Article • 08/01/2024

Here's a look at how Microsoft 365 services work in a Multi-Geo environment.

Administrator experience

The SharePoint admin center has a [Geo locations tab](#) in the left navigation that features a geo locations map where you can view and manage your geo locations. Use this page to add or delete geo locations for your *Tenant*.

Audit log search

A unified [Audit log](#) for all your *Satellite Geography* locations is available from the Microsoft 365 audit log search page. You can see all the audit log entries from across geo locations, for example, NAM & EUR users' activities will show up in one org view and then you can apply existing filters to see specific user's activities.

BCS, Secure Store, Apps

BCS, Secure Store, and Apps all have separate instances in each satellite location, and therefore the SharePoint administrator should manage and configure these services separately from each satellite location.

Compliance admin center

There's one central Microsoft Purview compliance portal for a Multi-Geo *Tenant*: [Microsoft Purview admin center](#).

eDiscovery

By default, an eDiscovery Manager or Administrator of a Multi-Geo *Tenant* will be able to conduct eDiscovery tasks only in the *Primary Provisioned Geography* of that *Tenant*. A member of the **Organization Management** role group or a user with the **Role Management** role must assign eDiscovery Manager permissions in the Microsoft Purview portal to allow others to perform eDiscovery tasks and assign a "Region"

parameter in their applicable Compliance Security Filter to specify the *Geography* for conducting eDiscovery as *Satellite Geography* location. Otherwise, no eDiscovery activities will be carried out for the *Satellite Geography* location. Only one "Region" security filter per user is supported.

See [Assign eDiscovery permissions in the compliance portal](#) for more information. To configure the Compliance Security Filter for a Region, see [Configure Office 365 Multi-Geo eDiscovery](#).

Exchange Online mailboxes

Users' Exchange Online mailboxes are moved automatically if their PDL is changed. When a new mailbox is created, it's provisioned to the user's PDL or to the central location if no value has been set for the user's PDL.

Information Protection (IP) Data Loss Prevention (DLP) policy

You can set your IP DLP policies for OneDrive, SharePoint, and Exchange Online in the Security and Compliance center, scoping policies as needed to the whole *Tenant* or to applicable users. For example: If you wish to select a policy for a user in a satellite location, select to apply the policy to a specific OneDrive and enter the user's OneDrive URL. See [Overview of data loss prevention policies](#) for general guidance in creating DLP policies.

The DLP policies are automatically synchronized based on their applicability to each geo location.

Implementing Information Protection and Microsoft Purview Data Loss Prevention policies to all users in a geo location isn't an option available in the UI, instead you must select the applicable accounts for the policy or apply the policy globally to all accounts.

Microsoft Power Apps

Power Apps created for the satellite location will use the end point located in the central location for the *Tenant*. Microsoft Power Apps isn't a Multi-Geo service.

Microsoft Power Automate

Flows created for the satellite location will use the end point located in the default geo location for the *Tenant*. Microsoft Power Automate isn't a Multi-Geo service.

SharePoint storage quota

By default, all geo locations of a multi-geo environment share the available *Tenant* storage quota. You can also manage the storage quota by allocating a specific quota for a particular geo location. For more information, see [SharePoint storage quotas in multi-geo environments](#).

Sharing

Administrators can set and manage sharing policies for each of their locations. The OneDrive and SharePoint sites in each geo location will honor only the corresponding geo-specific sharing settings. (For example, you can allow [external sharing](#) for your central location, but not for your satellite location or vice versa.) Note that the sharing settings don't allow configuring sharing limitations between geo locations.

Microsoft Stream

Videos uploaded to Microsoft Stream in a 1:1 chat are stored in the OneDrive of the person uploading. Meeting recordings are stored in the OneDrive of each attendee who records the meeting.

Taxonomy

We support a unified [taxonomy](#) for enterprise-managed metadata across geo locations, with the master being hosted in the central location for your company. We recommend that you manage your global taxonomy from the central location and only add location-specific terms to the satellite location's Taxonomy. Global taxonomy terms will synchronize to the satellite locations.

See [Manage metadata in a Multi-Geo tenant](#) for more details and for developer guidance.

User Profile Application

There's a [user profile application](#) in each geo location. Each user's profile information is hosted in their geo location and available to the administrator for that geo location.

If you have custom profile properties, then we recommend that you use the same profile schema across geographies and populate your custom profile properties either in all geo locations or where needed. For guidance regarding how to populate user profile data programmatically, please refer to the [Bulk User Profile Update API](#).

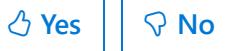
See [Work with user profiles in a Multi-Geo tenant](#) for additional details and for developer guidance.

Viva Engage

Viva Engage isn't a Multi-Geo workload. Viva Engage threads stored in Viva Engage will be placed in the *Tenant's* central location. Viva Engage is rolling out a file storage change which will store Viva Engage files within SharePoint. Viva Engage files stored in SharePoint will be placed the SharePoint site associated with the Viva Engage group. SharePoint group sites are based on PDL logic as outlined in [SharePoint Sites and Groups](#).

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

User experience in a Multi-Geo environment

Article • 12/11/2023

Here's what your users see in a OneDrive Multi-Geo configuration:

Exchange Online mailbox

A user's Exchange Online mailbox is provisioned to their preferred data location, and is automatically relocated if their PDL changes. Users can use Outlook and Outlook on the web normally with no change in user experience in a Multi-Geo environment.

Hub sites

SharePoint Hub sites enhance the discovery and engagement with content for employees, while creating a complete and consistent representation of projects, departments or regions. In a Multi-Geo environment, sites from satellite locations can easily be associated with a hub site regardless the hub site's *Geography* location. Users can search and get results across the hub through a single search experience, regardless of the geo location of the sites.

Microsoft 365 app launcher

The app launcher is multi-geo aware and will direct each tile to the appropriate geo location of the workload. The SharePoint and OneDrive tiles point the user to the location corresponding to the user's provisioned geo location. This means that if the user has a OneDrive in the central location, their SharePoint tile points them to SP Home in the central location but their group site will be provisioned in the location corresponding to their PDL.

Office applications

Office applications such as Microsoft Word, Excel, and PowerPoint will automatically detect the correct OneDrive geo-location for each user when they sign in. Users don't need to enter the geo-specific URL for their OneDrive or SharePoint sites.

OneDrive sync app

The OneDrive sync app (version 17.3.6943.0625 and later) will automatically detect the correct OneDrive *Geography* location for the user. Sync app support includes the ability to sync groups-based sites regardless of their *Geography* location. The Groove sync client isn't supported for Multi-Geo.

OneDrive location

Users have their OneDrive provisioned in their preferred data location. If a user navigates to a OneDrive URL that contains an incorrect *Geography* location (such as a bookmark from a previous geo location), they're automatically redirected to the OneDrive in the appropriate geo location.

OneDrive iOS and Android

The OneDrive iOS and Android mobile apps show you your OneDrive files and files shared with you regardless of their *Geography* location. Search from the OneDrive mobile apps show relevant results from all *Geography* locations. Download the latest version of these apps.

For more information, see [Use OneDrive on iOS](#) and [Use OneDrive for Android](#) for more information.

OneDrive mobile client

The OneDrive mobile client is Multi-Geo aware and will display pertinent content and results from all *Geography* locations.

Search

Each *Geography* location has its own search index and Search Center. When a user searches, the query is sent to all the *Geography* locations, and the returned results are merged and then ranked so the user gets unified results. Users get results from all *Geography* locations regardless of their own *Geography* location. See [Configure Search for OneDrive Multi-Geo](#) for specifics.

The following search clients are supported:

- OneDrive
- Office Delve

- SharePoint Home
- The Search Center
- Custom search applications that use the SharePoint Search API

SharePoint Home

In SharePoint Multi-Geo, your SharePoint home is hosted in the location where the user resides as determined by their OneDrive location. For example: if the user has their OneDrive hosted in a European satellite location, their SharePoint Home is rendered from Europe. SharePoint home includes all content relevant to the user regardless of its *Geography* location.

Followed Sites, News from Sites, Recent Sites, Frequent Sites, and Suggested sites

All of these components show up for the user regardless of the *Geography* location where the content is hosted, so long as the user has permissions to said content.

Features Links

Admins may configure Featured links in SharePoint home as appropriate to each *Geography* location. This allows the admin to feature in the SP Home for each region the links that are appropriate for users in the region.

SharePoint mobile client

The SharePoint mobile client is multi-geo aware and will display pertinent content and results from all geo locations.

Sharing

The people picker experience shows all users regardless of their *Geography* location. This allows a user to share with another user in their same geo or in any other of your *Tenant's Geography* locations. Content from different *Geography* locations show up in the **Shared with Me** view in the user's OneDrive, Word, Excel, PowerPoint, and Office.com and can be accessed with single sign-On experience regardless of which *Geography* location it's hosted in.

Microsoft Teams experience

Microsoft Teams is a Multi-Geo service. OneDrive files and recently viewed files are shown regardless of the user's *Geography* location. @ mentions work with users from all *Geography* locations.

User profiles

User profile information is mastered in the user's *Geography* location. When selecting a user, you'll be directed to the appropriate *Geography* location for the user, where you'll see their full profile details.

If Office Delve is turned off, you'll see the classic profile experience in SharePoint, which isn't Multi-Geo aware.

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Microsoft 365 Multi-Geo *Tenant* configuration

Article • 12/11/2023

Before you configure your *Tenant* for Microsoft 365 Multi-Geo, be sure you have read [Plan for Microsoft 365 Multi-Geo](#).

To follow the steps in this article, you need a list of the *Geography* locations that you want to enable as *Satellite Geography* locations, and the test users that you want to provision for those locations.

Not all Multi-Geo workloads require customer driven configuration.

Configuring Exchange Online for Multi-Geo

There is no customer driven configuration required to prepare Exchange Online in a Multi-Geo enabled *Tenant*. A customer may use all Geographies with Exchange Online as soon as Multi-Geo has been enabled within Exchange Online for their *Tenant*.

Configuring Microsoft Teams for Multi-Geo

There's no customer driven configuration required to prepare Microsoft Teams in a Multi-Geo enabled tenant. A customer may use all Geographies with Microsoft Teams as soon as Multi-Geo has been enabled within Microsoft Teams for their *Tenant*.

Configuring SharePoint and OneDrive for Multi-Geo

If you want to store data in a particular Geography, then that Geography must be configured for SharePoint and OneDrive ahead of time.

Once Multi-Geo has been enabled for your *Tenant* in SharePoint and OneDrive, the **Geo Locations** tab becomes available in the SharePoint admin center. If you don't see the **Geo Locations** tab, then your *Tenant* hasn't yet finished being enabled for Multi-Geo.

To add each Satellite Geography location for SharePoint and OneDrive where you want to store data:

1. Open the SharePoint admin center. and go to **Geo locations**.

2. Select **Add location**.
3. Select the location that you want to add, and then select **Next**.
4. Type the domain that you want to use with the geo location, and then select **Add**.
5. Select **Close**.

Provisioning may take from a few hours up to 72 hours, depending on the size of your *Tenant*. Once provisioning of a *Satellite Geography* location has completed, you'll receive an email confirmation. When the new *Geography* location appears in blue on the map on the Geo locations tab in the OneDrive and SharePoint admin center, then you can proceed to set users' preferred data location to that *Geography* location.

 **Important**

Your new *Satellite Geography* location will be set up with default settings. This will allow you to configure that *Satellite Geography* location as appropriate for your local compliance needs.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Microsoft Entra Connect Sync: Configure preferred data location for Microsoft 365 resources

Article • 11/06/2023

The purpose of this topic is to walk you through how to configure the attribute for preferred data location in Microsoft Entra Connect Sync. When someone uses Multi-Geo capabilities in Microsoft 365, you use this attribute to designate the geo-location of the user's Microsoft 365 data. (The terms *region* and *geo* are used interchangeably.)

Supported Multi-Geo locations

For a list of all geos supported by Microsoft Entra Connect see [Microsoft 365 Multi-Geo availability](#)

Enable synchronization of preferred data location

By default, Microsoft 365 resources for your users are located in the same geo as your Microsoft Entra tenant. For example, if the *Tenant* is located in North America, then the users' Exchange mailboxes are also located in North America. For a multinational organization, this might not be optimal.

By setting the attribute **preferredDataLocation**, you can define a user's geo. You can have the user's Microsoft 365 resources, such as the mailbox and OneDrive, in the same geo as the user, and still have one tenant for your entire organization.

Important

As of June 1, 2023, Multi-Geo is available for CSP partners to purchase, at a minimum of 5% of their customer's total Microsoft 365 subscription seats.

Multi-Geo is also available to customers with an active Enterprise Agreement. Please talk to your Microsoft representative for details.

For a list of all geos supported by Microsoft Entra Connect see [Microsoft 365 Multi-Geo availability](#).

Microsoft Entra Connect support for synchronization

Microsoft Entra Connect supports synchronization of the **preferredDataLocation** attribute for **User** objects in version 1.1.524.0 and later. Specifically:

- The schema of the object type **User** in the Microsoft Entra Connector is extended to include the **preferredDataLocation** attribute. The attribute is of the type, single-valued string.
- The schema of the object type **Person** in the metaverse is extended to include the **preferredDataLocation** attribute. The attribute is of the type, single-valued string.

By default, **preferredDataLocation** is not enabled for synchronization. This feature is intended for larger organizations. The Active Directory schema in Windows Server 2019 has an attribute **msDS-preferredDataLocation** you should use for this purpose. If you have not updated the Active Directory schema and cannot do so, then you must identify an attribute to hold the Microsoft 365 geo for your users. This is going to be different for each organization.

Important

Microsoft Entra ID allows the **preferredDataLocation** attribute on **cloud User objects** to be directly configured by using [Microsoft Graph PowerShell](#). To configure this attribute on **synchronized User objects**, you must use Microsoft Entra Connect.

Before enabling synchronization:

- If you have not upgraded the Active Directory schema to 2019, then decide which on-premises Active Directory attribute to be used as the source attribute. It should be of the type, **single-valued string**.
- If you have previously configured the **preferredDataLocation** attribute on existing **synchronized User objects** in Microsoft Entra ID by using Microsoft Graph PowerShell, you must backport the attribute values to the corresponding **User** objects in on-premises Active Directory.

Important

If you do not backport these values, Microsoft Entra Connect removes the existing attribute values in Microsoft Entra ID when synchronization for the **preferredDataLocation** attribute is enabled.

- Configure the source attribute on at least a couple of on-premises Active Directory User objects now. You can use this for verification later.

The following sections provide the steps to enable synchronization of the **preferredDataLocation** attribute.

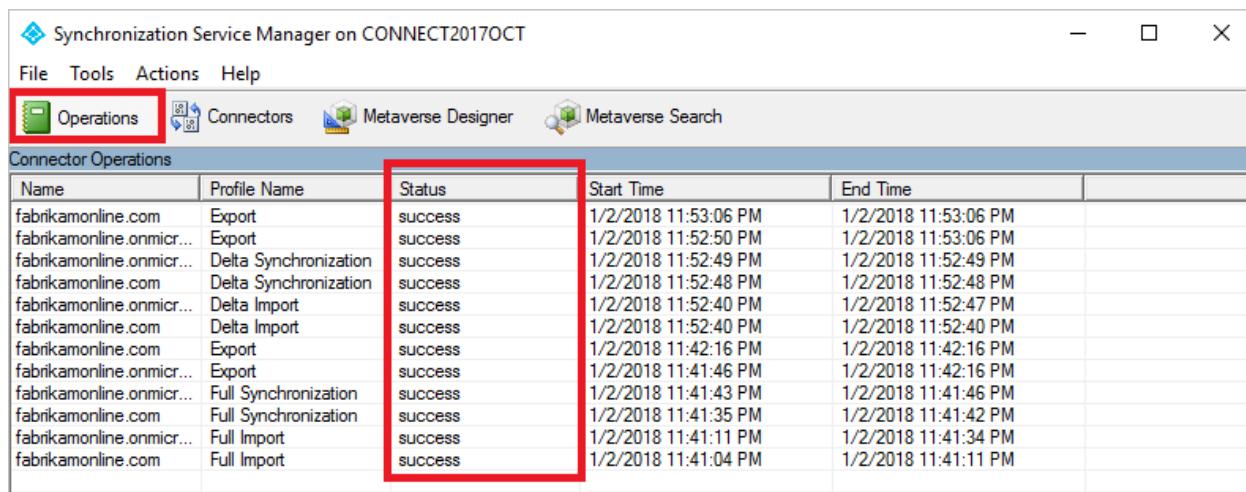
Note

The steps are described in the context of a Microsoft Entra deployment with single-forest topology, and without custom synchronization rules. If you have a multi-forest topology, custom synchronization rules configured, or have a staging server, you should adjust the steps accordingly.

Step 1: Disable sync scheduler and verify there is no synchronization in progress

To avoid unintended changes being exported to Microsoft Entra ID, ensure that no synchronization takes place while you are in the middle of updating synchronization rules. To disable the built-in sync scheduler:

- Start a PowerShell session on the Microsoft Entra Connect server.
- Disable scheduled synchronization by running this cmdlet: `Set-ADSyncScheduler -SyncCycleEnabled $false`.
- Start the **Synchronization Service Manager** by going to **START > Synchronization Service**.
- Select the **Operations** tab, and confirm there is no operation with the status *in progress*.



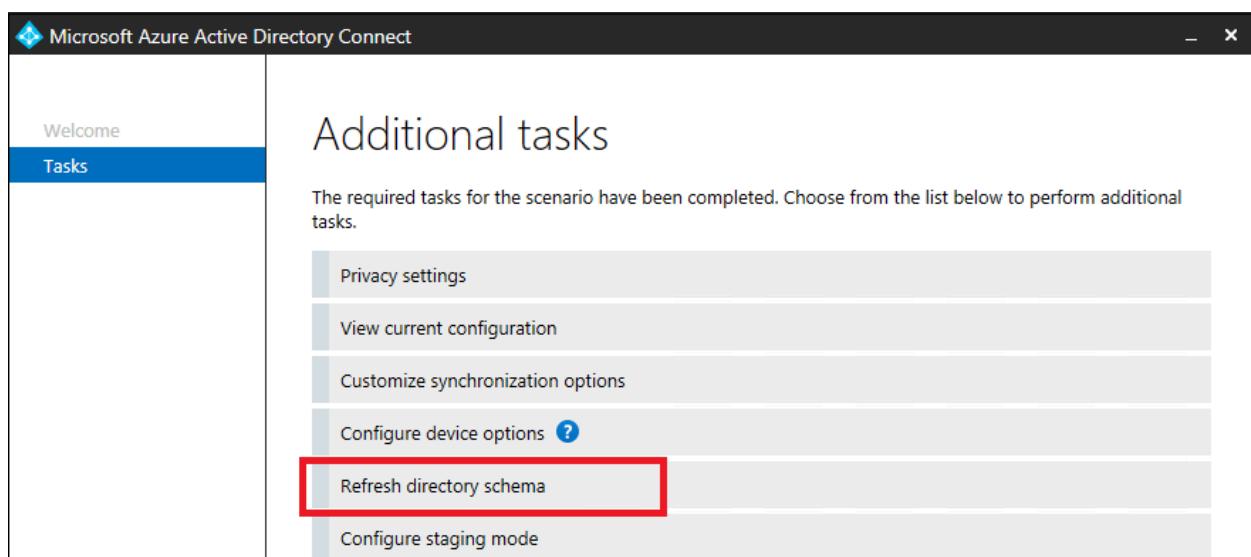
The screenshot shows the Microsoft Synchronization Service Manager interface. The title bar reads "Synchronization Service Manager on CONNECT2017OCT". The menu bar includes File, Tools, Actions, and Help. Below the menu is a toolbar with icons for Operations (highlighted with a red box), Connectors, Metaverse Designer, and Metaverse Search. The main window has a header "Connector Operations". A table below lists synchronization tasks with columns: Name, Profile Name, Status, Start Time, and End Time. All listed tasks show a "success" status and occurred between 1/2/2018 11:41:04 PM and 1/2/2018 11:53:06 PM.

Name	Profile Name	Status	Start Time	End Time
fabrikamonline.com	Export	success	1/2/2018 11:53:06 PM	1/2/2018 11:53:06 PM
fabrikamonline.onmicrosoft.com	Export	success	1/2/2018 11:52:50 PM	1/2/2018 11:53:06 PM
fabrikamonline.onmicrosoft.com	Delta Synchronization	success	1/2/2018 11:52:49 PM	1/2/2018 11:52:49 PM
fabrikamonline.com	Delta Synchronization	success	1/2/2018 11:52:48 PM	1/2/2018 11:52:48 PM
fabrikamonline.onmicrosoft.com	Delta Import	success	1/2/2018 11:52:40 PM	1/2/2018 11:52:47 PM
fabrikamonline.com	Delta Import	success	1/2/2018 11:52:40 PM	1/2/2018 11:52:40 PM
fabrikamonline.com	Export	success	1/2/2018 11:42:16 PM	1/2/2018 11:42:16 PM
fabrikamonline.onmicrosoft.com	Export	success	1/2/2018 11:41:46 PM	1/2/2018 11:42:16 PM
fabrikamonline.onmicrosoft.com	Full Synchronization	success	1/2/2018 11:41:43 PM	1/2/2018 11:41:46 PM
fabrikamonline.com	Full Synchronization	success	1/2/2018 11:41:35 PM	1/2/2018 11:41:42 PM
fabrikamonline.onmicrosoft.com	Full Import	success	1/2/2018 11:41:11 PM	1/2/2018 11:41:34 PM
fabrikamonline.com	Full Import	success	1/2/2018 11:41:04 PM	1/2/2018 11:41:11 PM

Step 2: Refresh the schema for Active Directory

If you have updated the Active Directory schema to 2019 and Connect was installed before the schema extension, then the Connect schema cache does not have the updated schema. You must then refresh the schema from the wizard for it to appear in the UI.

1. Start the Microsoft Entra Connect wizard from the desktop.
2. Select the option **Refresh directory schema** and click **Next**.
3. Enter your Microsoft Entra credentials and click **Next**.
4. On the **Refresh Directory Schema** page, make sure all forests are selected and click **Next**.
5. When completed, close the wizard.



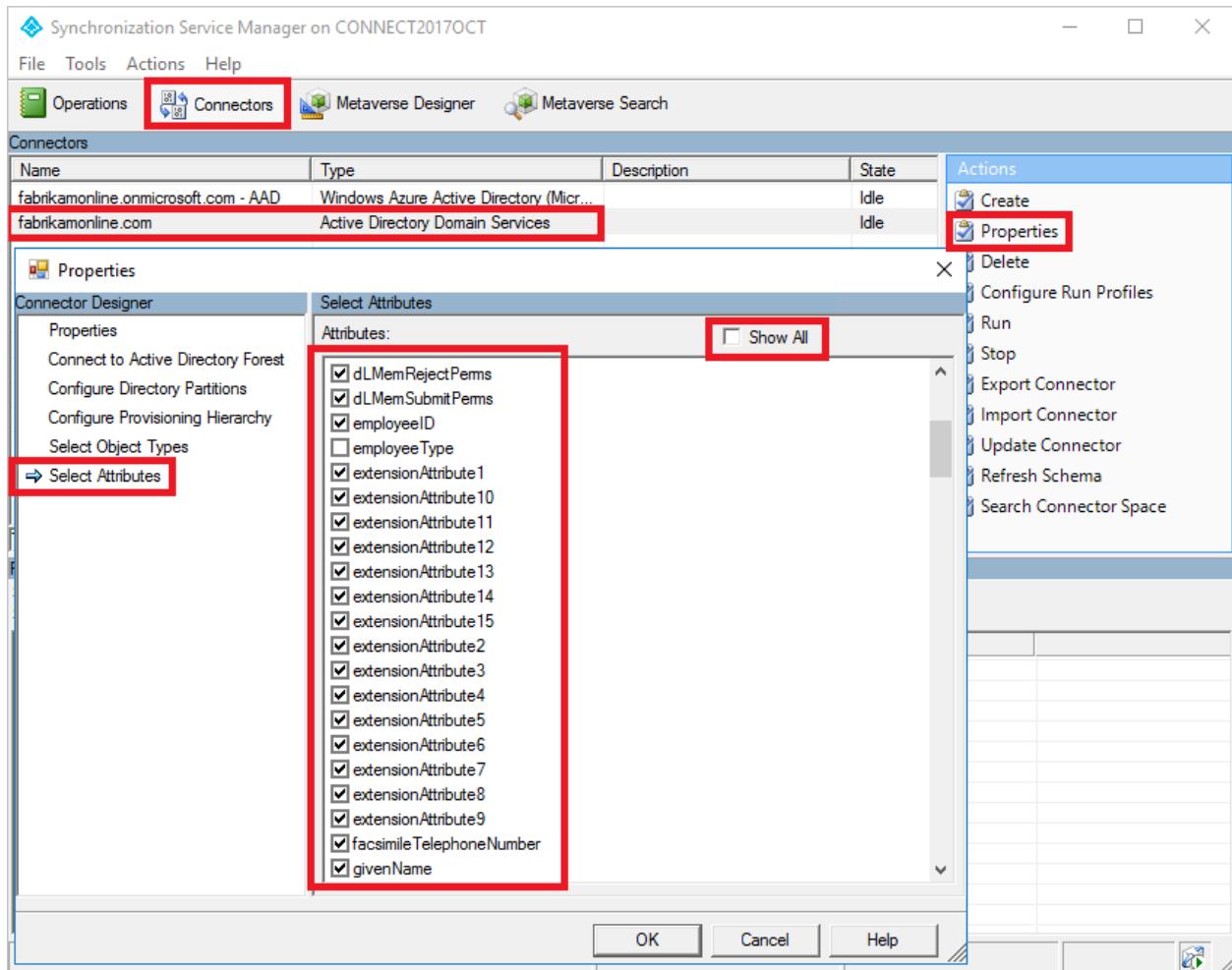
Step 3: Add the source attribute to the on-premises Active Directory Connector schema

This step is only needed if you run Connect version 1.3.21 or older. If you are on 1.4.18 or newer, then skip to step 5.

Not all Microsoft Entra attributes are imported into the on-premises Active Directory connector space. If you have selected to use an attribute that is not synchronized by default, then you need to import it. To add the source attribute to the list of the imported attributes:

1. Select the **Connectors** tab in the Synchronization Service Manager.
2. Right-click the on-premises Active Directory Connector, and select **Properties**.
3. In the pop-up dialog box, go to the **Select Attributes** tab.
4. Make sure the source attribute you selected to use is checked in the attribute list. If you do not see your attribute, select the **Show All** check box.

5. To save, select OK.

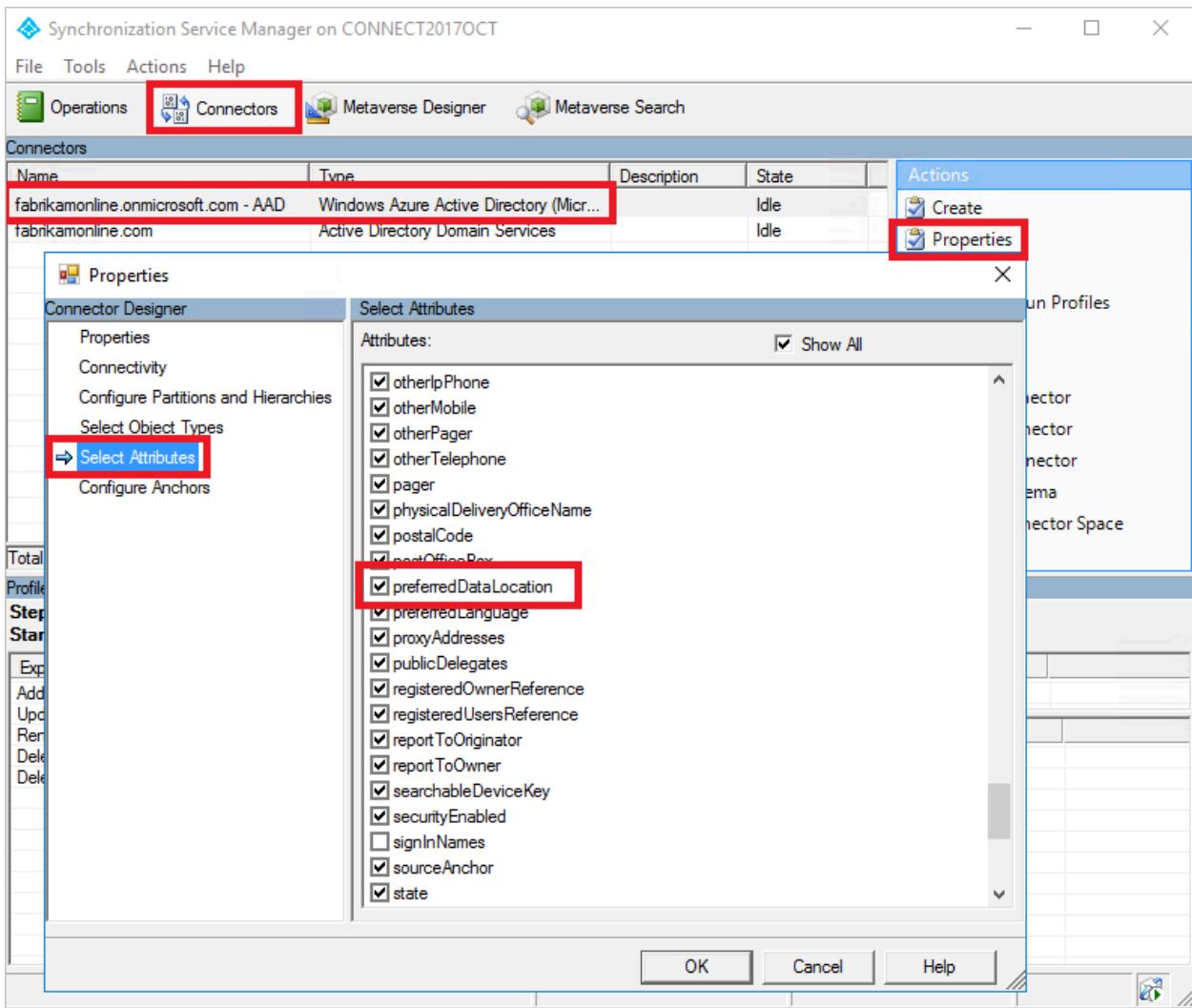


Step 4: Add **preferredDataLocation** to the Microsoft Entra Connector schema

This step is only needed if you run Connect version 1.3.21 or older. If you are on 1.4.18 or newer, then skip to step 5.

By default, the **preferredDataLocation** attribute is not imported into the Microsoft Entra Connector space. To add it to the list of imported attributes:

1. Select the **Connectors** tab in the Synchronization Service Manager.
2. Right-click the Microsoft Entra connector, and select **Properties**.
3. In the pop-up dialog box, go to the **Select Attributes** tab.
4. Select the **preferredDataLocation** attribute in the list.
5. To save, select **OK**.



Step 5: Create an inbound synchronization rule

The inbound synchronization rule permits the attribute value to flow from the source attribute in on-premises Active Directory to the metaverse.

1. Start the **Synchronization Rules Editor** by going to **START > Synchronization Rules Editor**.
2. Set the search filter **Direction** to be **Inbound**.
3. To create a new inbound rule, select **Add new rule**.
4. Under the **Description** tab, provide the following configuration:

[\[+\] Expand table](#)

Attribute	Value	Details
Name	<i>Provide a name</i>	For example, "In from AD – User preferredDataLocation"

Attribute	Value	Details
Description	<i>Provide a custom description</i>	
Connected System	<i>Pick the on-premises Active Directory Connector</i>	
Connected System Object Type	User	
Metaverse Object Type	Person	
Link Type	Join	
Precedence	<i>Choose a number between 1–99</i>	1–99 is reserved for custom sync rules. Do not pick a value that is used by another synchronization rule.

5. Keep the **Scoping filter** empty, to include all objects. You might need to tweak the scoping filter according to your Microsoft Entra Connect deployment.
6. Go to the **Transformation tab**, and implement the following transformation rule:

[\[+\] Expand table](#)

Flow type	Target attribute	Source	Apply once	Merge type
Direct	preferredDataLocation	Pick the source attribute	Unchecked	Update

7. To create the inbound rule, select **Add**.

The image displays three sequential screenshots of the 'Create inbound synchronization rule' dialog box, showing the progression through different configuration tabs:

- Description Tab:** Shows fields like Name (In from AD - User PreferredDataLocation), Description (Set the Office 365 region), Connected System (fabrikamonline.com), Connected System Object Type (user), Metaverse Object Type (person), Link Type (Join), Precedence (50), and Tags.
- Scoping filter Tab:** Shows a large input field for 'Add scoping filters, or click next to skip this step'.
- Transformations Tab:** Shows the 'Add transformations' section with a table for mapping attributes. The table has columns: FlowType, Target Attribute, Source, Apply Or, and Merge Type. A row is shown with Direct as FlowType, preferredDataLocation as Target Attribute, msDS-preferredDataLocation as Source, and Update as Merge Type.

Step 6: Create an outbound synchronization rule

The outbound synchronization rule permits the attribute value to flow from the metaverse to the **preferredDataLocation** attribute in Microsoft Entra ID:

1. Go to the **Synchronization Rules Editor**.
2. Set the search filter **Direction** to be **Outbound**.
3. Select **Add new rule**.
4. Under the **Description** tab, provide the following configuration:

Expand table

Attribute	Value	Details
Name	<i>Provide a name</i>	For example, "Out to Microsoft Entra ID – User preferredDataLocation"
Description	<i>Provide a description</i>	
Connected System	<i>Select the Microsoft Entra Connector</i>	
Connected System Object Type	User	
Metaverse Object Type	Person	
Link Type	Join	
Precedence	<i>Choose a number between 1–99</i>	1–99 is reserved for custom sync rules. Do not pick a value that is used by another synchronization rule.

5. Go to the **Scoping filter** tab, and add a single scoping filter group with two clauses:

[+] Expand table

Attribute	Operator	Value
sourceObjectType	EQUAL	User
cloudMastered	NOTEQUAL	True

Scoping filter determines which Microsoft Entra objects this outbound synchronization rule is applied to. In this example, we use the same scoping filter from "Out to Microsoft Entra ID – User Identity" OOB (out-of-box) synchronization rule. It prevents the synchronization rule from being applied to **User** objects that are not synchronized from an on-premises Active Directory. You might need to tweak the scoping filter according to your Microsoft Entra Connect deployment.

6. Go to the **Transformation** tab, and implement the following transformation rule:

[+] Expand table

Flow type	Target attribute	Source	Apply once	Merge type
Direct	preferredDataLocation	preferredDataLocation	Unchecked	Update

7. Close Add to create the outbound rule.

Create outbound synchronization rule

Description	Name	Out to AAD - User PreferredDataLocation
Scoping filter	Description	Set the Office 365 region
Join rules	Connected System	fabrikamonline.onmicrosoft.com
Transformations	Connected System Object Type	user
	Metaverse Object Type	person
	Link Type	Join
	Precedence	51
	Tag	
	Enable Password Sync	<input type="checkbox"/>
	Disabled	<input type="checkbox"/>

Create outbound synchronization rule

Description	Add scoping filters, or click next to skip this step											
Scoping filter	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th>Attribute</th> <th>Operator</th> <th>Value</th> </tr> <tr> <td>sourceObjectType</td> <td>EQUAL</td> <td>User</td> </tr> <tr> <td>cloudMastered</td> <td>NOTEQUAL</td> <td>True</td> </tr> </table>			Attribute	Operator	Value	sourceObjectType	EQUAL	User	cloudMastered	NOTEQUAL	True
Attribute	Operator	Value										
sourceObjectType	EQUAL	User										
cloudMastered	NOTEQUAL	True										
Join rules	<input type="button" value="Add clause"/>	<input type="button" value="Remove clause(s)"/>										
Transformations	<input type="button" value="Add group"/>	<input type="button" value="Remove group(s)"/>										

Create outbound synchronization rule

Description	Add transformations				
Scoping filter	FlowType	Target Attribute	Source	Apply Or	Merge Type
Join rules	Direct	preferredDataLocation	preferredDataLocation	<input type="checkbox"/>	Update
Transformations	<input type="button" value="Add transformation"/>	<input type="button" value="Remove"/>			

Step 7: Run full synchronization cycle

In general, full synchronization cycle is required. This is because you have added new attributes to both the Active Directory and Microsoft Entra Connector schema, and introduced custom synchronization rules. Verify the changes before exporting them to Microsoft Entra ID. You can use the following steps to verify the changes, while manually running the steps that make up a full synchronization cycle.

1. Run **Full import** on the on-premises Active Directory Connector:

- a. Go to the **Connectors** tab in the Synchronization Service Manager.
- b. Right-click the **on-premises Active Directory Connector**, and select **Run**.
- c. In the dialog box, select **Full Import**, and select **OK**.
- d. Wait for the operation to complete.

 **Note**

You can skip full import on the on-premises Active Directory Connector if the source attribute is already included in the list of imported attributes. In other words, you did not have to make any change during step 2 earlier in this article.

2. Run **Full import** on the Microsoft Entra Connector:

- a. Right-click the **Microsoft Entra Connector**, and select **Run**.
- b. In the dialog box, select **Full Import**, and select **OK**.
- c. Wait for the operation to complete.

3. Verify the synchronization rule changes on an existing **User** object.

The source attribute from on-premises Active Directory, and **preferredDataLocation** from Microsoft Entra ID, have been imported into each respective connector space. Before proceeding with the full synchronization step, do a preview on an existing **User** object in the on-premises Active Directory Connector space. The object you picked should have the source attribute populated. A successful preview with **preferredDataLocation** populated in the metaverse is a good indicator that you have configured the synchronization rules correctly. For information about how to do a preview, see [Verify the change](#).

4. Run **Full Synchronization** on the on-premises Active Directory Connector:

- a. Right-click the **on-premises Active Directory Connector**, and select **Run**.
- b. In the dialog box, select **Full Synchronization**, and select **OK**.
- c. Wait for the operation to complete.

5. Verify **Pending Exports** to Microsoft Entra ID:

- a. Right-click the **Microsoft Entra Connector**, and select **Search Connector Space**.
- b. In the **Search Connector Space** dialog box:

- a. Set Scope to Pending Export.
 - b. Select all three check boxes, including Add, Modify, and Delete.
 - c. To view the list of objects with changes to be exported, select Search. To examine the changes for a given object, double-click the object.
 - d. Verify that the changes are expected.
6. Run Export on the Microsoft Entra Connector
- a. Right-click the Microsoft Entra Connector, and select Run.
 - b. In the Run Connector dialog box, select Export, and select OK.
 - c. Wait for the operation to complete.

 Note

You might notice that the steps do not include the full synchronization step on the Microsoft Entra Connector, or the export step on the Active Directory Connector. The steps are not required, because the attribute values are flowing from on-premises Active Directory to Microsoft Entra-only.

Step 8: Re-enable sync scheduler

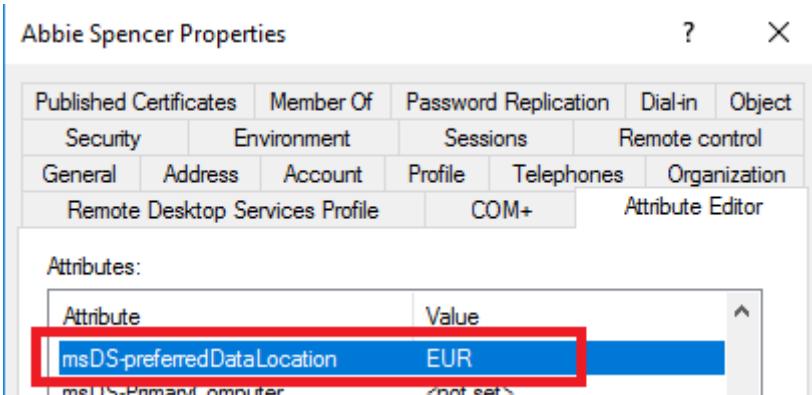
Re-enable the built-in sync scheduler:

1. Start a PowerShell session.
2. Re-enable scheduled synchronization by running this cmdlet: `Set-ADSyncScheduler -SyncCycleEnabled $true`

Step 9: Verify the result

It is now time to verify the configuration and enable it for your users.

1. Add the geo to the selected attribute on a user. The list of available geos can be found in this table.



Attribute	Value
msDS-preferredDataLocation	EUR
msDS-PrimaryComputer	<not set>

2. Wait for the attribute to be synchronized to Microsoft Entra ID.
3. Using Exchange Online PowerShell, verify that the mailbox region has been set correctly.

```
PS C:\Users\Administrator> Get-Mailbox -ANR abbie.spencer | fl MailboxRegion*
```

MailboxRegion	:	EUR
MailboxRegionLastUpdateTime	:	1/13/2018 9:50:50 AM

Assuming your tenant has been marked to be able to use this feature, the mailbox is moved to the correct geo. This can be verified by looking at the server name where the mailbox is located.

Next steps

Learn more about Multi-Geo in Microsoft 365:

- [Multi-Geo sessions at Ignite ↗](#)
- [Multi-Geo in OneDrive](#)
- [Multi-Geo in SharePoint Online](#)

Learn more about the configuration model in the sync engine:

- Read more about the configuration model in [Understanding Declarative Provisioning](#).
- Read more about the expression language in [Understanding Declarative Provisioning Expressions](#).

Overview topics:

- [Microsoft Entra Connect Sync: Understand and customize synchronization](#)
- [Integrating your on-premises identities with Microsoft Entra ID](#)

Configure Search for Microsoft 365 Multi-Geo

Article • 07/26/2024

Configure Multi-Geo Search

Your Multi-Geo *Tenant* will have aggregate search capabilities allowing a search query to return results from anywhere within the *Tenant*.

By default, searches from these entry points will return aggregate results, even though each search index is located within its relevant *Geography* location:

- OneDrive
- Delve
- SharePoint Home
- Search Center

Additionally, Multi-Geo search capabilities can be configured for your custom search applications that use the SharePoint search API.

Please review [Configure Search for OneDrive Multi-Geo](#) for instructions including any limitations and differences.

Validating the Microsoft 365 Multi-Geo configuration

Below are some basic use cases you may wish to include in your validation plan before broadly rolling out Microsoft 365 Multi-Geo to your company. Once you have completed these tests and any additional use cases that are relevant to your company, you may choose to move on to adding the users in your initial pilot group.

OneDrive:

Select OneDrive from the Microsoft 365 app launcher and confirm that you are automatically directed to the appropriate *Geography* location for the user, based on the user's PDL. OneDrive should now begin provisioning at that location. Once provisioned, try uploading and downloading some documents.

OneDrive Mobile App:

Log in to your OneDrive mobile App with your test account credentials. Confirm that you can see your OneDrive files and can interact with them from your mobile device.

OneDrive sync client:

Confirm that the OneDrive sync client automatically detects your OneDrive *Geography* location upon login. If you need to download the sync client, you can click **Sync** in the OneDrive library.

Office applications:

Confirm that you can access OneDrive by logging in from an Office application, such as Word. Open the Office application and select **OneDrive – <TenantName>**. Office will detect your OneDrive location and show you the files that you can open.

Sharing:

Try sharing OneDrive files. Confirm that the people picker shows you all your SharePoint users regardless of their *Geography* location.

In a multi-geo environment, each *Geography* location has its own search index and Search Center. When a user searches, the query is fanned out to all the indexes, and the returned results are merged.

For example, a user in one *Geography* location can search for content stored in another *Geography* location, or for content on a SharePoint site that's restricted to a different *Geography* location. If the user has access to this content, search will show the result.

Which search clients work in a Multi-Geo environment?

These clients can return results from all *Geography* locations:

- OneDrive
- Delve
- The SharePoint home page
- The Search Center
- Custom search applications that use the SharePoint Search API

OneDrive

As soon as the Multi-Geo environment has been set up, users that search in OneDrive get results from all *Geography* locations.

Delve

As soon as the Multi-Geo environment has been set up, users that search in Delve get results from all *Geography* locations.

The Delve feed and the profile card only show previews of files that are stored in the central location. For files that are stored in *Satellite Geography* locations, the icon for the file type is shown instead.

The SharePoint home page

As soon as the Multi-Geo environment has been set up, users will see news, recent and followed sites from multiple *Geography* locations on their SharePoint home page. If they use the search box on the SharePoint home page, they'll get merged results from multiple *Geography* locations.

The Search Center

After the multi-geo environment has been set up, each Search Center continues to only show results from their own *Geography* location. Admins must [change the settings of each Search Center](#) to get results from all *Geography* locations. Afterwards, users that search in the Search Center get results from all *Geography* locations.

Custom search applications

As usual, custom search applications interact with the search indexes by using the existing SharePoint Search REST APIs. To get results from all, or some *Geography* locations, the application must [call the API and include the new Multi-Geo query parameters](#) in the request. This triggers a fan out of the query to all *Geography* locations.

What's different about search in a Multi-Geo environment?

Some search features you might be familiar with, work differently in a multi-geo environment.

Feature	How it works	Workaround
Promoted results	You can create query rules with promoted results at different levels: for the whole _Tenant_, for a site collection, or for a site. In a Multi-Geo environment, define promoted results at the _Tenant_ level to promote the results to the Search Centers in all _Geography_ locations. If you only want to promote results in the Search Center that's in the _Geography_ location of the site collection or site, define the promoted results at the site collection or site level. These results are not promoted in other _Geography_ locations.	If you don't need different promoted results per _Geography_ location, for example different rules for traveling, we recommend defining promoted results at the _Tenant_ level.
Search refiners	Search returns refiners from all the _Geography_ locations of a _Tenant_ and then aggregates them. The aggregation is a best effort, meaning that the refiner counts might not be 100% accurate. For most search-driven scenarios, this accuracy is sufficient.	For search-driven applications that depend on refiner completeness, query each _Geography_ location independently.
	Multi-Geo search doesn't support dynamic bucketing for numerical refiners.	Use the "Discretize" parameter for numerical refiners.
Document IDs	If you're developing a search-driven application that depends on document IDs, note that document IDs in a Multi-Geo environment aren't unique across _Geography_ locations, they are unique per _Geography_ location.	We've added a column that identifies the _Geography_ location. Use this column to achieve uniqueness. This column is named "GeoLocationSource".
Number of results	The search results page shows combined results from the _Geography_ locations, but it's not possible to page beyond 500 results.	
Hybrid search	In a hybrid SharePoint environment with cloud hybrid search , on-premises content is added to the Microsoft 365 index of the central location.	

What's not supported for search in a multi-geo environment?

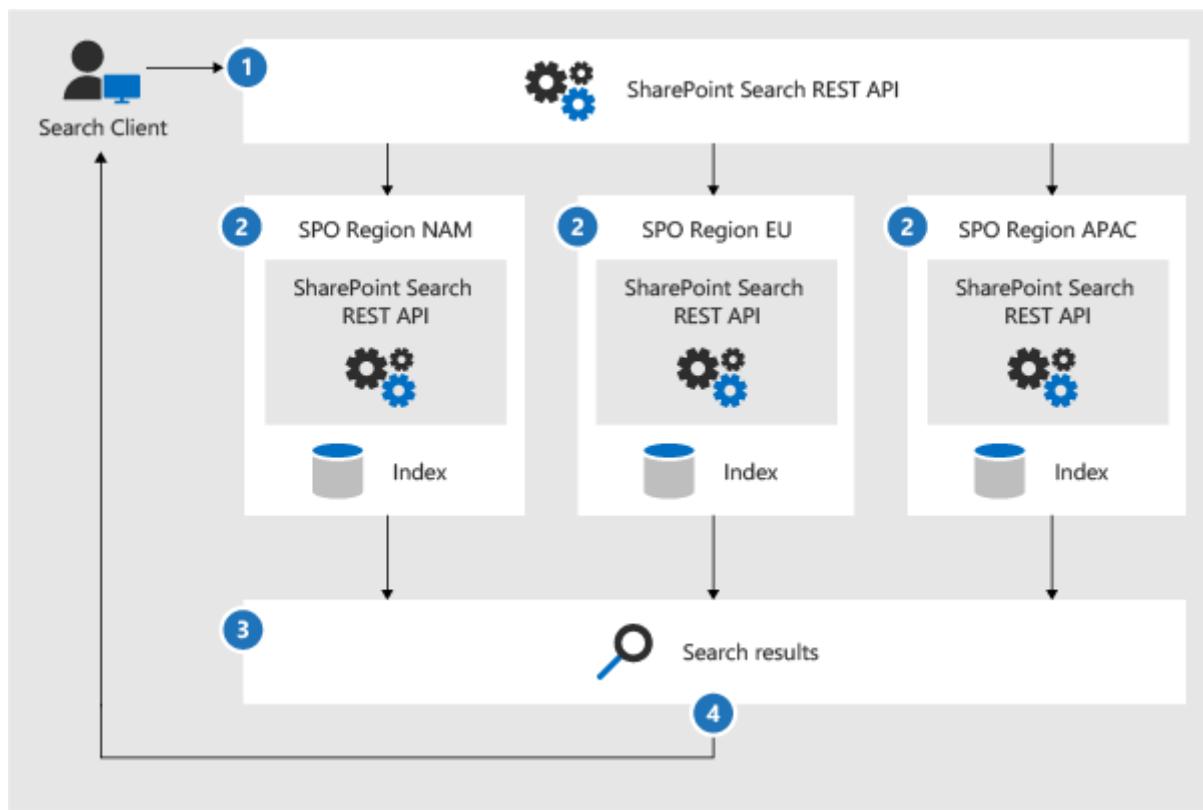
Some of the search features you might be familiar with, aren't supported in a multi-geo environment.

[] Expand table

Search feature	Note
App-only authentication	App-only authentication (privileged access from services) isn't supported in multi-geo search.
Guests	Guests only get results from the <code>_Geography_</code> location that they're searching from.

How does search work in a Multi-Geo environment?

All the search clients use the existing SharePoint Search REST APIs to interact with the search indexes.



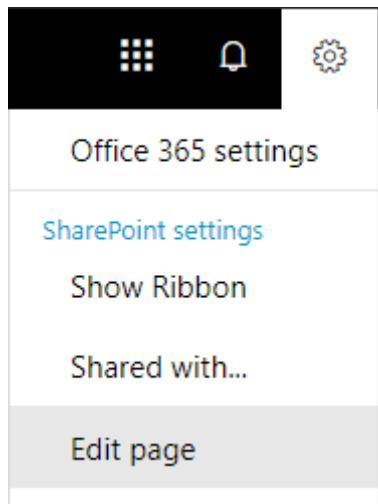
1. A search client calls the Search REST endpoint with the query property `EnableMultiGeoSearch= true`.
2. The query is sent to all *Geography* locations in the *Tenant*.
3. Search results from each *Geography* location are merged and ranked.
4. The client gets unified search results.

Notice that we don't merge the search results until we've received results from all the geo locations. This means that multi-geo searches have additional latency compared to searches in an environment with only one geo location.

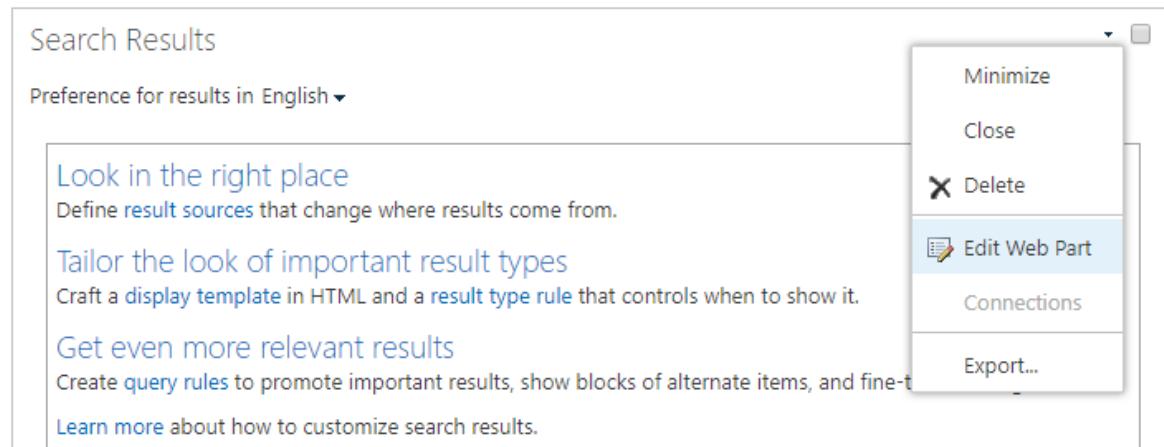
Get a Search Center to show results from all geo locations

Each Search Center has several verticals and you have to set up each vertical individually.

1. Ensure that you perform these steps with an account that has permission to edit the search results page and the Search Result Web Part.
2. Navigate to the search results page (see the [list](#) of search results pages)
3. Select the vertical to set up, click **Settings** gear icon in the upper, right corner, and then click **Edit Page**. The search results page opens in Edit mode.



4. In the Search Results Web Part, move the pointer to the upper, right corner of the web part, click the arrow, and then click **Edit Web Part** on the menu. The Search Results Web Part tool pane opens under the ribbon in the top right of the page.



5. In the Web Part tool pane, in the **Settings** section, under **Results control settings**, select **Show Multi-Geo results** to get the Search Results Web Part to show results from all geo locations.
6. Click **OK** to save your change and close the Web Part tool pane.

7. Check your changes to the Search Results Web Part by clicking **Check-In** on the Page tab of the main menu.
8. Publish the changes by using the link provided in the note at the top of the page.

Get custom search applications to show results from all or some geo locations

Custom search applications get results from all, or some, *Geography* locations by specifying query parameters with the request to the SharePoint Search REST API. Depending on the query parameters, the query is fanned out to all *Geography* locations, or to some geo locations. For example, if you only need to query a subset of *Geography* locations to find relevant information, you can control the fan out to only these. If the request succeeds, the SharePoint Search REST API returns response data.

Requirement

For each geo location, you must ensure that all users in the organization have been granted the **Read** permission level for the root website (for example contosoAPAC.sharepoint.com/ and contosoEU.sharepoint.com/). [Learn about permissions ↗](#).

Query parameters

EnableMultiGeoSearch - This is a Boolean value that specifies whether the query shall be fanned out to the indexes of other geo locations of the multi-geo *Tenant*. Set it to **true** to fan out the query; **false** to not fan out the query. If you don't include this parameter, the default value is **false**, except when making a REST API call against a site which uses the Enterprise Search Center template, in this case the default value is **true**. If you use the parameter in an environment that isn't multi-geo, the parameter is ignored.

ClientType - This is a string. Enter a unique client name for each search application. If you don't include this parameter, the query is not fanned out to other geo locations.

MultiGeoSearchConfiguration - This is an optional list of which geo locations in the multi-geo *Tenant* to fan the query out to when **EnableMultiGeoSearch** is **true**. If you don't include this parameter, or leave it blank, the query is fanned out to all geo locations. For each geo location, enter the following items, in JSON format:

[] [Expand table](#)

Item	Description
DataLocation	The _Geography_ location, for example NAM.
EndPoint	The endpoint to connect to, for example https://contoso.sharepoint.com
SourceId	The GUID of the result source, for example B81EAB55-3140-4312-B0F4-9459D1B4FFEE.

If you omit DataLocation or EndPoint, or if a DataLocation is duplicated, the request fails.

[You can get information about the endpoint of a tenant's geo locations by using Microsoft Graph.](#)

Response data

MultiGeoSearchStatus – This is a property that the SharePoint Search API returns in response to a request. The value of the property is a string and gives the following information about the results that the SharePoint Search API returns:

[\[+\] Expand table](#)

Value	Description
Full	Full results from all the _Geography_ locations.
Partial	Partial results from one or more _Geography_ locations. The results are incomplete due to a transient error.

Query using the REST service

With a GET request, you specify the query parameters in the URL. With a POST request, you pass the query parameters in the body in JavaScript Object Notation (JSON) format.

Request headers

[\[+\] Expand table](#)

Name	Value
Content-Type	application/json;odata=verbose

Sample GET request that's fanned out to all geo locations

HTTP

```
https:// \<tenant\>/\_api/search/query?  
querytext='sharepoint'&Properties='EnableMultiGeoSearch:true'&ClientType='my  
\_client\_id'
```

Sample GET request to fan out to some geo locations

HTTP

```
https:// \<tenant\>/\_api/search/query?  
querytext='site'&ClientType='my_client_id'&Properties='EnableMultiGeoSearch:  
true, MultiGeoSearchConfiguration:  
[{DataLocation\\:"NAM\"",Endpoint\\:"https\\://contosoNAM.sharepoint.com\"},  
SourceId\\:"B81EAB55-3140-4312-B0F4-9459D1B4FFEE"}\\,  
{DataLocation\\:"CAN\"",Endpoint\\:"https\\://contosoCAN.sharepoint-  
df.com"}]'
```

① Note

Commas and colons in the list of geo locations for the MultiGeoSearchConfiguration property are preceded by the **backslash** character. This is because GET requests use colons to separate properties and commas to separate arguments of properties. Without the backslash as an escape character, the MultiGeoSearchConfiguration property is interpreted wrongly.

Sample POST request that's fanned out to all geo locations

HTTP

```
{
  "request": {
    "__metadata": {
      "type": "Microsoft.Office.Server.Search.REST.SearchRequest"
    },
    "Querytext": "sharepoint",
    "Properties": {
      "results": [
        {
          "Name": "EnableMultiGeoSearch",
          "Value": {
            "QueryPropertyValueTypeIndex": 3,
            "BoolVal": true
          }
        }
      ]
    }
  }
}
```

```
    },
    "ClientType": "my_client_id"
}
}
```

Sample POST request that's fanned out to some geo locations

HTTP

```
{
  "request": {
    "Querytext": "SharePoint",
    "ClientType": "my_client_id",
    "Properties": {
      "results": [
        {
          "Name": "EnableMultiGeoSearch",
          "Value": {
            "QueryPropertyValueIndex": 3,
            "BoolVal": true
          }
        },
        {
          "Name": "MultiGeoSearchConfiguration",
          "Value": {
            "StrVal": "[{\\"DataLocation\\":\\"NAM\\",\\"Endpoint\\":\\"https://contoso.sharepoint.com\\",\\
\"SourceId\\":\\"B81EAB55-3140-4312-B0F4-9459D1B4FFEE\\"},
{\\\"DataLocation\\":\\"CAN\\",\\"Endpoint\\":\\"https://contosoCAN.sharepoint.com\\"
}]",

            "QueryPropertyValueIndex": 1
          }
        }
      ]
    }
  }
}
```

Query using CSOM

Here's a sample CSOM query that's fanned out to all *Geography* locations:

CSOM

```
var keywordQuery = new KeywordQuery(ctx);
keywordQuery.QueryText = query.SearchQueryText;
keywordQuery.ClientType = <enter a string here>;
keywordQuery.Properties["EnableMultiGeoSearch"] = true;
```

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

User Testing in Multi-Geo

Article • 06/19/2024

In Microsoft Entra there are two types of user objects: cloud only users and synchronized users. Follow the appropriate instructions for your type of user.

💡 Tip

We recommend that you begin validations with a test user or small group of users before rolling out multi-geo to your broader organization.

Synchronize user's Preferred Data Location (PDL) using Microsoft Entra Connect

If your company's users are synchronized from an on-premises Active Directory system to Microsoft Entra ID, their PreferredDataLocation must be populated in AD and synchronized to Microsoft Entra ID.

Follow the process in [Azure Active Directory Connect sync: Configure preferred data location for Microsoft 365 resources](#) to configure Preferred Data Location sync from your on-premises Active Directory Domain Services (AD DS) to Microsoft Entra ID.

We recommend that you include setting the user's Preferred Data Location as a part of your standard user creation workflow.

ⓘ Important

For new users with no OneDrive provisioned, license the account and wait at least 48 hours after a user's PDL is synchronized to Microsoft Entra ID for the changes to propagate before the user logs in to OneDrive. (Setting the preferred data location before the user logs in to provision their OneDrive ensures that the user's new OneDrive will be provisioned in the correct location.)

Setting Preferred Data Location (PDL) for cloud only users

ⓘ Note

The Azure Active Directory module is being replaced by the Microsoft Graph PowerShell SDK. You can use the Microsoft Graph PowerShell SDK to access all Microsoft Graph APIs. For more information, see [Get started with the Microsoft Graph PowerShell SDK](#).

ⓘ Note

Azure AD and MSOnline PowerShell modules are deprecated as of March 30, 2024. To learn more, read the [deprecation update](#). After this date, support for these modules are limited to migration assistance to Microsoft Graph PowerShell SDK and security fixes. The deprecated modules will continue to function through March, 30 2025.

We recommend migrating to [Microsoft Graph PowerShell](#) to interact with Microsoft Entra ID (formerly Azure AD). For common migration questions, refer to the [Migration FAQ](#). Note: Versions 1.0.x of MSOnline may experience disruption after June 30, 2024.

First, use a Microsoft Entra DC admin or Cloud Application Admin account to [connect to your Microsoft 365 tenant](#).

PowerShell

```
Connect-Graph -Scopes User.ReadWrite.All
```

Use the following script format:

PowerShell

```
$userUPN=<user's UPN>
$user = Get-MgUser -UserId $userUPN
Update-MgUser -UserId $user.Id -PreferredDataLocation <international location code>
```

In this example, you set the user adelev@contoso.com's preferred data location to EUR:

PowerShell

```
$userUPN="adelev@contoso.com"
$user = Get-MgUser -UserId $userUPN
Update-MgUser -UserId $user.Id -PreferredDataLocation EUR
```

You can check to confirm that the preferred data location was updated properly by navigating to the Microsoft 365 Admin Center and selecting **Settings > Users > Active Users > [username]**. Select the user from the list, and you'll find Preferred Data Location under the **Account** tab of the user's page.

We recommend that you include setting the user's Preferred Data Location as a part of your standard user creation workflow.

Important

For new users with no OneDrive provisioned, license the account and wait at least 48 hours after a user's PDL is set for the changes to propagate before the user logs in to OneDrive. (Setting the preferred data location before the user logs in to provision their OneDrive ensures that the user's new OneDrive will be provisioned in the correct location.)

OneDrive Provisioning and the effect of PDL

If the user already has a OneDrive site created in the *Tenant*, setting their PDL won't automatically move their existing OneDrive. To move a user's OneDrive, see [OneDrive Geo Move](#).

Note

Exchange Online automatically relocates the user's mailbox if the PDL changes and the MailboxRegion no longer matches the Mailbox Database Geo Location code. For more information, see [Administering Exchange Online mailboxes in a multi-geo environment](#).

If the user doesn't have a OneDrive site within the *Tenant*, OneDrive will be provisioned for them in accordance to their PDL value, assuming the PDL for the user matches one of the company's satellite locations.

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Add or remove a *Geography* administrator in Microsoft 365 Multi-Geo

Article • 12/11/2023

You can configure separate administrators for each *Geography* location that you have in your *Tenant*. These administrators will have access to the SharePoint and OneDrive settings that are specific to their *Geography* location.

Some services - such as the term store - are administered from the *Primary Provisioned Geography* location and replicated to *Satellite Geography* locations. The *Geography* admin for the *Primary Provisioned Geography* location has access to these, whereas *Geography* admins for *Satellite Geography* locations don't.

Global administrators and SharePoint administrators continue to have access to settings in the *Primary Provisioned Geography* location and all *Satellite Geography* locations.

Configuring *Geography* administrators

Configuring *Geography* admins requires the SharePoint PowerShell module.

Use [Connect-SPOService](#) to connect to the admin center of the *Geography* location where you want to add the *Geography* admin. (For example, Connect-SPOService <https://ContosoEUR-admin.sharepoint.com>.)

To view the existing *Geography* admins of a location, run `Get-SPOGeoAdministrator`

Adding a user as a *Geography* admin

To add a user as a *Geography* admin, run `Add-SPOGeoAdministrator -UserPrincipalName <UPN>`

To remove a user as a *Geography* Admin of a location, run `Remove-SPOGeoAdministrator -UserPrincipalName <UPN>`

Adding a group as a *Geography* admin

You can add a security group or a mail-enabled security group as a *Geography* admin. (Distribution groups and Microsoft 365 Groups aren't supported.)

To add a group as a *Geography* administrator, run `Add-SPOGeoAdministrator -GroupAlias <alias>`

To remove a group as a *Geography* administrator, run `Remove-SPOGeoAdministrator -GroupAlias <alias>`

Note that not all security groups have a group alias. If you want to add a security group that doesn't have an alias, run [Get-MgGroup](#) to retrieve a list of groups, find your security group's ObjectId, and then run:

```
Add-SPOGeoAdministrator -ObjectId <ObjectId>
```

To remove a group by using the ObjectId, run `Remove-SPOGeoAdministrator -ObjectId <ObjectId>`

Related articles

[Add-SPOGeoAdministrator](#)

[Get-SPOGeoAdministrator](#)

[Remove-SPOGeoAdministrator](#)

[Set an alias \(MailNickname\) for a security group](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Restrict SharePoint site content to a geo location

Article • 12/11/2023

Under certain circumstances you may choose to enforce a site and its file content to remain in the *Geography* location where the site was created, either by preventing the site from being moved or by preventing the caching of the site's file content in another *Geography* location.

You can do this task by using the [Set-SPOSite](#) cmdlet with the **RestrictedToGeo** parameter. This parameter has a default value of NULL, but you can change it to one of the following restrictions:

[] [Expand table](#)

Restriction	Description
NoRestriction	The site can be moved to another <i>Geography</i> location.
BlockMoveOnly	Site can't be moved to another <i>Geography</i> location, but site content can be cached in other <i>Geography</i> locations.
BlockFull	Site can't be moved to another <i>Geography</i> location, and full file content isn't cached in other <i>Geography</i> locations. Files' title (harvested from the content), file name, and other properties of the file can still be cached in other <i>Geography</i> locations. Content stored in the site before it was configured to BlockFull, may continue to be cached in other <i>Geography</i> locations.

Use the following syntax:

```
Set-SPOSite -Identity <siteURL> -RestrictedToGeo <restriction>
```

For example:

```
Set-SPOSite -Identity https://contoso.sharepoint.com/sites/RegionRestrictedTeamSite  
-RestrictedToGeo BlockFull
```

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Microsoft 365 Multi-Geo eDiscovery configuration

Article • 08/01/2024

[eDiscovery \(Premium\) capabilities](#) allow a Multi-Geo eDiscovery administrator to search all of the *Geographies* without needing to utilize a "Region" security filter. Data is exported to the Azure instance of the *Primary Provisioned Geography* location of the multi-geo *Tenant*.

Without eDiscovery (Premium) capabilities, an eDiscovery manager or administrator of a Multi-Geo *Tenant* will be able to conduct eDiscovery only in the *Primary Provisioned Geography* location of that *Tenant*. To support the ability to conduct eDiscovery for *Satellite Geography* locations, a new compliance security filter parameter named "Region" is available via PowerShell. This parameter can be used by *Tenants* whose *Primary Provisioned Geography* location is in North America, Europe, or Asia Pacific. eDiscovery (Premium) is recommended for *Tenants* whose *Primary Provisioned Geography* location is not in North America, Europe, or Asia Pacific and who need to perform eDiscovery across *Satellite Geography* locations.

A member of the **Organization Management** role group or a user with the **Role Management** role must assign eDiscovery Manager permissions in the Microsoft Purview portal to allow others to perform eDiscovery tasks and assign a "Region" parameter in their applicable Compliance Security Filter to specify the *Geography* for conducting eDiscovery as *Satellite Geography* location. Otherwise, no eDiscovery activities will be carried out for the *Satellite Geography* location. Only one "Region" security filter per user is supported.

See [Assign eDiscovery permissions in the compliance portal](#) for more information. To configure the Compliance Security Filter for a Region, see [Configure Office 365 Multi-Geo eDiscovery](#).

When the eDiscovery Manager or Administrator role is set for a particular *Satellite Geography* location, the eDiscovery Manager or Administrator will only be able to perform eDiscovery search actions against the SharePoint sites and OneDrive sites located in that *Satellite Geography* location. If an eDiscovery Manager or Administrator attempts to search SharePoint or OneDrive sites outside the specified *Satellite Geography* location, no results will be returned. Also, when the eDiscovery Manager or Administrator for a *Satellite Geography* location triggers an export, data is exported to the Azure instance of that region. This helps organizations stay in compliance by not allowing content to be exported across controlled borders.

 **Note**

If it's necessary for an eDiscovery Manager to search across multiple SharePoint *Satellite Geography* locations, another user account will need to be created for the eDiscovery Manager which specifies the alternate *Satellite Geography* location where the OneDrive or SharePoint sites are located.

 [Expand table](#)

Microsoft 365 Region	PreferredDataLocation (PDL) Value
South Korea, Japan, Singapore, Malaysia, Hong Kong Special Administrative Region	APC
Australia	AUS
Brazil	BRA
Canada	CAN
France, Netherlands, Ireland, Norway, Switzerland, Austria, Finland, Sweden, Germany	EUR
France	FRA
Germany	DEU
India	IND
Israel	ISR
Italy	ITA
Japan	JPN
Korea	KOR
Mexico	MEX
Norway	NOR
Poland	POL
Qatar	QAT
South Africa	ZAF
Spain	ESP

Microsoft 365 Region	PreferredDataLocation (PDL) Value
Sweden	SWE
Switzerland	CHE
United Arab Emirates	ARE
United Kingdom	GBR
United States	NAM

To set the Compliance Security Filter for a Region:

1. [Connect to Microsoft 365 Security & Compliance PowerShell](#)
2. Use the following syntax:

PowerShell

```
New-ComplianceSecurityFilter -Action All -FilterName
<TheNameYouWantToAssign> -Region <RegionValue> -Users
<UserPrincipalName>
```

For example:

PowerShell

```
New-ComplianceSecurityFilter -Action All -FilterName "NAM eDiscovery
Managers" -Region NAM -Users adwood@contoso.onmicrosoft.com
```

See the [New-ComplianceSecurityFilter](#) article for additional parameters and syntax.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Create a Microsoft 365 group with a specific preferred data location

Article • 05/06/2024

When users in a multi-geo environment create a Microsoft 365 group, the group preferred data location (PDL) is automatically set to that of the user. Global, SharePoint, and Exchange Administrators can create groups in any *Geography* they select.

If you need to create a group with a specific PDL, you can do that using from the [SharePoint admin center](#) or through the Exchange Online New-UnifiedGroup Microsoft PowerShell cmdlet. When you do this, both the group mailbox and SharePoint site associated with the group will be provisioned in the specified PDL.

To create a Microsoft 365 group with the PDL that you specify, go to the [SharePoint admin center](#) in the *Geography* location where you want to create the group site.

For example:

If you want to create a group site in your Australia location, you can go to

```
https://ContosoAUS-  
admin.sharepoint.com/_layouts/15/online/AdminHome.aspx#/siteManagement
```

1. Select + Create.
2. Follow the process to create a group site.

Your group site will be provisioned in the *Geography* location corresponding to the SharePoint admin center from which you initiated the site creation request.

Using Exchange PowerShell

Connect to Exchange Online PowerShell and pass the parameter `-MailBoxRegion` with the geo location code.

For example:

```
PowerShell  
  
New-UnifiedGroup -DisplayName MultiGeoEUR -Alias "MultiGeoEUR" -AccessType  
Public -MailboxRegion EUR
```

```
PS C:\> New-UnifiedGroup -DisplayName MultiGeoEUR -Alias "MultiGeoEUR" -AccessType Public -MailboxRegion EUR
Name DisplayName GroupType PrimarySmtpAddress
---- -----
MultiGeoEUR_675508cb-5c1b-4523-bc26-2ddb740b04d3 MultiGeoEUR Universal MultiGeoEUR@ContosoEnterprise.onmicrosoft.com
```

! Note

SharePoint group site provisioning is on-demand. The site will be provisioned the first time a group owner or member attempts to access it.

Geo location codes

[] [Expand table](#)

Geo location	Code	eDiscovery data location
Macro Region Geography 2 - Asia-Pacific	APC	Southeast or East Asia datacenters
Australia	AUS	Southeast or East Asia datacenters
Brazil	BRA	(eDiscovery data location coming soon)
Canada	CAN	- eDiscovery (Premium): Canada datacenters - eDiscovery (Standard): US datacenters
Macro Region Geography 1 - EMEA	EUR	Europe datacenters
France	FRA	Europe datacenters
Germany	DEU	Europe datacenters
India	IND	Southeast or East Asia datacenters
Israel	ISR	(eDiscovery data location coming soon)
Italy	ITA	(eDiscovery data location coming soon)
Japan	JPN	Southeast or East Asia datacenters
Korea	KOR	Southeast or East Asia datacenters
Macro Region Geography 3 - Americas	NAM	US datacenters
Norway	NOR	(eDiscovery data location coming soon)
Poland	POL	(eDiscovery data location coming soon)
Qatar	QAT	(eDiscovery data location coming soon)

Geo location	Code	eDiscovery data location
South Africa	ZAF	Europe datacenters
Sweden	SWE	Europe datacenters
Switzerland	CHE	Europe datacenters
United Arab Emirates	ARE	Southeast or East Asia datacenters
United Kingdom	GBR	Europe datacenters

Related articles

[Connect to Exchange Online PowerShell](#)

[Create groups with a specific preferred data location using Graph API](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Delete a *Satellite Geography* location in Microsoft 365 Multi-Geo

Article • 08/27/2024

If you no longer need a *Satellite Geography* location, you can delete it from your *Tenant* from the [SharePoint admin center](#).

⚠️ Warning

All user data in the *Satellite Geography* location will be permanently deleted. This includes all OneDrive content, SharePoint sites and Exchange mailboxes including Microsoft 365 Group mailboxes. You must migrate any data to another *Satellite Geography* location or the *Primary Provisioned Geography* location before you delete the *Satellite Geography* location. This action cannot be undone.

Only SharePoint Administrators can delete *Satellite Geography* locations.

The screenshot shows the Microsoft 365 Multi-Geo admin center. On the left, there's a map of North America with a callout for 'North America'. Below the map, there are buttons for 'Add location' and 'Delete location (EUR)'. On the right, a modal window titled 'Delete satellite location' is open. It contains a warning message: 'If you delete this location, you won't be able to restore it. All the data will be permanently deleted.' Below this is a section titled 'Delete all data in geo location EMEA:' with counts for SharePoint sites (47) and OneDrive sites (12). At the bottom of the modal, there are two checkboxes: one acknowledging responsibility for data migration and another for permanent deletion. There are also 'Delete' and 'Cancel' buttons at the bottom.

To delete a *Satellite Geography* location

1. Open the SharePoint admin center, and go to the [Geo locations](#) tab ↗.
2. On the map, select the *Satellite Geography* location that you want to delete.
3. Select **Delete location**.
4. Confirm the deletion by selecting the confirmation check boxes.
5. Select **Delete**.

The deletion will take at least 7 days to complete.

Feedback

Was this page helpful?



[Provide product feedback](#) ↗

Data Residency for Exchange Online

Article • 02/29/2024

Data Residency Commitments Available

Product Terms

Required Conditions:

Tenant has a sign-up country/region included in Local Region Geography, the European Union or the United States.

For current language, please refer to the Privacy and Security Product Terms [webpage](#) and view the section titled "Location of Customer Data at Rest for Core Online Services".

Commitment:

ⓘ Note

If Customer provisions its tenant in Australia, Brazil, Canada, the European Union, France, Germany, India, Japan, Norway, Qatar, South Africa, South Korea, Sweden, Switzerland, United Arab Emirates, United Kingdom, or United States, Microsoft will store the following Customer Data at rest only within that Geo: Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments)

Advanced Data Residency add-on

Required Conditions:

1. Tenant has a sign-up country/region included in *Local Region Geography* or *Expanded Local Region Geography*.
2. Tenant has a valid Advanced Data Residency subscription for all users in the tenant
3. The Exchange Online subscription customer data is provisioned in Local Geography or Expanded Local Geography

Commitment:

Please refer to the [ADR commitment page](#) to understand the specific commitments provided via Product Terms. Examples of the committed data include: all types of

mailboxes, including user mailboxes, resource mailboxes, and archive mailboxes.

Multi-Geo add-on

Required Conditions:

1. Tenants have a valid Multi-Geo subscription that covers all users assigned to a *Satellite Geography*.
2. Customer must have an active Enterprise Agreement.
3. Total purchased Multi-Geo units must be greater than 5% of the total eligible users in the tenant.

Commitment:

Customers can assign a Satellite Geography supported by Multi-Geo to a supported mailbox type. See the [Microsoft 365 Multi-Geo availability section](#) of the Microsoft 365 Multi-Geo page for details. The Data at Rest for Office 365 Services for the mailbox as defined by the product terms shall be stored in the assigned Satellite Geography. Supported mailbox types include Exchange Online user primary and archive mailboxes, resource mailboxes, Microsoft 365 Group mailboxes, and shared mailboxes.

Multi-Geo Capabilities in Exchange Online

Customers may assign a *Satellite Geography* supported by Multi-Geo to a user. See the [Microsoft 365 Multi-Geo availability section](#) of the Microsoft 365 Multi-Geo page for details. The user's Data at Rest for Office 365 Services as defined by the product terms shall be stored in the assigned *Satellite Geography*. This includes all types of Exchange Online mailboxes, including user mailboxes, resource mailboxes, Microsoft 365 Group mailboxes, shared mailboxes, and archive mailboxes.

You can place mailboxes in *Satellite Geography* locations by:

1. Creating a new Exchange Online mailbox directly in a *Satellite Geography* location.
2. Moving an existing Exchange Online mailbox to a *Satellite Geography* location by changing the user's preferred data location.
3. Onboarding a mailbox from an on-premises Exchange organization directly into a *Satellite Geography* location.

Mailbox placement and moves

After Microsoft completes the prerequisite Multi-Geo configuration steps, Exchange Online will honor the PreferredDataLocation attribute on user objects in Microsoft Entra

ID. Exchange Online synchronizes the PreferredDataLocation property from Microsoft Entra ID into the MailboxRegion property in the Exchange Online directory service. The value of MailboxRegion determines the *Macro Region Geography* or *Local Region Geography* where user mailboxes and any associated archive mailboxes are placed. It isn't possible to configure a user's primary mailbox and archive mailboxes to reside in different *Geography* locations. Only one *Macro Region Geography* or *Local Region Geography* can be configured per user object.

- When PreferredDataLocation is configured on a user with an existing mailbox, the mailbox is put into a relocation queue and automatically moved to the specified *Macro Region Geography* or *Local Region Geography*.
- When PreferredDataLocation is configured on a user without an existing mailbox, when you provision the mailbox, it's provisioned into the specified *Macro Region Geography* or *Local Region Geography*.
- When PreferredDataLocation isn't specified on a user, when you provision the mailbox, it's provisioned in the *Primary Provisioned Geography*.
- If the PreferredDataLocation code is incorrect (for example, a typo of NAN instead of NAM), the mailbox is provisioned in the *Primary Provisioned Geography*.

 **Note**

Multi-geo capabilities and Skype for Business Online regionally hosted meetings both use the PreferredDataLocation property on user objects to locate services. If you configure PreferredDataLocation values on user objects for regionally hosted meetings, the mailbox for those users will be automatically moved to the specified *Macro Region Geography* or *Local Region Geography* after Multi-Geo is enabled on the Microsoft 365 tenant.

Feature limitations for Multi-Geo in Exchange Online

- Security and compliance features (for example, auditing and eDiscovery) that are available in the Exchange admin center (EAC) aren't available in Multi-Geo organizations. Instead, you need to use Microsoft Defender and Microsoft Purview to configure security and compliance features.
- Outlook for Mac users might experience a temporary loss of access to their Online Archive folder while you move their mailbox to a new *Geography* location. This condition occurs when the user's the primary and archive mailboxes are in different *Geography* locations, because cross-geo mailbox moves might complete at different times.

- Users can't share mailbox folders across *Geography* locations in Outlook on the web (formerly known as Outlook Web App or OWA). For example, a user in the European Union can't use Outlook on the web to open a shared folder in a mailbox located in the United States. However, Outlook on the Web users can open other mailboxes in different *Geography* locations by using a separate browser window as described in Open another person's mailbox in a separate browser window in Outlook Web App.

 **Note**

Cross-geo mailbox folder sharing is supported in Outlook on Windows.

- Public folders are supported in Multi-Geo organizations. However, the public folders must remain in the *Primary Provisioned Geography* location. You can't move public folders to satellite geo locations.
- In a Multi-Geo environment, cross-geo mailbox auditing isn't supported. For example, if a user is assigned permissions to access a shared mailbox in a different *Geography* location, mailbox actions performed by that user aren't logged in the mailbox audit log of the shared mailbox. Exchange admin audit events are also only available for the default location. For more information, see Manage mailbox auditing.

Administering Exchange Multi-Geo

Administering Exchange Online mailboxes in a Multi-Geo environment

Exchange Online PowerShell is required to view and configure Multi-Geo properties in your Microsoft 365 environment. To connect to Exchange Online PowerShell, see [Connect to Exchange Online PowerShell](#).

In Exchange Online Multi-Geo environments, you don't need to do any manual steps to add Geographies to your tenant. After you receive the Message Center post that says multi-geo is ready for Exchange Online, all available Geographies will be ready and configured for you to use.

Connect directly to a geo location using Exchange Online PowerShell

Typically, Exchange Online PowerShell connects to *Primary Provisioned Geography* location. But, you can also connect directly to *Satellite Geography* locations. Because of performance improvements, we recommend connecting directly to the *Satellite Geography* location when you only manage users in that location.

The requirements for installing and using the Exchange Online PowerShell module are described in [Install and maintain the Exchange Online PowerShell module](#).

To connect Exchange Online PowerShell to a specific *Geography* location, the *ConnectionUri* parameter is different than the regular connection instructions. The rest of the commands and values are the same.

Specifically, you need to add the `?email=<emailaddress>` value to end of the *ConnectionUri* value, where `<emailaddress>` is the email address of **any** mailbox in the target *Geography* location. Your permissions to that mailbox or the relationship to your credentials aren't a factor; the email address simply tells Exchange Online PowerShell where to connect.

Microsoft 365 or Microsoft 365 GCC customers typically don't need to use the *ConnectionUri* parameter to connect to Exchange Online PowerShell. But, to connect to a specific *Geography* location, you do need to use *ConnectionUri* parameter so you can use `?email=<emailaddress>` in the value.

Connect to a *Geography* location in Exchange Online PowerShell

The following connection instructions work for accounts that are or aren't configured for multifactor authentication (MFA).

1. In a Windows PowerShell window, load the EXO V2 module by running the following command:

```
PowerShell  
  
Import-Module ExchangeOnlineManagement
```

1. In the following example, `admin@contoso.onmicrosoft.com` is the admin account, and the target geo location is where the mailbox `olga@contoso.onmicrosoft.com` resides.

```
PowerShell  
  
Connect-ExchangeOnline -UserPrincipalName admin@contoso.onmicrosoft.com -  
ConnectionUri https://outlook.office365.com/powershell?
```

```
email=olga@contoso.onmicrosoft.com
```

1. Enter the password for the admin@contoso.onmicrosoft.com in the prompt that appears. If the account is configured for MFA, you also need to enter the security code.

View the available *Geography* locations that are configured in your Exchange Online organization

To see the list of configured *Geography* locations in Microsoft 365 Multi-Geo, run the following command in Exchange Online PowerShell:

```
PowerShell
```

```
Get-OrganizationConfig | Select -ExpandProperty AllowedMailboxRegions | Format-Table
```

View the *Primary Provisioned Geography* location for your Exchange Online organization

To view your tenant's *Primary Provisioned Geography* location, run the following command in Exchange Online PowerShell:

```
PowerShell
```

```
Get-OrganizationConfig | Select DefaultMailboxRegion
```

Find the *Geography* location of a mailbox

The **Get-Mailbox** cmdlet in Exchange Online PowerShell displays the following multi-geo related properties on mailboxes:

- **Database**: The first three letters of the database name correspond to the *Geography* code, which tells you where the mailbox is currently located. For Online Archive Mailboxes the **ArchiveDatabase** property should be used.
- **MailboxRegion**: Specifies the *Geography* location code that was set by the admin (synchronized from PreferredDataLocation in Microsoft Entra ID).
- **MailboxRegionLastUpdateTime**: Indicates when MailboxRegion was last updated (either automatically or manually).

To see these properties for a mailbox, use the following syntax:

PowerShell

```
Get-Mailbox -Identity <MailboxIdentity> | Format-List  
Database,MailboxRegion*
```

For example, to see the *Geography* location information for the mailbox chris@contoso.onmicrosoft.com, run the following command:

PowerShell

```
Get-Mailbox -Identity chris@contoso.onmicrosoft.com | Format-List Database,  
MailboxRegion*
```

The output of the command looks like this:

PowerShell

```
Database      : EURPR03DG077-db007  
MailboxRegion  : EUR  
MailboxRegionLastUpdateTime : 2/6/2018 8:21:01 PM
```

ⓘ Note

If the *Geography* location code in the database name doesn't match **MailboxRegion** value, the mailbox will be automatically be put into a relocation queue and moved to the *Geography* location specified by the **MailboxRegion** value (Exchange Online looks for a mismatch between these property values).

Move an existing cloud-only mailbox to a specific geo location

ⓘ Note

The Azure Active Directory (AzureAD) PowerShell module is being deprecated and replaced by the Microsoft Graph PowerShell SDK. You can use the Microsoft Graph PowerShell SDK to access all Microsoft Graph APIs. For more information, see [Get started with the Microsoft Graph PowerShell SDK](#).

Also see [Install the Microsoft Graph PowerShell SDK](#) and [Upgrade from Azure AD PowerShell to Microsoft Graph PowerShell](#) for information on how to install and upgrade to Microsoft Graph PowerShell, respectively.

A cloud-only user is a user not synchronized to the tenant via Microsoft Entra Connect. This user was created directly in Microsoft Entra ID. Use the **Get-MgUser** and **Set-MgUser** cmdlets in the Microsoft Graph PowerShell SDK to view or specify the *Geography* location where a cloud-only user's mailbox will be stored.

First, you must connect to Microsoft Graph using the required permission scopes for the actions you'll take in your Microsoft Graph PowerShell session.

The Microsoft Graph PowerShell SDK supports two types of authentication: delegated access, and app-only access. In this guide, you'll use delegated access to sign in as a user, grant consent to the SDK to act on your behalf, and call the Microsoft Graph.

For details on using app-only access for unattended scenarios, see [Use app-only authentication with the Microsoft Graph PowerShell SDK](#).

Determine required permission scopes

Each API in the Microsoft Graph is protected by one or more permission scopes. The user logging in must consent to one of the required scopes for the APIs you plan to use. In this example, we'll use the following APIs.

List users to find the user ID of the logged-in user. Modify the **PreferredDataLocation** value for a user.

The *User.Read.All* permission scope enables the first call, and the *User.ReadWrite.All* scope enables the second. These permissions require an admin account.

For more information about how to determine what permission scopes you'll need, see [Using Find-MgGraphCommand cmdlet](#).

To connect to your Microsoft 365 Organization, run the following command:

PowerShell

```
Connect-MgGraph -Scopes "User.Read.All", "Group.ReadWrite.All"
```

The command prompts you to go to a web page to sign in with your credentials. Once you've done that, the command indicates success with a Welcome To Microsoft Graph! message. You only need to sign in once per session.

Tip

You can accretively add permissions by repeating the `Connect-MgGraph` command with the new permission scopes.

To view the **PreferredDataLocation** value for a user, use this syntax in Microsoft Graph PowerShell:

```
PowerShell
```

```
Get-MgUser -ConsistencyLevel eventual -Count userCount -Search  
' "UserPrincipalName:<UserPrincipalName>"' | Format-List  
UserPrincipalName,PreferredDataLocation
```

For example, to see the **PreferredDataLocation** value for the user michelle@contoso.onmicrosoft.com, run the following command:

```
PowerShell
```

```
Get-MgUser -ConsistencyLevel eventual -Count userCount -Search  
' "UserPrincipalName:michelle@contoso.onmicrosoft.com"' | Format-List
```

To modify the **PreferredDataLocation** value for a cloud-only user object, use the following syntax in Microsoft Graph PowerShell:

```
PowerShell
```

```
Update-MgUser -UserID <UserID> -PreferredDataLocation <GeoLocationCode>
```

For example, to set the **PreferredDataLocation** value to the European Union (EUR) geo for the user michelle@contoso.onmicrosoft.com, get the UserID value from the last command output and run the following command:

```
PowerShell
```

```
Update-MgUser -UserID michelle@contoso.onmicrosoft.com -  
PreferredDataLocation EUR
```

① Note

- As mentioned previously, you cannot use this procedure for synchronized user objects from on-premises Active Directory. You need to change the **PreferredDataLocation** value in Active Directory and synchronize it using Microsoft Entra Connect. For more information, see [Azure Active Directory Connect sync: Configure preferred data location for Microsoft 365 resources](#).

- How long it takes to relocate a mailbox to a new geo location depends on several factors:
 - The size and type of mailbox.
 - The number of mailboxes being moved.
 - The availability of move resources.

Move an inactive mailbox to a specific *Geography*

You can't move inactive mailboxes that are preserved for compliance purposes (for example, mailboxes on Litigation Hold) by changing their **PreferredDataLocation** value. To move an inactive mailbox to a different *Geography*, do the following steps:

1. Recover the inactive mailbox. For instructions, see [Recover an inactive mailbox](#).
2. Prevent the Managed Folder Assistant from processing the recovered mailbox by replacing <MailboxIdentity> with the name, alias, account, or email address of the mailbox and running the following command in [Exchange Online PowerShell](#):

PowerShell

```
Set-Mailbox <MailboxIdentity> -ElcProcessingDisabled $true
```

1. Assign an **Exchange Online Plan 2** license to the recovered mailbox. This step is required to place the mailbox back on Litigation Hold. For instructions, see [Assign licenses to users](#).
2. Configure the **PreferredDataLocation** value on the mailbox as described in the previous section.
3. After you confirm the mailbox moves to the new geo location, place the recovered mailbox back on Litigation Hold. For instructions, see [Place a mailbox on Litigation Hold](#).
4. After verifying that the Litigation Hold is in place, allow the Managed Folder Assistant to process the mailbox again by replacing <MailboxIdentity> with the name, alias, account, or email address of the mailbox and running the following command in [Exchange Online PowerShell](#):

PowerShell

```
Set-Mailbox <MailboxIdentity> -ElcProcessingDisabled $false
```

1. Make the mailbox inactive again by removing the user account associated with the mailbox. For instructions, see [Delete a user from your organization](#). This step also releases the Exchange Online Plan 2 license for other uses.

Note: When you move an inactive mailbox to a different geo location, you might affect content search results or the ability to search the mailbox from the former geo location. For more information, see [Searching and exporting content in Multi-Geo environments](#).

Create new cloud mailboxes in a specific *Geography* location

To create a new mailbox in a specific *Geographic* location, you need to do either of these steps:

- Configure the **PreferredDataLocation** value as described in the previous [Move an existing cloud-only mailbox to a specific *Geographic* location](#) section before you create the mailbox in Exchange Online. For example, configure the **PreferredDataLocation** value on a user before you assign a license.
- Assign a license at the same time you set the **PreferredDataLocation** value.

To create a new cloud-only licensed user (not Microsoft Entra Connect synchronized) in a specific *Geographic* location, use the following syntax in Microsoft Graph PowerShell:

PowerShell

```
$params = @{
    accountEnabled = $true
    displayName = "<display name>"
    mailNickname = "<mailbox name>"
    userPrincipalName = "<sign-in name>"
    usageLocation = "<ISO 3166-1 alpha-2 country code>"
    passwordProfile = @{
        forceChangePasswordNextSignIn = $true
        password = "<temp password>"
    }
}

$user = New-MgUser -BodyParameter $params

$EmsSku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq '<license SKU ID>'

Set-MgUserLicense -UserId $user.Id -AddLicenses @{$skuId = $EmsSku.SkuId} -
RemoveLicenses @()
```

💡 Tip

The `usageLocation` is A two-letter country code (ISO standard 3166). Required for users that are assigned licenses due to legal requirements to check for availability of services in countries. Examples include: US, JP, and GB.

This example creates a new user account for Elizabeth Brunner with the following values:

- User principal name: ebrunner@contoso.onmicrosoft.com
- First name: Elizabeth
- Last name: Brunner
- Display name: Elizabeth Brunner
- Password: Manually add password in the form of a hashtable
- License: `contoso:ENTERPRISEPREMIUM` (E5)
- Location: Australia (AU)

First, [connect to your Microsoft 365 tenant](#) using Microsoft Graph Powershell.

After you connect, use the following syntax to create an individual account:

PowerShell

```
$params = @{
    accountEnabled = $true
    displayName = "Elizabeth Brunner"
    mailNickname = "ElizabethB"
    userPrincipalName = "ebrunner@contoso.onmicrosoft.com"
    usageLocation = "AU"
    passwordProfile = @{
        forceChangePasswordNextSignIn = $true
        password = "xWwvJ]6NMw+bWH-d"
    }
}

$user = New-MgUser -BodyParameter $params

$EmsSku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq
'ENTERPRISEPREMIUM'
Set-MgUserLicense -UserId $user.Id -AddLicenses @{}{SkuId = $EmsSku.SkuId} -
RemoveLicenses @()
```

For more information about creating new user accounts and finding `LicenseAssignment` values in Azure AD PowerShell, see [Create user accounts with PowerShell](#) and [View licenses and services with PowerShell](#).

Note

If you are using Exchange Online PowerShell to enable a mailbox and need the mailbox to be created directly in the *Geographic* location that's specified in **PreferredDataLocation**, you need to use an Exchange Online cmdlet such as **Enable-Mailbox** or **New-Mailbox** directly against the cloud service. If you use the **Enable-RemoteMailbox** cmdlet in on-premises Exchange PowerShell, the mailbox will be created in the *Primary Provisioned Geography* location.

Onboard existing on-premises mailboxes in a specific *Geography* location

You can use the standard onboarding tools and processes to migrate a mailbox from an on-premises Exchange organization to Exchange Online, including the [Migration dashboard in the EAC](#), and the [New-MigrationBatch](#) cmdlet in Exchange Online PowerShell.

The first step is to verify a user object exists for each mailbox to be onboarded, and verify the correct **PreferredDataLocation** value is configured in Microsoft Entra ID. The onboarding tools respect the **PreferredDataLocation** value and migrate the mailboxes directly to the specified geo location.

Or, you can use the following steps to onboard mailboxes directly in a specific *Geographic* location using the [New-MoveRequest](#) cmdlet in Exchange Online PowerShell.

1. Verify the user object exists for each mailbox to be onboarded and that **PreferredDataLocation** is set to the desired value in Microsoft Entra ID. The value of **PreferredDataLocation** will be synchronized to the **MailboxRegion** attribute of the corresponding mail user object in Exchange Online.
2. Connect directly to the specific *Satellite Geography* location using the connection instructions from earlier in this article.
3. In Exchange Online PowerShell, store the on-premises administrator credentials used to perform a mailbox migration in a variable by running the following command:

PowerShell

```
$RC = Get-Credential
```

1. In Exchange Online PowerShell, create a new **New-MoveRequest** similar to the following example:

```
PowerShell
```

```
New-MoveRequest -Remote -RemoteHostName mail.contoso.com -RemoteCredential  
$RC -Identity user@contoso.com -TargetDeliveryDomain <YourAppropriateDomain>
```

1. Repeat step #4 for every mailbox you need to migrate from on-premises Exchange to the satellite geo location you're currently connected to.
2. If you need to migrate other mailboxes to different satellite geo locations, repeat steps 2 through 4 for each specific location.

Multi-Geo reporting

 **Note**

The multi-geo reporting feature is currently in Preview, is not available in all organizations, and is subject to change.

Multi-Geo Usage Reports in the Microsoft 365 admin center displays the user count by *Geographic* location. The report displays user distribution for the current month and provides historical data for the past six months.

Migration

Because it takes time to move each user to the new datacenter *Geography* for a single tenant, some users will be in the old datacenter *Geography* during the move, while others are in the new datacenter *Geography*. This means that some features that involve accessing multiple mailboxes might not fully work during a period of the move process, which can last weeks. These features are described in the following sections.

Open "Shared Folder" in Outlook Web Access

Some users open a shared mail folder from another mailbox (that the user has read or write permissions to) in Outlook Web Access using the "Shared Folder" feature. The following table describes how access to shared folders works during a mailbox move. Note that users with full permissions to a shared mailbox can open the mailbox by using Outlook Web Access during the move.

Configuration	Description
User has mailbox folder permission to another mailbox	Potentially limited. If User A and Mailbox B aren't in the same <i>Geography</i> during the tenant move, User A can't open Mailbox B's folder in Outlook Web Access if User A only has permission to a specific folder in Mailbox B. To add a shared folder, right-click the user name in the left navigation panel and select Add shared folder .
User with full mailbox permission to another mailbox	Fully supported. If User A has <i>Full Access</i> permission to Mailbox B, then User A can select the shared folder in the left navigation panel in Outlook Web Access to open a window showing Mailbox B. A user can open a shared mailbox using Outlook Web Access during the move without any adverse effect. The limitation only applies to folder-level sharing in a mailbox.

The process of email data migration to Microsoft 365 during the Exchange Online is a common scenario and is supported. Cloud migration between datacenter geos doesn't interfere with any on-premises to cloud mailbox migrations.

How can I determine customer data location?

You can find the actual data location in Tenant Admin Center. As a tenant administrator you can find the actual data location, for committed data, by navigating to **Admin->Settings->Org Settings->Organization Profile->Data Location**.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Data Residency for SharePoint and OneDrive

Article • 02/29/2024

Data Residency Commitments Available

Product Terms

Required Conditions:

- *Tenant* has a sign-up country/region included in *Local Region Geography*, the European Union or the United States.

Commitment:

For current language, refer to the [Privacy and Security Product Terms](#) and view the section titled "Location of Customer Data at Rest for Core Online Services."

Advanced Data Residency add-on

Required Conditions:

1. *Tenant* has a sign-up country/region included in *Local Region Geography* or *Expanded Local Region Geography*.
2. *Tenant* has a valid Advanced Data Residency subscription for all users in the *Tenant*.
3. The SharePoint subscription customer data is provisioned in *Local Region Geography* or *Expanded Local Region Geography*.

Commitment:

Refer to the [ADR Commitment page](#) for the specific customer data at rest commitment for SharePoint and OneDrive.

Multi-Geo add-on

Required Conditions:

1. *Tenants* have a valid Multi-Geo subscription that covers all users assigned to a *Satellite Geography*.
2. Customer must have an active Enterprise Agreement.

3. Total purchased Multi-Geo units must be greater than 5% of the total eligible licenses in the *Tenant*.

Commitment:

Customers can assign users of SharePoint/OneDrive to any *Satellite Geography* supported by Multi-Geo (see Section 4.1.3). The following customer data will be stored in the relevant *Satellite Geography*:

- SharePoint site content and the files stored within that site, and files uploaded to OneDrive.

Migration with Advanced Data Residency

When SharePoint is moved, data for the following services is also moved:

- OneDrive
- Microsoft 365 Video services
- Office in a browser
- Microsoft 365 Apps for enterprise
- Visio Pro for Microsoft 365

After we've completed moving your SharePoint data, you might see some of the following effects.

Microsoft 365 Video Services

- The data move for video takes longer than the moves for the rest of your content in SharePoint.
- After the SharePoint content is moved, there will be a time frame when videos aren't able to be played.
- We're removing the trans-coded copies from the previous datacenter and transcoding them again in the new datacenter.

Search

In the course of moving your SharePoint data, we migrate your search index and search settings to a new location. Until we've **completed** the move of your SharePoint data, we continue to serve your users from the index in the original location. In the new location, search automatically starts crawling your content after we've completed moving your SharePoint data. From this point and onwards, we serve your users from the migrated index. Changes to your content that occurred after the migration aren't included in the

migrated index until crawling picks them up. Most customers don't notice that results are less fresh right after we've completed moving their SharePoint data, but some customers might experience reduced freshness in the first 24-48 hours.

The following search features are affected:

- Search results and Search Web Parts: Results don't include changes that occurred after the migration until crawling picks them up.
- Delve: Delve doesn't include changes that occurred after the migration until crawling picks them up.
- Popularity and Search Reports for the site: Counts for Excel reports in the new location only include migrated counts and counts from usage reports that have run after we completed moving your SharePoint data. Any counts from the interim period are lost and can't be recovered. This period is typically a couple of days. Some customers might experience shorter or longer losses.
- Video Portal: View counts and statistics for the Video Portal depend on the statistics for Excel Reports, so view counts and statistics for the Video Portal are lost for the same time period as for the Excel reports.
- eDiscovery: Items that changed during the migration aren't shown until crawling picks up the changes.
- Data Loss Protection (DLP): Policies aren't enforced on items that change until crawling picks up the changes.

As part of the migration, the *Primary Provisioned Geography* changes and all new content will be stored at rest in the new *Primary Provisioned Geography*. Existing content will move in the background with no impact to you for up to 90 days after the first change to the SharePoint data location in the admin center.

SharePoint 2013 workflow

As part of our ongoing efforts to modernize SharePoint workflow capabilities, we have previously announced the [retirement plan of SharePoint 2013 workflow service](#). In alignment with this plan, SharePoint 2013 workflow will not be available in the new local regions of Mexico and Spain, or in any future local regions that we may launch. This means that if you migrate your SharePoint data to a new region, you will not be able to use SharePoint 2013 workflow for your business processes and scenarios.

Refer to the link above for more information about the retirement plan and the alternatives for SharePoint workflow. If you have any questions or concerns, please contact Microsoft support.

Multi-Geo Capabilities in SharePoint / OneDrive

Multi-Geo capabilities in OneDrive and SharePoint enable control of shared resources like SharePoint team sites and Microsoft 365 group mailboxes stored at rest in a specified *Macro Region Geography* or *Local Region Geography*.

Each user, Group mailbox, and SharePoint site have a Preferred Data Location (PDL) which denotes the *Macro Region Geography* or *Local Region Geography* (location where related data is to be stored). Users' personal data (Exchange mailbox and OneDrive) along with any Microsoft 365 Groups or SharePoint sites that they create can be stored in the specified *Macro Region Geography* or *Local Region Geographies* location to meet data residency requirements. You can specify different administrators for each *Macro Region Geography* or *Local Region Geographies* location.

Users get a seamless experience when using Microsoft 365 services, including Office applications, OneDrive, and Search. See User experience in a Multi-Geo environment for details.

① Note

Once your tenant has enabled the Multi-Geo add-on, changing the default location for the tenant is not supported. This applies even for the [Data Residency Legacy Move Program](#) and the Advanced Data Residency add-on.

OneDrive

Each user's OneDrive can be provisioned in or moved by an administrator to a *Satellite Geography* location in accordance with the user's PDL. Personal files are then kept in that *Satellite Geography* location, though they can be shared with users in other *Macro Region Geography* or *Local Region Geography* locations.

SharePoint Sites and Groups

Management of the Multi-Geo feature is available through the SharePoint admin center.

When a user creates a SharePoint group-connected site in a multi-geo environment, their PDL is used to determine the *Macro Region Geography* or *Local Region Geography* location where the site and its associated Group mailbox are created. (If the user's PDL value isn't set, or is set to *Macro Region Geography* or *Local Region Geography* location that isn't configured as a *Satellite Geography* location, then the site and mailbox are created in the *Primary Provisioned Geography*.)

Microsoft 365 services other than Exchange, OneDrive, SharePoint, and Teams aren't available with Multi-Geo. However, Microsoft 365 Groups that are created by these services are configured with the PDL of the creator and their Exchange Group mailbox, SharePoint site are provisioned in the corresponding *Macro Region Geography* or *Local Region Geography*.

Managing the Multi-Geo environment

Setting up and managing your Multi-Geo environment is done through the SharePoint admin center.

SharePoint storage quotas in multi-geo environments

By default, all *Geography* locations of a multi-geo environment share the available *Tenant* storage quota.

With the SharePoint geo storage quota setting, you can manage the storage quota for each *Geography* location. When you allocate a storage quota for a *Geography* location, it becomes the maximum amount of storage available for that *Geography* location, and is deducted from the available *Tenant* storage quota. The remaining available *Tenant* storage quota is then shared across the configured *Geography* locations for which a specific storage quota hasn't been allocated.

The SharePoint storage quota for any *Geography* location can be allocated by the SharePoint administrator by connecting to the *Primary Provisioned Geography*. *Geography* administrators for *Satellite Geography* locations can view the storage quota but can't allocate it.

Configure a storage quota for a *Geography* location

Use the [Microsoft SharePoint Management Shell](#) and connect to the *Primary Provisioned Geography* location to allocate the storage quota for a *Geography* location.

To allocate Storage Quota for a location, run cmdlet:

PowerShell

```
Set-SPOGeoStorageQuota -GeoLocation <geolocationcode> -StorageQuotaMB  
<value>
```

To view Storage Quota for the current *Geography* location, run:

```
PowerShell
```

```
Get-SPOGeoStorageQuota
```

To view Storage Quota for all *Geography* locations, run:

```
PowerShell
```

```
Get-SPOGeoStorageQuota -AllLocations
```

To remove the allocated storage quota for a *Geography* location, set `StorageQuota value = 0`:

```
PowerShell
```

```
Set-SPOGeoStorageQuota -GeoLocation <geolocationcode> -StorageQuotaMB 0
```

Move a OneDrive site

Move a OneDrive site to a different *Geography* location

With OneDrive *Geography* move, you can move a user's OneDrive to a different *Geography* location. OneDrive *Geography* move is performed by the SharePoint administrator. Before you start a OneDrive *Geography* move, be sure to notify the user whose OneDrive is being moved and recommend they close all files for the duration of the move. (If the user has a document open using the Office client during the move, then upon move completion the document will need to be saved to the new location.) The move can be scheduled for a future time, if desired.

The OneDrive service uses Azure Blob Storage to store content. The Storage blob associated with the user's OneDrive is moved from the source to destination *Geography* location within 40 days of destination OneDrive being available to the user. The access to the user's OneDrive is restored as soon as the destination OneDrive is available.

During OneDrive *Geography* move window (about 2-6 hours) the user's OneDrive is set to read-only. The user can still access their files via the OneDrive sync app or their OneDrive site in SharePoint. After OneDrive *Geography* move is complete, the user will be automatically connected to their OneDrive at the destination *Geography* location when they navigate to OneDrive in the Microsoft 365 app launcher. The sync app will automatically begin syncing from the new location.

The procedures in this article require the [Microsoft SharePoint PowerShell Module](#).

Communicating to your users

When moving OneDrive sites between *Geography* locations, it's important to communicate to your users what to expect. This can help reduce user confusion and calls to your help desk. Email your users before the move and let them know the following information:

- When the move is expected to start and how long it's expected to take
- What *Geography* location their OneDrive is moving to, and the URL to access the new location
- They should close their files and not make edits during the move.
- File permissions and sharing won't change as a result of the move.
- What to expect from the user experience in a multi-geo environment

Be sure to send your users an email when the move completes, informing them that they can resume working in OneDrive.

Scheduling OneDrive site moves

You can schedule OneDrive site moves in advance (described later in this article). We recommend that you start with a small number of users to validate your workflows and communication strategies. Once you're comfortable with the process, you can schedule moves as follows:

- You can schedule up to 4,000 moves at a time.
- As the moves begin, you can schedule more, with a maximum of 4,000 pending moves in the queue and any given time.
- The maximum size of a OneDrive that can be moved is 5 terabytes (5 TB).
- The count of list items for the site is < 1 million.

Moving a OneDrive site

To perform a OneDrive *Geography* move, the *Tenant* administrator must first set the user's Preferred Data Location (PDL) to the appropriate *Geography* location. Once the PDL is set, wait for at least 24 hours for the PDL update to sync across the *Geography* locations before starting the OneDrive *Geography* move.

When using the *Geography* move cmdlets, connect to SPO Service at the user's current OneDrive *Geography* location, using the following syntax:

PowerShell

```
Connect-SPOService -url https://<tenantName>-admin.sharepoint.com
```

For example: To move OneDrive of user 'Matt@contosoenergy.onmicrosoft.com', connect to EUR SharePoint Admin center as the user's OneDrive is in EUR *Geography* location:

PowerShell

```
Connect-SPOService -url https://contosoenergyeur-admin.sharepoint.com
```

Validating the environment

Before you start a OneDrive *Geography* move, we recommend that you validate the environment.

To ensure that all *Geography* locations are compatible, run:

PowerShell

```
Get-SPOGeoMoveCrossCompatibilityStatus
```

You'll see a list of your *Geography* locations and whether content can be moved between will be denoted as "Compatible". If the command returns "Incompatible" please retry validating the status at a later date.

If a OneDrive contains a subsite, for example, it can't be moved. You can use the `Start-SPOUserAndContentMove` cmdlet with the `-ValidationOnly` parameter to validate if the OneDrive is able to be moved:

PowerShell

```
Start-SPOUserAndContentMove -UserPrincipalName <UPN> -  
DestinationDataLocation <DestinationDataLocation> -ValidationOnly
```

This will return Success if the OneDrive is ready to be moved or Fail if there's a legal hold or subsite that would prevent the move. Once you have validated that the OneDrive is ready to move, you can start the move.

Start a OneDrive geo move

To start the move, run:

PowerShell

```
Start-SPOUserAndContentMove -UserPrincipalName <UserPrincipalName> -  
DestinationDataLocation <DestinationDataLocation>
```

Using these parameters:

- *UserPrincipalName* – UPN of the user whose OneDrive is being moved.
- *DestinationDataLocation* – Geo-Location where the OneDrive needs to be moved.
This should be same as the user's preferred data location.

For example, to move the OneDrive of matt@contosoenergy.onmicrosoft.com from EUR to AUS, run:

PowerShell

```
Start-SPOUserAndContentMove -UserPrincipalName  
matt@contosoenergy.onmicrosoft.com -DestinationDataLocation AUS
```

To schedule a *Geography* move for a later time, use one of the following parameters:

- *PreferredMoveBeginDate* – The move will likely begin at this specified time. Time must be specified in Coordinated Universal Time (UTC).
- *PreferredMoveEndDate* – The move will likely be completed by this specified time, on a best effort basis. Time must be specified in Coordinated Universal Time (UTC).

Cancel a OneDrive *Geography* move

You can stop the *Geography* move of a user's OneDrive, provided the move isn't in progress or completed by using the cmdlet:

PowerShell

```
Stop-SPOUserAndContentMove -UserPrincipalName <UserPrincipalName>
```

Where *UserPrincipalName* is the UPN of the user whose OneDrive move you want to stop.

Determining current status

You can check the status of a OneDrive *Geography* move in or out of the *Geography* that you're connected to by using the Get-SPOUserAndContentMoveState cmdlet.

The move statuses are described in the following table.

[+] Expand table

Status	Description
NotStarted	The move hasn't started
InProgress (n/4)	The move is in progress in one of the following states: <ul style="list-style-type: none">• Validation (1/4)• Backup (2/4)• Restore (3/4)• Cleanup (4/4)
Success	The move completed successfully.
Failed	The move failed.

To find the status of a specific user's move, use the *UserPrincipalName* parameter:

PowerShell

```
Get-SPOUserAndContentMoveState -UserPrincipalName <UPN>
```

To find the status of all of the moves in or out of the *Geography* location that you're connected to, use the *MoveState* parameter with one of the following values:

NotStarted, InProgress, Success, Failed, All.

PowerShell

```
Get-SPOUserAndContentMoveState -MoveState <value>
```

You can also add the *Verbose* parameter for more verbose descriptions of the move state.

User Experience

Users of OneDrive should notice minimal disruption if their OneDrive is moved to a different *Geography* location. Aside from a brief read-only state during the move, existing links and permissions continue to work as expected once the move is completed.

User's OneDrive

While the move is in progress, the user's OneDrive is set to read-only. Once the move is completed, the user is directed to their OneDrive in the new *Geography* location when they navigate to OneDrive the Microsoft 365 app launcher or a web browser.

Permissions on OneDrive content

Users with permissions to OneDrive content continue to have access to the content during the move and after it's complete.

OneDrive sync app

The OneDrive sync app automatically detects and seamlessly transfers syncing to the new OneDrive location once the OneDrive *Geography* move is complete. The user doesn't need to sign-in again or take any other action. (Version 17.3.6943.0625 or later of the sync app required.) If a user updates a file while the OneDrive *Geography* move is in progress, the sync app notifies them that file uploads are pending while the move is underway.

Sharing links

Upon OneDrive *Geography* move completion, the existing shared links for the files that were moved automatically redirect to the new *Geography* location.

OneNote Experience

OneNote Win32 client and UWP (Universal) App automatically detects and seamlessly syncs notebooks to the new OneDrive location once OneDrive *Geography* move is complete. The user doesn't need to sign-in again or take any other action. The only visible indicator to the user is notebook sync would fail when OneDrive *Geography* move is in progress. This experience is available on the following OneNote client versions:

- OneNote Win32 – Version 16.0.8326.2096 (and later)
- OneNote UWP – Version 16.0.8431.1006 (and later)
- OneNote Mobile App – Version 16.0.8431.1011 (and later)

Teams app

Upon OneDrive *Geography* move completion, users have access to their OneDrive files on the Teams app. Additionally, files shared via Teams chat from their OneDrive before the *Geography* move continue to work after move is complete.

OneDrive Mobile App (iOS)

Upon OneDrive *Geography* move completion, the user would need to sign out and sign in again on the iOS Mobile App to sync to the new OneDrive location.

Existing followed groups and sites

Followed sites and groups show up in the user's OneDrive regardless of their *Geography* location. Sites and groups hosted in another *Geography* location will open in a separate tab.

Delve Geo URL updates

Users are sent to the Delve *Geography* corresponding to their PDL only after their OneDrive has been moved to the new *Geography*.

Move a SharePoint site or SharePoint Embedded container site

Move a SharePoint site or SharePoint Embedded container site to a different *Geography* location

With SharePoint site *Geography* move, you can move SharePoint sites and SharePoint Embedded container sites to other *Geography* locations within your Multi-Geo environment. The following types of site can be moved between *Geography* locations:

- Microsoft 365 group-connected sites, including those sites associated with Microsoft Teams
- Modern sites without a Microsoft 365 group association
- Classic SharePoint sites
- Communication sites
- SharePoint Embedded container sites (excluding those where the owner is a group)

Note

You must be a SharePoint Administrator to move a site between *Geography* locations.

There's a read-only window during the SharePoint site *Geography* move of approximately 4-6 hours, depending on site contents.

Best practices

- Try a SharePoint site move on a test site to get familiar with the procedure.
- Validate whether the site can be moved before scheduling or performing the move.
- When possible schedule cross-geo sites moves for outside business hours to reduce user impact.
- Communicate with impacted users before the sites move.

Communicating to your users

When moving SharePoint sites between *Geography* locations, it's important to communicate to the sites' users (generally anyone with the ability to edit the site) what to expect. This can help reduce user confusion and calls to your help desk. Email your sites' users before the move and let them know the following information:

- When the move is expected to start and how long it is expected to take.
- What *Geography* location their site is moving to, and the URL to access the new location.
- They should close their files and not make edits during the move.
- File permissions and sharing won't change because of the move.
- What to expect from the user experience in a multi-geo environment.

Be sure to send your sites' users an email when the move completes, informing them that they can resume working on their sites.

Scheduling SharePoint site moves

You can schedule SharePoint site moves in advance (described later in this article). You can schedule moves as follows:

- You can schedule up to 4,000 moves at a time.
- As the moves begin, you can schedule more, with a maximum of 4,000 pending moves in the queue and any given time.
- The maximum size of a SharePoint site that can be moved is 5 terabytes (5 TB).
- The count of list items for the site is < 1 million.

To schedule a SharePoint site *Geography* move for a later time, include one of the following parameters when you start the move:

- PreferredMoveBeginDate – The move will likely begin at this specified time.
- PreferredMoveEndDate – The move will likely be completed by this specified time, on a best effort basis.

Time must be specified in Coordinated Universal Time (UTC) for both parameters.

Moving the site

SharePoint site *Geography* move requires that you connect and perform the move from the SharePoint Admin URL in the *Geography* location where the site is.

For example, if the site URL is

`https://contosohealthcare.sharepoint.com/sites/Turbines`, connect to the SharePoint Admin URL at `https://contosohealthcare-admin.sharepoint.com`:

PowerShell

```
Connect-SPOService -Url https://contosohealthcare-admin.sharepoint.com
```

Validating the environment

We recommend that before scheduling any site move, you perform a validation to ensure that the site can be moved.

We don't support moving sites with:

- Business Connectivity Services
- InfoPath forms
- Information Rights Management (IRM) templates applied

 **Note**

Sites archived with Microsoft 365 Archive need to be reactivated before being moved. Archiving sites while a move is in progress is not supported.

To ensure all *Geography* locations are compatible, run `Get-SPOGeoMoveCrossCompatibilityStatus`. This will display all your *Geography* locations and whether the environment is compatible with the destination *Geography* location.

To perform a validation-only check on your site, use `Start-SPOSiteContentMove` with the `-ValidationOnly` parameter to validate if the site is able to be moved. For example:

PowerShell

```
Start-SPOSiteContentMove -SourceSiteUrl <SourceSiteUrl> -ValidationOnly -DestinationDataLocation <DestinationLocation>
```

This returns *Success* if the site is ready to be moved or *Fail* if any of blocked conditions are present.

Start a SharePoint site *Geography* move for a site with no associated Microsoft 365 group or a SharePoint Embedded container site

By default, initial URL for the site will change to the URL of the destination *Geography* location. For example:

```
https://Contoso.sharepoint.com/sites/projectx to
```

```
https://ContosoEUR.sharepoint.com/sites/projectx
```

For sites with no Microsoft 365 group association, you can also rename the site by using the `-DestinationUrl` parameter. For example:

```
https://Contoso.sharepoint.com/sites/projectx to
```

```
https://ContosoEUR.sharepoint.com/sites/projecty
```

This capability to rename the site as part of the move is not applicable for SharePoint Embedded container sites.

To start the site move without renaming the site, run:

```
PowerShell
```

```
Start-SPOSiteContentMove -SourceSiteUrl <siteURL> -DestinationDataLocation  
<DestinationDataLocation>
```

To get the `SourceSiteUrl` for a SharePoint Embedded container site, you must use the SharePoint Embedded admin cmdlets. You can use the `Get-SPOContainer` PowerShell cmdlet and pass the container ID as the `-Identity` parameter to determine the site URL of a specific container.

If the SharePoint Embedded container site is owned by an individual user, the container site can only be moved to the geography matching the Preferred Data Location (PDL) of the user.

And to start the site move while also renaming the site (excluding SharePoint Embedded container sites), run:

```
PowerShell
```

```
Start-SPOSiteContentMove -SourceSiteUrl <siteURL> -DestinationUrl  
<DestinationSiteURL>
```

You cannot use the `-DestinationDataLocation` and `-DestinationUrl` parameters in the same command.

Start a SharePoint site *Geography* move for a Microsoft 365 group-connected site

To move a Microsoft 365 group-connected site, the SharePoint Administrator must first change the Preferred Data Location (PDL) attribute for the Microsoft 365 group.

To set the PDL for a Microsoft 365 group:

PowerShell

```
Set-SPOUnifiedGroup -PreferredDataLocation <PDL> -GroupAlias <GroupAlias>  
Get-SPOUnifiedGroup -GroupAlias <GroupAlias>
```

Once you update the PDL, you can start the site move:

PowerShell

```
Start-SPOUnifiedGroupMove -GroupAlias <GroupAlias> -DestinationDataLocation  
<DestinationDataLocation>
```

Cancel a SharePoint site *Geography* move

You can stop a SharePoint site *Geography* move, provided the move isn't in progress or completed by using the `Stop-SPOSiteContentMove` cmdlet.

Determining the status of a SharePoint site *Geography* move

You can determine the status of a site move in our out of the *Geography* that you're connected to by using the following cmdlets:

- `Get-SPOSiteContentMoveState` (non-Group-connected sites and SharePoint Embedded container sites)
- `Get-SPOUnifiedGroupMoveState` (Group-connected sites)

Use the `-SourceSiteUrl` parameter to specify the site for which you want to see move status.

The move statuses are described in the following table.

[\[+\] Expand table](#)

Status	Description
Ready to Trigger	The move hasn't started.
Scheduled	The move is in queue but hasn't yet started.
InProgress (n/4)	The move is in progress in one of the following states: Validation (1/4), Back up (2/4), Restore (3/4), Cleanup (4/4).
Success	The move completed successfully.
Failed	The move failed.

You can also apply the `-Verbose` option to see additional information about the move.

User experience

Site users should notice minimal disruption when their site is moved to a different *Geography* location. Aside from a brief read-only state during the move, existing links and permissions continue to work as expected once the move is completed.

Site

While the move is in progress, the site is set to read-only. Once the move is completed, the user is directed to the new site in the new *Geography* location when they click on bookmarks or other links to the site.

Permissions

Users with permissions to site continue to have access to the site during the move and after it's complete.

Sync app

The sync app automatically detects and seamlessly transfers syncing to the new site location once the site move is complete. The user doesn't need to sign in again or take any other action. (Version 17.3.6943.0625 or later of the sync app required.) If a user

updates a file while the move is in progress, the sync app notifies them that file uploads are pending while the move is underway.

Sharing links

When the SharePoint site *Geography* move completes, the existing shared links for the files that were moved automatically redirect to the new *Geography* location.

Most Recently Used files in Office (MRU)

The MRU service is updated with the site url and its content URLs once the move completes. This applies to Word, Excel, and PowerPoint.

OneNote experience

OneNote Win32 client and UWP (Universal) App automatically detects and seamlessly syncs notebooks to the new site location once site move is complete. The user doesn't need to sign in again or take any other action. The only visible indicator to the user is notebook sync would fail when site move is in progress. This experience is available on the following OneNote client versions:

- OneNote Win32 – Version 16.0.8326.2096 (and later)
- OneNote UWP – Version 16.0.8431.1006 (and later)
- OneNote Mobile App – Version 16.0.8431.1011 (and later)

Teams (applicable to Microsoft 365 group connected sites)

When the SharePoint site *Geography* move completes, users will have access to their Microsoft 365 group site files on the Teams app. Additionally, files shared via Teams chat from their site prior to *Geography* move will continue to work after move is complete. SharePoint site *Geography* move doesn't support moving sites backing Private and Shared Channels from one *Geography* to another, when using the `Start-SPOUnifiedGroupMove` command. Sites backing Private and Shared Channels remain in the original *Geography*. To move those sites individually, admins can initiate direct moves using the `Start-SPOSiteContentMove` command.

SharePoint Mobile App (iOS/Android)

The SharePoint Mobile App is cross *Geography* compatible and able to detect the site's new *Geography* location.

SharePoint workflows

SharePoint 2013 workflows have to be republished after the site move. SharePoint 2010 workflows should continue to function normally.

Apps

If you're moving a site with apps, you must reinstantiate the app in the site's new *Geography* location as the app and its connections may not be available in the destination *Geography* location.

Power Automate

In most cases, Power Automate Flows continue to work after a SharePoint site *Geography* move. We recommend that you test them once the move completes.

Power Apps

Power Apps need to be recreated in the destination location.

Data movement between geo locations

SharePoint uses Azure Blob Storage for its content, while the metadata associated with sites and its files is stored within SharePoint. After the site is moved from its source *Geography* location to its destination *Geography* location, the service will also move its associated Blob Storage. Blob Storage moves complete in approximately 40 days. This won't have any impact to users interaction with the data.

Enabling SharePoint Multi-Geo in your *Satellite Geography* location

This article is for Global or SharePoint administrators who have created a Multi-Geo *Satellite Geography* location **before** SharePoint Multi-Geo capabilities became generally available on March 27, 2019, and who haven't enabled SharePoint Multi-Geo in their *Satellite Geography* location(s).

ⓘ Note

If you have added a new *Geography* location **after** March 27th, 2019, you don't need to perform these instructions, as your new *Geography* location will already be

enabled for OneDrive and SharePoint Multi-Geo.

These instructions allow you to enable SharePoint in your *Satellite Geography* location, so your Multi-Geo satellite users can take advantage of both OneDrive and SharePoint Multi-Geo capabilities in Microsoft 365.

Important

Please note that this is a one way enablement. Once you set SPO mode, you will not be able to revert your *Tenant* to OneDrive only Multi-Geo mode without an escalation with support.

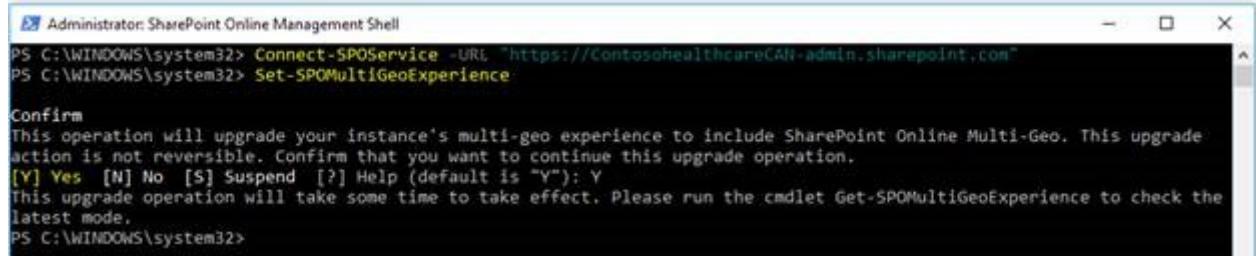
To set a *Geography* location into SPO Mode

To set a *Geography* location into SPO mode, connect to the *Geography* location you want to set in SPO Mode:

1. Open your SharePoint Management Shell and then run and confirm the following code:

PowerShell

```
Connect-SPOSERVICE -URL "https://$tenantGeo-admin.sharepoint.com" -  
Credential $credential  
Set-SPOMultiGeoExperience
```



The screenshot shows a Windows Command Prompt window titled "Administrator: SharePoint Online Management Shell". The command "Set-SPOMultiGeoExperience" is being run. A confirmation dialog box is displayed, asking if the user wants to continue with the upgrade operation. The dialog includes options [Y] Yes, [N] No, [S] Suspend, and [?] Help. The default response is "Y". The message in the dialog states: "This operation will upgrade your instance's multi-geo experience to include SharePoint Online Multi-Geo. This upgrade action is not reversible. Confirm that you want to continue this upgrade operation." At the bottom of the dialog, it says: "This upgrade operation will take some time to take effect. Please run the cmdlet Get-SPOMultiGeoExperience to check the latest mode." The command prompt shows the path "PS C:\WINDOWS\system32>" and the results of the command execution.

This operation usually takes about an hour while we perform various publish backs in the service and restamp your *Tenant*. After at least 1 hour, please perform a Get-SPOMultiGeoExperience. This shows you whether this *Geography* location is in SPO mode.

```
PS C:\WINDOWS\system32> Get-SPOMultiGeoExperience  
>>  
GeoLocation MultiGeoExperienceMode  
-----  
CAN SPO  
  
PS C:\WINDOWS\system32>
```

ⓘ Note

Certain caches in the service update every 24 hours, so it is possible that for a period of up to 24 hours, your *Satellite Geography* may intermittently behave as if it was still in ODB mode. This doesn't cause any technical issues.

How can I determine customer data location?

You can find the actual data location in Microsoft 365 admin center. As a *Tenant* administrator you can find the actual data location, for committed data, by navigating to **Admin->Settings->Org Settings->Organization Profile->Data Location**. If you don't have a *Tenant* created, you can have a *Tenant* created when signing up for a Microsoft 365 trial.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Data Residency for Microsoft Teams

Article • 02/29/2024

Data Residency Commitments Available

Product Terms

Required Conditions:

1. *Tenant* has a sign-up country/region included in *Local Region Geography*, the European Union, or the United States.

Commitment:

For current language, please refer to the [Privacy and Security Product Terms](#) and view the section titled "Location of Customer Data at Rest for Core Online Services."

Advanced Data Residency add-on

Required Conditions:

1. *Tenant* has a sign-up country/region included in *Local Region Geography* or *Expanded Local Region Geography*.
2. *Tenant* has a valid Advanced Data Residency subscription for all users in the *Tenant*.
3. The Microsoft Teams subscription customer data is provisioned in *Local Region Geography* or *Expanded Local Region Geography*.

Commitment:

Refer to the [ADR Commitment page](#) to understand the specific commitments provided via Product Terms. Examples of the committed data include:

- Chat/ channel messages and team structure: Every team in Microsoft Teams is backed by a Microsoft 365 Modern Group and its SharePoint site and Exchange mailbox. Private chats (including group chats), messages sent as part of a conversation in a channel, and the structure of teams and channels are stored in an Azure powered chat service. The data is also stored in a hidden folder in the user and group mailboxes to enable information protection features.
- Images and Media: Media used in chats (except for Giphy GIFs which aren't stored but are a reference link to the original Giphy URL) are stored in an Azure based Media Service deployed to the same locations as the chat service.

- Meeting Recordings: For users of Microsoft Stream (on SharePoint) Meeting Recordings are stored in the OneDrive storage of the user that initiates the recording.

Multi-Geo add-on

Required Conditions:

1. *Tenants* have a valid Multi-Geo subscription that covers all users assigned to a *Satellite Geography*
2. Customer must have an active Enterprise Agreement.
3. Total purchased Multi-Geo units must be greater than 5% of the total eligible seats in the *Tenant*.

Commitment: Customers can assign users of Microsoft Teams to any *Satellite Geography* supported by Multi-Geo. The following customer data will be stored in the relevant *Satellite Geography*: Teams chat data that consists of chat messages, including private messages, channel messages, and images used in chats.

Multi-Geo Capabilities in Microsoft Teams

Multi-Geo capabilities in Teams enable Teams chat data to be stored at rest in a specified *Macro Region Geography* or *Local Region Geography* location. Chat data consists of chat messages, including private messages, channel messages, and images used in chats.

Teams uses the Preferred Data Location (PDL) for users and groups to determine where to store data. If the PDL isn't set or is invalid, data is stored in the tenant's *Primary Provisioned Geography* location.

Note

Multi-Geo capabilities in Teams rolled out in July 2021. Your chat and channel messages will be automatically migrated to the correct *Macro Region Geography* or *Local Region Geography* location over the next few quarters. Any new PDL changes will be processed after the *Tenant* has completed the initial sync, and new PDL changes beyond that will be queued and processed in the order they are received.

User chat

User chat includes one-to-one, one-to-many, and private meeting messages.

When a new user is created, Teams reads the user's PDL and stores all their chat data in that *Macro Region Geography* or *Local Region Geography* location. For existing users, if an administrator adds or modifies the PDL for a user, that user's chat data is added to a migration queue to be moved to the specified *Macro Region Geography* or *Local Region Geography* location.

The storage location for a one-to-one or one-to-many chat is based on the PDL of the person who created the chat. If that user's PDL is changed, the chat will be migrated to the new *Macro Region Geography* or *Local Region Geography* location. The storage location for a meeting chat is based on the PDL of the meeting organizer.

To find the current location of a user's Teams data, connect to Teams PowerShell and run the following command:

```
PowerShell
```

```
Get-MultiGeoRegion -EntityType User -EntityId <UPN>
```

Channel messages

Each Microsoft 365 group has a Preferred Data Location (PDL) which denotes the *Geography* location where related data is to be stored. Teams uses the PDL for the group associated with each team to determine where to store channel messaging data for that team. This includes private channels and chat that occurs within a channel meeting.

When a user creates a new team, that user's PDL determines what PDL is assigned to the Microsoft 365 group. The group PDL determines where that team's data is stored. If that user's PDL later changes, the group's PDL isn't changed.

For existing teams, if an administrator adds or modifies the PDL for the Microsoft 365 group that backs a team, that team's channel messaging data is added to a migration queue to be moved to the specified *Macro Region Geography* or *Local Region Geography* location.

Changing the PDL of the Microsoft 365 group queues the Teams data to migrate to the chosen *Macro Region Geography* or *Local Region Geography* location. However, this doesn't migrate the SharePoint site or files associated with the Group automatically. You must move the site separately by following the procedures in Move a SharePoint site to a different *Geography* location. Be sure to do both steps to avoid Teams data and SharePoint data for one group in different locations.

To find the current location of a team's data, connect to Teams PowerShell and run the following command:

PowerShell

```
Get-MultiGeoRegion -EntityType Group -EntityId <GroupObjectId>
```

User Experience

Teams Multi-Geo is seamless to the end user. Once you change the PDL of a user or a group, the respective data will queue for migration and the migration will occur automatically with no impact to the user or their Teams client even if they're active while the migration occurs.

Migration

Files Tab After the migration is complete the Files tab might take additional time (up to 7 seconds) to fully load when the user first attempts to use it.

Read-only period Teams chat services moves each thread individually. The thread is locked in a read-only state during the move, which lasts a few seconds per thread. Threads remain accessible during the migration.

In-scope for Migration In addition to Exchange Online, SharePoint, and OneDrive; Microsoft will migrate Teams data to the local datacenter.

- Teams chat messages, including private messages and channel messages.
- Teams images used in chats.

Teams files are stored in SharePoint and Teams chat files are stored in OneDrive. Voicemail, calendar, and contacts are stored in Exchange Online. In many cases, Exchange Online, SharePoint, and OneDrive are already used by the customer in the local datacenter *Geography* and are also part of the Microsoft 365 migration program for eligible customer countries/regions.

How can I determine customer data location?

You can find the actual data location in *Tenant Admin Center*. As a *Tenant* administrator you can find the actual data location, for committed data, by navigating to **Settings > Org settings > Organization profile > Data location**.

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Data Residency for Microsoft Copilot for Microsoft 365

Article • 07/26/2024

Overview

Service documentation: [Microsoft Copilot for Microsoft 365 overview](#) and [Data, Privacy, and Security for Microsoft Copilot for Microsoft 365](#)

Capability Summary: Microsoft Copilot for Microsoft 365 is an AI-powered productivity tool that coordinates large language models (LLMs), content in Microsoft Graph, and the Microsoft 365 apps that you use every day, such as Word, Excel, PowerPoint, Outlook, and Teams. This integration provides real-time intelligent assistance, enabling users to enhance their creativity, productivity, and skills. The following applications provide the ability to interact with Microsoft Copilot for Microsoft 365: Microsoft Word, Excel, PowerPoint, Loop, Outlook, Teams (Chat, Meetings, Calls, Whiteboard), and OneNote.

The content of interactions and the related semantic index with Microsoft Copilot for Microsoft 365 are stored at rest in the relevant *Local Region Geography*.

Data Residency Commitments Available for Microsoft Copilot for Microsoft 365

Product Terms

Required Conditions:

1. *Tenant* has a sign-up country/region included in Australia, Brazil, Canada, the European Union, France, Germany, India, Japan, Norway, Qatar, South Africa, South Korea, Sweden, Switzerland, the United Kingdom, the United Arab Emirates, or the United States.

Commitment:

For current language, refer to the [Privacy and Security Product Terms](#) and view the section titled "Location of Customer Data at Rest for Core Online Services."

Advanced Data Residency (ADR) add-on

Required Conditions:

1. *Tenant* has a sign-up country/region included in *Local Region Geography*.
2. *Tenant* has a valid Advanced Data Residency subscription for all users in the *Tenant*.
3. For existing *Tenant* that has data stored in a *Macro Region Geography*, the *Tenant* Global Admin must opt in to move the *Tenant* data into the *Local Region Geography*.
4. The Microsoft Copilot for Microsoft 365 subscription customer data is provisioned in *Local Region Geography*.

Commitment:

Refer to the [ADR Commitment page](#) to understand the specific data at rest commitments for Microsoft Copilot for Microsoft 365. Examples of the committed data include:

- "Content of Interactions" such as the user's prompt and Microsoft Copilot's response, including citations to any information used to ground Microsoft Copilot's response.

Multi-Geo add-on

Required Conditions:

1. *Tenants* have a valid Multi-Geo subscription that covers all users assigned to a *Satellite Geography*.
2. Customer must have an active Enterprise or CSP Partner Agreement.
3. Total purchased Multi-Geo units must be greater than 5% of the total eligible licenses in the *Tenant*.

Commitment: Multi-Geo capabilities in Microsoft Copilot for Microsoft 365 enable content of interactions with Microsoft Copilot for Microsoft 365 to be stored at rest in a specified *Macro Region Geography* or *Local Region Geography* location. Microsoft Copilot for Microsoft 365 uses the Preferred Data Location (PDL) for users and groups to determine where to store data. If the PDL isn't set or is invalid, data is stored in the *Tenant's Primary Provisioned Geography* location. The *Geography* where the content of interactions with Microsoft Copilot for Microsoft 365 are stored is determined by the PDL of the user interacting with Microsoft Copilot for Microsoft 365. This means that the storage of content of interactions for users in different regions will be based on their respective PDL configurations.

To find the current location of a user's content of interactions with Microsoft Copilot for Microsoft 365 by referencing the PDL configuration for that user. Refer to [Multi-Geo](#)

Testing

Illustrative examples

Collaboration Experience Two people are working together on a Microsoft Word document. User A authored the document and stored it in the OneDrive for Business personal storage site, which is located in France. User B is in Canada and asks Microsoft Copilot for Microsoft 365 to rewrite a paragraph in the document. The paragraph User B submitted as the prompt, as well as the rewrite options Microsoft Copilot for Microsoft 365 provides (the “content of interactions” in this case) are stored in Canada; the original document remains in France, as does any rewrite the user accepts into that document.

Teams Meeting Experience Microsoft Teams meeting recording video location is determined by the user PDL that starts the recording, or when meetings have an automatic recording policy, the location is determined from the first person joining the meeting. When users in other regions interact with Microsoft Copilot for Microsoft 365 in Teams, those user prompts and corresponding responses are stored in the location of the user that asks the Microsoft Copilot for Microsoft 365 questions.

Migration and User Experience

When a user interacts with Microsoft Copilot for Microsoft 365 (using apps such as Word, PowerPoint, Excel, OneNote, Loop, or Whiteboard), we store data about these interactions. The stored data includes the user's prompt and Copilot's response, including citations to any information used to ground Copilot's response. We refer to the user's prompt and Copilot's response to that prompt as the “content of interactions” and the record of those interactions is the user's Copilot interaction history. For example, this stored data provides users with Copilot interaction history in [Microsoft Copilot with Graph-grounded chat](#) and [meetings in Microsoft Teams](#). This data is processed and stored in alignment with contractual commitments with your organization's other content in Microsoft 365, such as [Advanced data residency in Microsoft 365](#).

When a customer elects [Advanced data residency in Microsoft 365](#), they are subject to [ADR Migration](#). For detailed information regarding customer impact during the migration, please refer to [Data Residency for Microsoft Teams](#).

How can I determine customer data location?

You can find the actual data location in Microsoft 365 admin center. In the coming months, you will be able to find the actual data location for committed data, by

navigating to **Settings > Org settings > Organization profile > Data location.**

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Data Residency for Microsoft Defender for Office P1

Article • 03/01/2024

Overview

Service documentation: [Office 365 Security including Microsoft Defender for Office 365 and Exchange Online Protection](#)

Capability Summary: Protects email and collaboration from zero-day malware, phish, and business email compromise. MDO P1 builds on Exchange Online Protection (EOP).

Data Residency commitments available

Advanced Data Residency add-on

Required Conditions:

1. *Tenant* has a sign-up country included in *Local Region Geography* or *Expanded Local Region Geography*.
2. *Tenant* has a valid Advanced Data Residency subscription for all users in the *Tenant*.
3. The MDO P1 subscription customer data is provisioned in *Local Region Geography* or *Expanded Local Region Geography*.

Commitment:

Refer to the [ADR Commitment page](#) for the specific customer data at rest commitment for Microsoft Defender for Office P1.

Other Information

In addition, processing of data that is required to analyze threats and inspect suspicious emails, documents, messages, and links is done in a sandbox environment and performed within the *Local Region Geography* or *Expanded Local Region*.

Exchange Online Protection

Overview

Capability summary: Exchange Online Protection (EOP) is the cloud-based filtering service that protects your organization against spam, malware, and other email threats.

Data Residency commitments available

Advanced Data Residency add-on

Required Conditions:

1. *Tenant* has a sign-up country included in *Local Region Geography* or *Expanded Local Region Geography*.
2. *Tenant* has a valid Advanced Data Residency subscription for all users in the *Tenant*
3. The EOP subscription customer data is provisioned in *Local Region Geography* or *Expanded Local Region Geography*

Commitment:

Refer to the [Advanced Data Residency Commitment](#) page for the specific customer data at rest commitment for Exchange Online Protection.

Migration

EOP customer data migrates after ADR migration is initiated. MDO P1 doesn't have customer data to migrate.

How can I determine customer data location?

You can find the actual data location in Tenant Admin Center. As a tenant administrator you can find the actual data location, for committed data, by navigating to **Admin->Settings->Org Settings->Organization Profile->Data Location**.

Feedback

Was this page helpful?

Yes

No

[Provide product feedback ↗](#)

Data Residency for Office for the Web

Article • 03/01/2024

Overview

Service documentation: [Office for the web service description - Service Descriptions](#)

Capability summary: Office for the web (formerly Office Web Apps) opens Word, Excel, and PowerPoint documents in your web browser. Office for the web makes it easier to work and share Office files from anywhere with an internet connection, from almost any device. Microsoft 365 customers with Word, Excel, or PowerPoint can view, create, and edit files on the go.

Data Residency commitments available

Advanced Data Residency add-on

Required Conditions:

1. *Tenant* has a sign-up country/region included in *Local Region Geography* or *Expanded Local Region Geography*.
2. *Tenant* has a valid *Advanced Data Residency* subscription for all users in the *Tenant*.
3. The Office for the Web subscription customer data is provisioned in *Local Region Geography* or *Expanded Local Region Geography*.

Commitment:

Refer to the [ADR Commitment page](#) for the specific customer data at rest commitment for Office for the Web.

Migration

The cache for documents isn't migrated to the new *Geography*, and will be reestablished as users work on documents.

How can I determine customer data location?

We are in the process of updating the actual data location in *Tenant Admin Center*. When this change is complete the tenant will be able to see the actual data location, for

in scope data, by navigating to Admin|Settings|Org Settings|Organization Profile|Data Location. Until that change is visible, you can view the Exchange Online data or SharePoint location information in order to understand where the in scope data is stored for this service.

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Data Residency for Viva Connections

Article • 03/01/2024

Overview

Service documentation: [Overview: Viva Connections](#)

Capability Summary: Microsoft Viva Connections is your gateway to a modern employee experience designed to keep everyone engaged and informed. Viva Connections is a customizable app in Microsoft Teams that gives everyone a personalized destination to discover relevant news, conversations, and the tools they need to succeed. Data storage is related to the following Viva Connections Components: Dashboard and feed.

Data Residency Commitments Available

Advanced Data Residency add-on

Required Conditions:

1. *Tenant* has a sign-up country/region included in *Local Region Geography* or *Expanded Local Region Geography*.
2. *Tenant* has a valid Advanced Data Residency subscription for all users in the *Tenant*.
3. The Viva Connections subscription customer data is provisioned in *Local Region Geography* or *Expanded Local Region Geography*.

Commitment:

Refer to the [ADR Commitment page](#) for the specific customer data at rest commitment for Viva Connections.

Migration

Data is stored within Exchange Online, SharePoint and Microsoft Teams. Migration processes are handled by the applicable/relevant workloads.

How can I determine customer data location?

You can find the actual data location in Tenant Admin Center. As a tenant administrator you can find the actual data location, for committed data, by navigating to Admin-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Data Residency for Viva Topics

Article • 03/01/2024

Summary

Service documentation: [Microsoft Viva Topics overview](#)

Capability summary: Viva Topics uses Microsoft Artificial Intelligence technology, Microsoft 365, Microsoft Graph, Search, and other components and services to bring knowledge to your users in the Microsoft 365 apps they use everyday, starting with SharePoint modern pages, Outlook, Microsoft Search, and Search in Word, PowerPoint, and Excel.

Data Residency Commitments Available

Advanced Data Residency add-on

Required Conditions:

1. *Tenant* has a sign-up country/region included in *Local Region Geography* or *Expanded Local Region Geography*.
2. *Tenant* has a valid Advanced Data Residency subscription for all users in the *Tenant*.
3. The Viva Topics subscription customer data is provisioned in *Local Region Geography* or *Expanded Local Region Geography*.

Commitment:

Refer to the [ADR Commitment page](#) for the specific customer data at rest commitment for Viva Topics.

Migration

Data stored is maintained within Exchange Online, SharePoint, and Microsoft Teams. Migration processes are handled by the applicable/relevant workloads.

How can I determine customer data location?

You can find the actual data location in Tenant Admin Center. As a tenant administrator you can find the actual data location, for committed data, by navigating to Admin-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Data Residency support for Microsoft Purview

Article • 03/01/2024

This article lists the Data Residency commitments (available with the Advanced Data Residency add-on) for supported Microsoft Purview services and solutions.

The required conditions for the related commitments for the following services are:

1. *Tenant* has a sign-up country/region included in *Local Region Geography* or *Expanded Local Region Geography*.
2. *Tenant* has a valid Advanced Data Residency subscription for all users in the *Tenant*.
3. The Purview service Customer Data is provisioned in *Local Region Geography* or *Expanded Local Region Geography*.

Migration

Customer Data supporting Purview services is closely aligned with the Exchange Online and SharePoint services, and the bulk of the data migrated, if required to fulfill the data residency commitments for the Purview services, will be handled by those services. In the cases where supporting Customer Data is maintained in an Azure Service, for example, the migration of that data is tied to the migration of the underlying Exchange Online/SharePoint data.

How can I determine Customer Data location?

We are in the process of updating the actual data location in *Tenant* Admin Center. When this change is complete you will be able to see the actual data location, for committed data, by navigating to Admin->Settings->Org Settings->Organization Profile->Data Location. Until that change is visible, you can view the Exchange Online data location information in order to understand where your committed data is stored for this service.

Purview Audit (Standard)

Summary

Service documentation: [Microsoft Purview auditing solutions](#)

Capability summary: Microsoft Purview Audit (Standard) provides you with the ability to log and search your data for audit activities and power your forensics, IT, and compliance efforts and legal investigations.

Data Residency commitments available

Commitment:

Refer to the [ADR Commitment page](#) for the specific Customer Data at rest commitment for Purview Audit (Standard).

Purview Audit (Premium)

Summary

Service documentation: [Microsoft Purview auditing solutions](#)

Capability summary: Microsoft Purview Audit (Premium) builds on the capabilities of Audit (Standard) by providing audit log retention policies, longer retention of audit records, capability to identify high-value crucial events, and higher bandwidth access to the Office 365 Management Activity API.

Data Residency commitments available

Commitment:

Refer to the [ADR Commitment page](#) for the specific Customer Data at rest commitment for Purview Audit (Premium).

Data lifecycle management - Data Retention

Summary

ADR applies to the following services within Purview Data lifecycle management, Data Retention:

- Manual retention labels
- Basic org-wide or location-wide retention policies
- Rules-based automatic retention policies
- Machine Learning-based retention
- Teams message retention policies

Service documentation: [Learn about retention policies & labels](#)

For more detailed information about how retention settings work for different workloads, see the following articles:

- [Learn about retention for Exchange](#)
- [Learn about retention for SharePoint and OneDrive](#)
- [Learn about retention for Microsoft Teams](#)

Capability summary: Lets you retain or delete content with policy management for email, documents, and Teams.

Data Residency commitments available

Commitment:

Refer to the [ADR Commitment page](#) for the specific Customer Data at rest commitment for Data lifecycle management - Data Retention.

Data lifecycle management - Records Management

Summary

Service documentation: [Learn about Microsoft Purview Records Management](#)

Capability summary: Organizations of all types require a records-management solution to manage regulatory, legal, and business-critical records across their corporate data. Records management for Microsoft Purview helps an organization manage their legal obligations, provides the ability to demonstrate compliance with regulations, and increases efficiency with regular disposition of items that are no longer required to be retained, no longer of value, or no longer required for business purposes.

Data Residency commitments available

Commitment:

Refer to the [ADR Commitment page](#) for the specific Customer Data at rest commitment for Data lifecycle management - Records Management.

Information Protection - Sensitivity labels

Summary

ADR applies to the following services within Purview Information Protection, Sensitivity labels:

- Manual, default, and mandatory sensitivity labeling in Office 365
- Automatic sensitivity labeling in Office 365 apps
- Automatic sensitivity labels in Exchange, SharePoint, and OneDrive
- Sensitivity labels based on advanced classification
- Sensitivity labeling for containers in Office 365

Service documentation:

- [Learn about sensitivity labels](#)
- [Get started with Activity explorer](#)

Capability summary: Sensitivity labels from Microsoft Purview Information Protection let you classify and protect your organization's data, while making sure that user productivity and their ability to collaborate isn't hindered.

Data Residency commitments available

Commitment:

Refer to the [ADR Commitment page](#) for the specific Customer Data at rest commitment for Information Protection - Sensitivity labels.

Information Protection - Data Loss Prevention (DLP)

Summary

ADR applies to the following services within Purview Information Protection, Data Loss Prevention (DLP):

- Office 365 Data Loss Prevention (DLP) for emails and files
- DLP for Teams chat

Service documentation: [Learn about data loss prevention](#)

Capability summary:

Organizations have sensitive information under their control such as financial data, proprietary data, credit card numbers, health records, or social security numbers. To help protect this sensitive data and reduce risk, they need a way to prevent their users from

inappropriately sharing it with people who shouldn't have it. This practice is called data loss prevention (DLP).

In Microsoft Purview, you implement data loss prevention by defining and applying DLP policies. With a DLP policy, you can identify, monitor, and automatically protect sensitive items across:

- Microsoft 365 services such as Teams, Exchange, SharePoint, and OneDrive
- Office applications such as Word, Excel, and PowerPoint
- Windows 10, Windows 11, and macOS (Catalina 10.15 and higher) endpoints
- non-Microsoft cloud apps
- on-premises file shares and on-premises SharePoint.

DLP detects sensitive items by using deep content analysis, not by just a simple text scan. Content is analyzed for primary data matches to keywords, by the evaluation of regular expressions, by internal function validation, and by secondary data matches that are in proximity to the primary data match. Beyond that DLP also uses machine learning algorithms and other methods to detect content that matches your DLP policies.

Data Residency commitments available

Commitment:

Refer to the [ADR Commitment page](#) for the specific Customer Data at rest commitment for Information Protection - Data Loss Prevention (DLP).

Information Protection - Office Message Encryption

Summary

ADR applies to the following services within Purview Information Protection, Office Message Encryption:

- Basic Office Message Encryption
- Advanced Office Message Encryption

Service documentation: [Office 365 Message Encryption - Microsoft Purview](#)

Capability summary: With Office 365 Message Encryption, your organization can send and receive encrypted email messages between people inside and outside your organization. Office 365 Message Encryption works with Outlook.com, Yahoo!, Gmail, and other email services. Email message encryption helps to ensure that only intended recipients can view message content.

Data Residency commitments available

Commitment:

Refer to the [ADR Commitment page](#) for the specific Customer Data at rest commitment for Information Protection - Office Message Encryption.

Risk and compliance - information barriers

Summary

Service documentation: [Learn about information barriers](#)

Capability summary: Microsoft Purview Information Barriers (IB) is a compliance solution that allows you to restrict two-way communication and collaboration between groups and users in Microsoft Teams, SharePoint, and OneDrive. Often used in highly regulated industries, IB can help to avoid conflicts of interest and safeguard internal information between users and organizational areas.

Data Residency commitments available

Commitment:

Refer to the [ADR Commitment page](#) for the specific Customer Data at rest commitment for IB.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Data Residency for Other Microsoft 365 Services

Article • 02/29/2024

ⓘ Note

Unless otherwise stated in the [Microsoft Product Terms](#), the following Microsoft 365 services do not have specific commitments for data residency. You can use the following guidance to determine where your data may be provisioned at this time.

Use the following guidance to determine where your data is located. Reference your *tenant Default Geography*.

Microsoft Entra ID

Refer to [Microsoft Entra Data Locations](#).

Forms

Tenants in EU member Countries/regions maintain data in Macro Region Geography 1 – EMEA. All other tenants have customer data stored in the United States, except Australia. For customers in Australia, Microsoft Forms customer data is stored at rest in Australia for all new tenants using Forms and existing tenants that haven't previously used Forms.

Intune

Refer to [endpoint.microsoft.com, Tenant Administration | Tenant Status](#) for existing tenants. If you don't have an existing tenant, create a trial tenant and provision Intune. Microsoft won't store Intune customer data at rest outside the stated geo, except if:

- It's necessary for Microsoft to provide customer support, troubleshoot the service, or comply with legal requirements.
- The customer configures an account to enable such storage of customer data, including by using the following:
 - Features that are designed to operate globally, such as Content Delivery Network (CDN), which provides a global caching service and stores customer data at edge locations around the world.

- If you're using the Remote Help feature, the Helper and Sharer's information might be sent outside of the stated Geo for 48 hours.
- If you are using Intune's enrollment and compliance notification features to send emails to end-users, the emails will be processed within the respective country for sovereign cloud customers, in EMEA for customers located in EMEA, and in North America for all other customers.
- For Microsoft Entra ID: Refer to [Microsoft Entra Data Locations](#).
- Preview, beta, or other prerelease services, which typically store customer data in the United States but might store it globally. Regardless, Microsoft doesn't control or limit the Geo from which customers or their end users might access customer data. Similarly, where customer data in other services is subsequently integrated into Intune, the originating customer data will continue to be stored subject to the other service's own Geo commitments (if any); only the copy of the customer data integrated into Intune will be stored in the stated Geo for Intune.

Office for Mobile

Customer data for this service comes from other services, like Exchange Online and SharePoint Online. There's no customer data stored outside of those services with the exception of the mobile device.

OneNote Services

OneNote stores customer data in OneDrive. It does however have an API that can cause persistent caches to be made outside of the Geography where OneDrive stores customer data.

Planner

See the [Static data location information for select workloads](#) section.

Power Apps for Microsoft 365

Refer to [Dynamics 365 availability and data locations | Microsoft Learn](#).

Stream

You can find this information from the "?" option in the Stream UI, if you have it running and then click on "About Microsoft Stream" and see where your data is stored. If

needed, create a trial tenant.

Viva Glint

The data region for Viva Glint is determined by the default geography of the tenant, not individual users, and is stored in US or EU data centers based on central tenant location. If the central tenant location is *outside* the US or EU, the data for Viva Glint is stored in the US data center.

Viva Goals

Summary

Service documentation: [Introduction to Microsoft Viva Goals](#)

Capability summary: Microsoft Viva Goals is a goal-alignment solution that connects teams to your organization's strategic priorities, unites them around your mission and purpose, and drives business results. Viva Goals enables individuals and companies to organize and track their goals through "Objectives and Key Results" (OKRs). Viva Goals immerses everyone in the company's purpose and top priorities and creates a culture of engaged employees focused on achieving common goals.

Data Residency Available

Starting December 5, 2022, Viva Goals [Customer Data](#) for new tenants in the [European Union Data Boundary \(EUDB\)](#) and in the United Kingdom will be stored in data centers located in the EU. All other tenants will have their Viva Goals Customer Data stored in data centers located in the United States. Tenants aren't provided with a choice for the specific deployment region for data storage.

To be considered a tenant in the EUDB:

1. The tenant must have a *default geography* in a EUDB country or select a country in EUDB country as their residence during free trial sign-up; and
2. The tenant must not purchase a Multi-Geo offering

Migration

Customers based in EU and UK who signed up for Viva Goals prior to December 5, 2022, have now been migrated to EU data centers.

Viva Insights – Advanced, Mgr, Leader

See the [Static data location information for select workloads](#) section. The data region for Manager/Leader and Advanced is determined by the *Default Geography* of the *tenant*, not individual users.

Starting June 2024, Viva Insights (Advanced, Manager, Leader) customer data for new tenants in Australia will be provisioned in data centers located in Australia.

Viva Insights – Personal

Customer data is processed and stored in the employee's Exchange Online mailbox. Data residency for Personal insights in Viva Insights is based on the employee's mailbox location. For more information, see [Personal insights in Viva Insights privacy guide for admins](#).

Viva Learning

See the [Static data location information for select workloads](#) section.

Whiteboard

Refer to [Manage data for Microsoft Whiteboard | Microsoft Learn](#).

Viva Engage

Refer to [Data Residency - Viva Engage | Microsoft Learn](#).

Static data location information for select workloads

1. Macro Region Geography 1 – EMEA / European Union
2. Macro Region Geography 2 - Asia Pacific
3. Macro Region Geography 3 – Americas
4. Australia
5. Canada
6. Japan
7. India
8. United Kingdom

9. France

[\[+\] Expand table](#)

Country Code	Countries/Regions	Viva Insights Advanced	Viva Learning	Planner
AF	Afghanistan	APC ²	APC ²	APC ²
AX	Aland Islands	APC ²	AMER ³	EUR ¹
AL	Albania	EUR ¹	EUR ¹	EUR ¹
DZ	Algeria	EUR ¹	EUR ¹	EUR ¹
AS	American Samoa	APC ²	APC ²	APC ²
AD	Andorra	EUR ¹	EUR ¹	EUR ¹
AO	Angola	EUR ¹	EUR ¹	EUR ¹
AI	Anguilla	AMER ³	AMER ³	AMER ³
AQ	Antarctica	AMER ³	EUR ¹	AMER ³
AG	Antigua and Barbuda	AMER ³	AMER ³	AMER ³
AR	Argentina	AMER ³	AMER ³	AMER ³
AM	Armenia	EUR ¹	EUR ¹	EUR ¹
AW	Aruba	AMER ³	AMER ³	AMER ³
AU	Australia	AUS ⁴	AUS ⁴	AUS ⁴
AT	Austria	EUR ¹	EUR ¹	EUR ¹
AZ	Azerbaijan	EUR ¹	EUR ¹	EUR ¹
BS	Bahamas	AMER ³	AMER ³	AMER ³
BH	Bahrain	EUR ¹	EUR ¹	EUR ¹
BD	Bangladesh	APC ²	APC ²	APC ²
BB	Barbados	AMER ³	AMER ³	AMER ³
BY	Belarus	EUR ¹	EUR ¹	EUR ¹
BE	Belgium	EUR ¹	EUR ¹	EUR ¹
BZ	Belize	AMER ³	AMER ³	AMER ³

Country Code	Countries/Regions	Viva Insights Advanced	Viva Learning	Planner
BJ	Benin	EUR ¹	EUR ¹	EUR ¹
BM	Bermuda	AMER ³	AMER ³	AMER ³
BT	Bhutan	APC ²	APC ²	APC ²
BO	Bolivia	AMER ³	AMER ³	AMER ³
BQ	Bonaire	AMER ³	AMER ³	AMER ³
BA	Bosnia and Herzegovina	EUR ¹	EUR ¹	EUR ¹
BW	Botswana	EUR ¹	EUR ¹	EUR ¹
BV	Bouvet Island	AMER ³	EUR ¹	AMER ³
BR	Brazil	AMER ³	AMER ³	AMER ³
IO	British Indian Ocean Territory	APC ²	APC ²	APC ²
VG	British Virgin Islands	AMER ³	AMER ³	AMER ³
BN	Brunei Darussalam	APC ²	APC ²	APC ²
BG	Bulgaria	EUR ¹	EUR ¹	EUR ¹
BF	Burkina Faso	EUR ¹	EUR ¹	EUR ¹
BI	Burundi	EUR ¹	EUR ¹	EUR ¹
KH	Cambodia	APC ²	APC ²	APC ²
CM	Cameroon	EUR ¹	EUR ¹	EUR ¹
CA	Canada	AMER ³	Canada ⁵	CAN ⁵
CV	Cabo Verde	EUR ¹	EUR ¹	EUR ¹
KY	Cayman Islands	AMER ³	AMER ³	AMER ³
CF	Central African Republic	EUR ¹	EUR ¹	EUR ¹
TD	Chad	EUR ¹	EUR ¹	EUR ¹
CL	Chile	AMER ³	AMER ³	AMER ³
CN	China	APC ²	APC ²	APC ²
CX	Christmas Island	APC ²	APC ²	APC ²
CC	Cocos (Keeling) Islands	APC ²	APC ²	APC ²

Country Code	Countries/Regions	Viva Insights Advanced	Viva Learning	Planner
CO	Colombia	AMER ³	AMER ³	AMER ³
KM	Comoros	EUR ¹	EUR ¹	EUR ¹
CG	Congo (Brazzaville)	EUR ¹	EUR ¹	EUR ¹
CD	Congo, (Kinshasa)	EUR ¹	EUR ¹	EUR ¹
CK	Cook Islands	APC ²	APC ²	APC ²
CR	Costa Rica	AMER ³	AMER ³	AMER ³
CI	Côte d'Ivoire	EUR ¹	EUR ¹	EUR ¹
HR	Croatia	EUR ¹	EUR ¹	EUR ¹
CW	Curaçao	AMER ³	EUR ¹	AMER ³
CY	Cyprus	EUR ¹	EUR ¹	EUR ¹
CZ	Czech Republic	EUR ¹	EUR ¹	EUR ¹
DK	Denmark	EUR ¹	EUR ¹	EUR ¹
DJ	Djibouti	EUR ¹	EUR ¹	EUR ¹
DM	Dominica	AMER ³	AMER ³	AMER ³
DO	Dominican Republic	AMER ³	AMER ³	AMER ³
EC	Ecuador	AMER ³	AMER ³	AMER ³
EG	Egypt	EUR ¹	EUR ¹	EUR ¹
SV	El Salvador	AMER ³	AMER ³	AMER ³
GQ	Equatorial Guinea	EUR ¹	EUR ¹	EUR ¹
ER	Eritrea	EUR ¹	EUR ¹	EUR ¹
EE	Estonia	EUR ¹	EUR ¹	EUR ¹
ET	Ethiopia	EUR ¹	EUR ¹	EUR ¹
FK	Falkland Islands	AMER ³	AMER ³	AMER ³
FO	Faroe Islands	EUR ¹	EUR ¹	EUR ¹
FM	Federated States of Micronesia	APC ²	APC ²	APC ²
FJ	Fiji	APC ²	APC ²	AUS ⁴

Country Code	Countries/Regions	Viva Insights Advanced	Viva Learning	Planner
FI	Finland	EUR ¹	EUR ¹	EUR ¹
FR	France	EUR ¹	France ⁹	EUR ¹
GF	French Guiana	AMER ³	AMER ³	AMER ³
PF	French Polynesia	APC ²	APC ²	APC ²
TF	French Southern Territories	AMER ³	EUR ¹	AMER ³
GA	Gabon	EUR ¹	EUR ¹	EUR ¹
GM	Gambia	EUR ¹	EUR ¹	EUR ¹
GE	Georgia	EUR ¹	EUR ¹	EUR ¹
DE	Germany	EUR ¹	EUR ¹	EUR ¹
GH	Ghana	EUR ¹	EUR ¹	EUR ¹
GI	Gibraltar	EUR ¹	EUR ¹	EUR ¹
GR	Greece	EUR ¹	EUR ¹	EUR ¹
GL	Greenland	AMER ³	AMER ³	AMER ³
GD	Grenada	AMER ³	AMER ³	AMER ³
GP	Guadeloupe	AMER ³	AMER ³	AMER ³
GU	Guam	APC ²	APC ²	APC ²
GT	Guatemala	AMER ³	AMER ³	AMER ³
GG	Guernsey	EUR ¹	EUR ¹	EUR ¹
GN	Guinea	EUR ¹	EUR ¹	EUR ¹
GW	Guinea-Bissau	EUR ¹	EUR ¹	EUR ¹
GY	Guyana	AMER ³	AMER ³	AMER ³
HT	Haiti	AMER ³	AMER ³	AMER ³
HM	Heard and McDonald Islands	AMER ³	AMER ³	AMER ³
VA	Holy See (Vatican City State)	EUR ¹	EUR ¹	EUR ¹
HN	Honduras	AMER ³	AMER ³	AMER ³
HK	Hong Kong SAR	APC ²	APC ²	APC ²

Country Code	Countries/Regions	Viva Insights Advanced	Viva Learning	Planner
HU	Hungary	EUR ¹	EUR ¹	EUR ¹
IS	Iceland	EUR ¹	EUR ¹	EUR ¹
IN	India	APC ²	APC ²	IND ⁷
ID	Indonesia	APC ²	APC ²	APC ²
IQ	Iraq	EUR ¹	EUR ¹	EUR ¹
IE	Ireland	EUR ¹	EUR ¹	EUR ¹
IM	Isle of Man	EUR ¹	EUR ¹	EUR ¹
IL	Israel	EUR ¹	EUR ¹	EUR ¹
IT	Italy	EUR ¹	EUR ¹	EUR ¹
JM	Jamaica	AMER ³	AMER ³	AMER ³
JP	Japan	APC ²	APC ²	JPN ⁶
JE	Jersey	EUR ¹	EUR ¹	EUR ¹
JO	Jordan	EUR ¹	EUR ¹	EUR ¹
KZ	Kazakhstan	EUR ¹	EUR ¹	EUR ¹
KE	Kenya	EUR ¹	EUR ¹	EUR ¹
KI	Kiribati	APC ²	APC ²	APC ²
KP	Korea (North)	APC ²	APC ²	APC ²
KR	Korea (South)	APC ²	APC ²	APC ²
XK	Kosovo	EUR ¹	AMER ³	EUR ¹
KW	Kuwait	EUR ¹	EUR ¹	EUR ¹
KG	Kyrgyzstan	EUR ¹	APC ²	EUR ¹
LA	Lao PDR	APC ²	APC ²	APC ²
LV	Latvia	EUR ¹	EUR ¹	EUR ¹
LB	Lebanon	EUR ¹	EUR ¹	EUR ¹
LS	Lesotho	EUR ¹	EUR ¹	EUR ¹
LR	Liberia	EUR ¹	EUR ¹	EUR ¹

Country Code	Countries/Regions	Viva Insights Advanced	Viva Learning	Planner
LY	Libya	EUR ¹	EUR ¹	EUR ¹
LI	Liechtenstein	EUR ¹	EUR ¹	EUR ¹
LT	Lithuania	EUR ¹	EUR ¹	EUR ¹
LU	Luxembourg	EUR ¹	EUR ¹	EUR ¹
MO	Macao, SAR	APC ²	APC ²	APC ²
MG	Madagascar	EUR ¹	EUR ¹	EUR ¹
MW	Malawi	EUR ¹	EUR ¹	EUR ¹
MY	Malaysia	APC ²	APC ²	APC ²
MV	Maldives	APC ²	APC ²	APC ²
ML	Mali	EUR ¹	EUR ¹	EUR ¹
MT	Malta	EUR ¹	EUR ¹	EUR ¹
MH	Marshall Islands	APC ²	APC ²	APC ²
MQ	Martinique	AMER ³	AMER ³	AMER ³
MR	Mauritania	EUR ¹	EUR ¹	EUR ¹
MU	Mauritius	EUR ¹	EUR ¹	EUR ¹
YT	Mayotte	EUR ¹	EUR ¹	EUR ¹
MX	Mexico	AMER ³	AMER ³	AMER ³
MC	Monaco	EUR ¹	EUR ¹	EUR ¹
MD	Moldova	EUR ¹	EUR ¹	EUR ¹
MN	Mongolia	APC ²	APC ²	APC ²
ME	Montenegro	EUR ¹	EUR ¹	EUR ¹
MS	Montserrat	AMER ³	AMER ³	AMER ³
MA	Morocco	EUR ¹	EUR ¹	EUR ¹
MZ	Mozambique	EUR ¹	EUR ¹	EUR ¹
MM	Myanmar	APC ²	APC ²	APC ²
NA	Namibia	EUR ¹	EUR ¹	EUR ¹

Country Code	Countries/Regions	Viva Insights Advanced	Viva Learning	Planner
NR	Nauru	APC ²	APC ²	APC ²
NP	Nepal	APC ²	APC ²	APC ²
NL	Netherlands	EUR ¹	EUR ¹	EUR ¹
AN	Netherlands Antilles	AMER ³	AMER ³	AMER ³
NC	New Caledonia	APC ²	APC ²	APC ²
NZ	New Zealand	APC ²	APC ²	AUS ⁴
NI	Nicaragua	AMER ³	AMER ³	AMER ³
NE	Niger	EUR ¹	EUR ¹	EUR ¹
NG	Nigeria	EUR ¹	EUR ¹	EUR ¹
NU	Niue	APC ²	APC ²	APC ²
NF	Norfolk Island	APC ²	APC ²	APC ²
MP	Northern Mariana Islands	APC ²	APC ²	APC ²
NO	Norway	EUR ¹	EUR ¹	EUR ¹
OM	Oman	EUR ¹	APC ²	EUR ¹
PK	Pakistan	EUR ¹	APC ²	EUR ¹
PW	Palau	APC ²	APC ²	APC ²
PS	Palestinian Authority	APC ²	EUR ¹	APC ²
PA	Panama	AMER ³	AMER ³	AMER ³
PG	Papua New Guinea	APC ²	APC ²	APC ²
PY	Paraguay	AMER ³	AMER ³	AMER ³
PE	Peru	AMER ³	AMER ³	AMER ³
PH	Philippines	APC ²	APC ²	APC ²
PN	Pitcairn	APC ²	APC ²	APC ²
PL	Poland	EUR ¹	EUR ¹	EUR ¹
PT	Portugal	EUR ¹	EUR ¹	EUR ¹
PR	Puerto Rico	AMER ³	AMER ³	AMER ³

Country Code	Countries/Regions	Viva Insights Advanced	Viva Learning	Planner
QA	Qatar	EUR ¹	EUR ¹	EUR ¹
MK	Republic of North Macedonia	EUR ¹	EUR ¹	EUR ¹
RE	Réunion	EUR ¹	EUR ¹	EUR ¹
RO	Romania	EUR ¹	EUR ¹	EUR ¹
RU	Russian Federation	EUR ¹	EUR ¹	EUR ¹
RW	Rwanda	EUR ¹	EUR ¹	EUR ¹
SH	Saint Helena	EUR ¹	EUR ¹	EUR ¹
KN	Saint Kitts and Nevis	AMER ³	AMER ³	AMER ³
LC	Saint Lucia	AMER ³	AMER ³	AMER ³
PM	Saint Pierre and Miquelon	AMER ³	AMER ³	AMER ³
VC	Saint Vincent and Grenadines	AMER ³	AMER ³	AMER ³
BL	Saint-Barthélemy	AMER ³	EUR ¹	AMER ³
MF	Saint-Martin (French part)	AMER ³	EUR ¹	AMER ³
WS	Samoa	APC ²	APC ²	APC ²
SM	San Marino	EUR ¹	EUR ¹	EUR ¹
ST	São Tomé and Príncipe	EUR ¹	EUR ¹	EUR ¹
SA	Saudi Arabia	EUR ¹	EUR ¹	EUR ¹
SN	Senegal	EUR ¹	EUR ¹	EUR ¹
RS	Serbia	EUR ¹	EUR ¹	EUR ¹
SC	Seychelles	EUR ¹	EUR ¹	EUR ¹
SL	Sierra Leone	EUR ¹	EUR ¹	EUR ¹
SG	Singapore	APC ²	APC ²	APC ²
SX	Sint Maarten	AMER ³	EUR ¹	AMER ³
SK	Slovakia	EUR ¹	EUR ¹	EUR ¹
SI	Slovenia	EUR ¹	EUR ¹	EUR ¹
SB	Solomon Islands	APC ²	APC ²	APC ²

Country Code	Countries/Regions	Viva Insights Advanced	Viva Learning	Planner
SO	Somalia	EUR ¹	EUR ¹	EUR ¹
ZA	South Africa	EUR ¹	EUR ¹	EUR ¹
GS	South Georgia and the South Sandwich Islands	AMER ³	EUR ¹	AMER ³
SS	South Sudan	EUR ¹	EUR ¹	EUR ¹
ES	Spain	EUR ¹	EUR ¹	EUR ¹
LK	Sri Lanka	APC ²	APC ²	APC ²
SR	Suriname	AMER ³	AMER ³	AMER ³
SJ	Svalbard and Jan Mayen Islands	EUR ¹	EUR ¹	EUR ¹
SZ	Swaziland	EUR ¹	EUR ¹	EUR ¹
SE	Sweden	EUR ¹	EUR ¹	EUR ¹
CH	Switzerland	EUR ¹	EUR ¹	EUR ¹
TW	Taiwan	APC ²	APC ²	APC ²
TJ	Tajikistan	EUR ¹	APC ²	EUR ¹
TH	Thailand	APC ²	APC ²	APC ²
TL	Timor-Leste	APC ²	EUR ¹	APC ²
TG	Togo	EUR ¹	EUR ¹	EUR ¹
TK	Tokelau	APC ²	APC ²	APC ²
TO	Tonga	APC ²	APC ²	APC ²
TT	Trinidad and Tobago	AMER ³	AMER ³	AMER ³
TN	Tunisia	EUR ¹	EUR ¹	EUR ¹
TR	Türkiye	EUR ¹	EUR ¹	EUR ¹
TM	Turkmenistan	EUR ¹	APC ²	EUR ¹
TC	Turks and Caicos Islands	AMER ³	AMER ³	AMER ³
TV	Tuvalu	APC ²	APC ²	APC ²
UG	Uganda	EUR ¹	EUR ¹	EUR ¹

Country Code	Countries/Regions	Viva Insights Advanced	Viva Learning	Planner
UA	Ukraine	EUR ¹	EUR ¹	EUR ¹
AE	United Arab Emirates	EUR ¹	EUR ¹	EUR ¹
GB	United Kingdom	EUR ¹	UK ⁸	EUR ¹
TZ	United Republic of Tanzania	EUR ¹	EUR ¹	EUR ¹
US	United States of America	AMER ³	AMER ³	AMER ³
UY	Uruguay	AMER ³	AMER ³	AMER ³
UM	US Minor Outlying Islands	APC ²	APC ²	APC ²
UZ	Uzbekistan	EUR ¹	APC ²	EUR ¹
VU	Vanuatu	APC ²	APC ²	APC ²
VE	Venezuela (Bolivarian Republic)	AMER ³	AMER ³	AMER ³
VN	Vietnam	APC ²	APC ²	APC ²
VI	Virgin Islands, US	AMER ³	AMER ³	AMER ³
WF	Wallis and Futuna Islands	APC ²	APC ²	APC ²
YE	Yemen	EUR ¹	EUR ¹	EUR ¹
ZM	Zambia	EUR ¹	EUR ¹	EUR ¹
ZW	Zimbabwe	EUR ¹	EUR ¹	EUR ¹

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Data Residency Legacy Move Program

Article • 02/29/2024

ⓘ Note

Coinciding with the launch of the Microsoft 365 Advanced Data Residency add-on, the Move Program will no longer be offered during the launch of new local datacenter regions. Our most recent local datacenter region launch in Qatar (August 2022) is the final region to receive Move Program benefits. The following information is still valid for regions that were part of Move Program and all customers currently opted-in for migration will be processed. For more information, see [the ADR page](#).

When Can I Request a Move (final opt-in opportunity)

[+] Expand table

Customers with signup country/region in	Request period begins	Request deadline	Migration Commitment *
Japan	Nov. 1, 2022	Apr. 30, 2023	May 1, 2025
Australia, New Zealand, Fiji	Nov. 1, 2022	Apr. 30, 2023	May 1, 2025
India	Nov. 1, 2022	Apr. 30, 2023	May 1, 2025
Canada	Nov. 1, 2022	Apr. 30, 2023	May 1, 2025
United Kingdom	Nov. 1, 2022	Apr. 30, 2023	May 1, 2025
South Korea	Nov. 1, 2022	Apr. 30, 2023	May 1, 2025
France	Nov. 1, 2022	Apr. 30, 2023	May 1, 2025
United Arab Emirates	Nov. 1, 2022	Apr. 30, 2023	May 1, 2025
South Africa	Nov. 1, 2022	Apr. 30, 2023	May 1, 2025
Switzerland, Liechtenstein	Nov. 1, 2022	Apr. 30, 2023	May 1, 2025
Norway	Nov. 1, 2022	Apr. 30, 2023	May 1, 2025
Germany	Nov. 1, 2022	Apr. 30, 2023	May 1, 2025

Customers with signup country/region in	Request period begins	Request deadline	Migration Commitment *
Brazil	Nov. 1, 2022	Apr. 30, 2023	May 1, 2025
Sweden	Nov. 1, 2022	Apr. 30, 2023	May 1, 2025

Remaining Countries/regions in the Move Program

ⓘ Note

Even though the Move Program is officially ending, we still have some in-flight geographies that we will see through to completion, based on the original 24-month migration commitment. Please refer to the following table for the remaining countries/regions and their migration deadlines.

[+] [Expand table](#)

Customers with signup country/region in	Original Opt-in: migration commitment date	Final Opt-in (above): migration commitment date
Germany	May 1, 2023	May 1, 2025
Brazil	June 1, 2023	May 1, 2025
Sweden	June 1, 2024	May 1, 2025
Qatar	March 1, 2025	Not Applicable

Data Residency Option Moving Forward

With the release of Advanced Data Residency, we're only providing a data residency option to eligible Microsoft 365 customers who are covered by the data centers listed in the *Local Region Geography* on the [Overview and Definitions page](#).

Migration Expectations

Microsoft will use reasonable efforts to try to complete a legacy Move Program migration for customers who request a migration between November 1, 2022 and April 30, 2023, by June 2025. Customers who requested a migration in the legacy Move Program prior to November 1, 2022, will continue being migrated with reasonable

efforts by Microsoft towards the intended completion date provided to them previously. However, Microsoft might not be able to complete the migration within this timeframe for all customers. For example, significantly larger or more complex customers or situations outside of Microsoft's control might require more time to complete the migration. Customers utilizing the Advanced Data Residency feature for a data migration will instead follow the [Advanced Data Residency Migration Expectations](#).

Data moves are a back-end service operation with minimal impact to end-users. We adhere to the [Microsoft Online Services Service Level Agreement \(SLA\)](#) for availability so there's nothing that customers need to prepare for or to monitor during the move. Notification of any service maintenance is done if needed.

Data move general FAQ

ⓘ Note

The following Q&A content relates to Move Program customers **only**.

Here are answers to general questions about moving applicable customer data at rest to a new datacenter geo.

How do we define Applicable Customer Data?

▼ Select to expand

Applicable customer data is a term that refers to a subset of customer data defined in the [Microsoft Online Services Terms](#):

- Exchange Online mailbox content (email body, calendar entries, and the content of email attachments)
- SharePoint site content and the files stored within that site
- Files uploaded to OneDrive
- Teams chat data for group and private chats (files in Teams folders or placed in chat are managed by SharePoint and OneDrive, respectively)

What is in scope for Teams migration?

▼ Select to expand

In addition to Exchange Online, SharePoint, and OneDrive; Microsoft will migrate Teams data to the local datacenter.

- Teams chat messages, including private messages and channel messages.
- Teams images used in chats.

Teams files are stored in SharePoint and Teams chat files are stored in OneDrive. Voicemail, calendar, and contacts are stored in Exchange Online. In many cases, Exchange Online, SharePoint, and OneDrive are already used by the customer in the local datacenter geo and are also part of the Microsoft 365 migration program for eligible customer countries/regions.

At what point is my migration complete so that my *Tenant*'s applicable customer data is being stored at rest in my new geo?

▼ Select to expand

Due to shared dependencies between Exchange Online and SharePoint/OneDrive, any migration can't be considered completed until both services are migrated. Exchange Online and SharePoint/OneDrive often migrate at separate times and independently from one another. Customer *Tenant* admins receive confirmation in Message Center when each service migration is completed and can view the data location card in the Admin Center at any time to confirm the applicable customer data at rest location for each service.

How do you make sure my customer data is safe during the move and that I won't experience downtime?

▼ Select to expand

Data moves are a back-end service operation with minimal impact to end users. Features that can be impacted are listed in [User experience in a Multi-Geo environment](#). We adhere to the [Microsoft Online Services Service Level Agreement \(SLA\)](#) for availability so there's nothing that customers need to prepare for or to monitor during the move.

All Microsoft 365 services run the same versions in the datacenters, so you can be assured of consistent functionality. Your service is fully supported throughout the process.

What is the impact of having different services located in different geos?

▼ Select to expand

Some of the Microsoft 365 services may be located in different geos for some existing customers and for customers that are in the middle of the move process. Our services run independently of each other and there's no impact on the user experience if this is the case. However, for data residency purposes, a *Tenant* migration can't be considered as complete until both Exchange Online and SharePoint/OneDrive are migrated to the same datacenter geo.

Where is my applicable customer data located?

▼ Select to expand

Customer *Tenant* admins can view the data location card in the Admin Center at any time to confirm the applicable customer data at rest location for each service, specifically for their *Tenant*. We also publish the location of datacenter geos, datacenters, and location of Microsoft 365 customer data in [Where your Microsoft 365 customer data is stored](#) ↗ as a reference for the current default applicable customer data at rest locations for new *Tenant*. You can verify the location of your customer data at rest via the Data Location section under your Organization Profile in the Microsoft 365 admin center.

Do all the services move their data on the same day?

▼ Select to expand

Each service moves independently and will likely move their data at different times.

Can I choose when I want my data to be moved?

▼ Select to expand

Customers aren't able to select a specific date, they can't delay their move, and we can't share a specific date or timeframe for the moves.

Can you share when my data will be moved?

▼ Select to expand

Data moves are a back-end operation with minimal impact to end users. The complexity, precision, and scale at which we need to perform data moves within a globally operated and automated environment prohibit us from sharing when a data move is expected to

complete for your *Tenant* or any other single *Tenant*. Customers receive one confirmation in Message Center per participating service when its data move has completed.

What happens if users access services while the data is being moved?

▼ Select to expand

See [User experience in a Multi-Geo environment](#) for a complete list of features that may be limited during portions of the data move for each service.

How do I know the move is complete?

▼ Select to expand

Watch the Microsoft 365 Message Center for confirmation that the move of each service's data is complete. When each service's data is moved, we post a completion notice so you get three completion notices: one each for Exchange Online, SharePoint, and Skype for Business Online. You can also verify the location of your customer data at rest via the Data Location section under your Organization Profile in the Microsoft 365 admin center.

What happens if we are in process of email data migration to Microsoft 365 during the Exchange Online move?

▼ Select to expand

This is a very common scenario and is fully supported. Cloud migration between datacenter geos doesn't interfere with any on-premises to cloud mailbox migrations.

I don't want to wait for Microsoft to move my data. Can I just create a new *Tenant* and move myself?

▼ Select to expand

Yes, however the process won't be as seamless as if Microsoft were to perform the data move.

If you create a new *Tenant* after the new datacenter geo is available, the new *Tenant* will be hosted in the new geo. This new *Tenant* is completely separate from your previous *Tenant* and you would be responsible for moving all user mailboxes, site content, domain names, and any other data. Note that you can't move the *Tenant* name from one *Tenant* to another. We recommend that you wait for the move program provided by Microsoft as we take care of moving all settings, data, and subscriptions for your users.

My customer data has already been moved to a new datacenter geo. Can I move back?

▼ Select to expand

No, this isn't possible. Customers who have been moved to new geo datacenters can't be moved back. As a customer in any geo, you'll experience the same quality of service, performance, and security controls as you did before. [Microsoft 365 Multi Geo](#) is available to some customers as an add-on and lets a single *Tenant* create multiple satellite geos and move user data to those geos with data residency commitments.

Will Microsoft 365 *Tenants* hosted in the new datacenters be available to users outside of the country/region?

▼ Click to expand

Yes. Microsoft maintains a large global network with public Internet connections in more than 130 locations in 35 countries/regions around the world with peering agreements with more than 2,700 Internet Service Providers (ISPs). Users will be able to access the datacenters from wherever they are on the Internet.

I have public folders deployed in my *Tenant*. What will be the impact on public folder access during or after the move?

▼ Select to expand

There's no impact to end users accessing public folders during or after the move of public folders. However, the public folders may not be available for administration in the Exchange Admin Center tool till all public folder mailboxes are moved in same region. Please check [this article](#) for more details.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Where your Microsoft 365 customer data is stored

Article • 06/24/2024

ⓘ Note

The **Spain** local data center region launched on May 31, 2024. If your organization requires the migration of your Microsoft 365 customer data to Spain, and data residency commitments for Spain, see [Advanced Data Residency](#).

ⓘ Note

The **Mexico** local data center region launched on May 3, 2024. If your organization requires the migration of your Microsoft 365 customer data to Mexico, and data residency commitments for Mexico, see [Advanced Data Residency](#).

ⓘ Note

For tenants in Australia, Brazil, Canada, France, Germany, India, Israel, Italy, Japan, Mexico, Norway, Poland, Qatar, South Africa, South Korea, Spain, Sweden, Switzerland, United Arab Emirates, and the United Kingdom, additional workloads are available for data residency commitments. For more information, see [Advanced Data Residency](#).

See the following links to understand how you can determine current data residency and data residency commitments.

- Exchange Online [Data Location](#)
- SharePoint (ODSP) and OneDrive [Data Location](#)
- Microsoft Teams [Data Location](#)
- Microsoft Copilot for Microsoft 365 [Data Location](#)
- Microsoft Defender for Office (MDO P1) [Data Location](#)
- Office for the Web (Office Online) [Data Location](#)
- Viva Connections [Data Location](#)

- Viva Topics [Data Location](#)
 - Microsoft Purview (select services) [Data Location](#)
 - Audit (Standard)
 - Audit (Premium)
 - Data loss prevention
 - Data retention
 - Information barriers
 - Office message encryption
 - Records management
 - Sensitivity labels
 - Microsoft Entra ID [Data Location](#)
 - Whiteboard [Data Location](#)
 - Forms [Data Location](#)
 - Intune [Data Location](#)
 - Planner [Data Location](#)
 - Viva Goals [Data Location](#)
 - Viva Insights – Advanced, Manager and leader [Data Location](#)
 - Viva Insights – Personal [Data Location](#)
 - Viva Learning [Data Location](#)
 - Viva Pulse [Data Location](#)
 - Yammer [Data Location](#)
 - Viva Engage [Data Location](#)
 - Office for mobile [Data Location](#)
 - OneNote Services [Data Location](#)
 - Power Apps for Microsoft 365 [Data Location](#)
 - Stream [Data Location](#)
 - Shifts [Data Location](#)
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

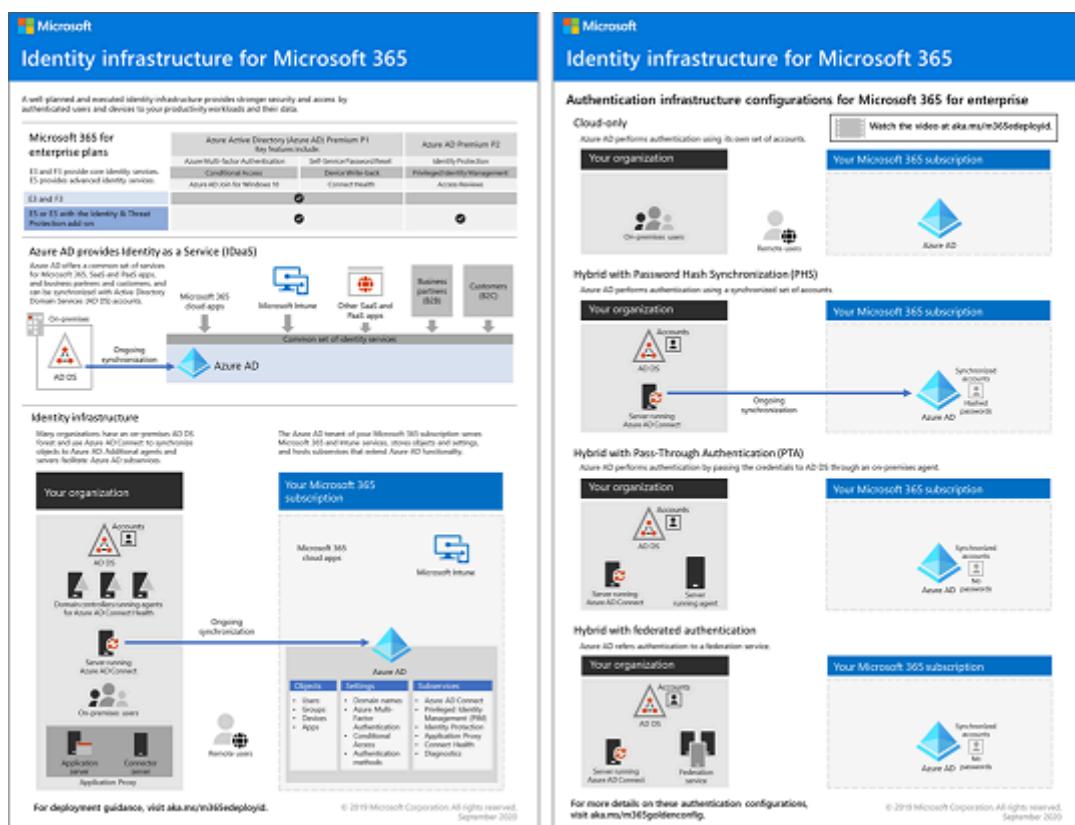
Deploy your identity infrastructure for Microsoft 365

Article • 03/15/2024

Check out all of our small business content on [Small business help & learning](#).

In Microsoft 365 for enterprise, a well-planned and executed identity infrastructure paves the way for stronger security, including restricting access to your productivity workloads and their data to only authenticated users and devices. Security for identities is a key element of a Zero Trust deployment, in which all attempts to access resources both on-premises and in the cloud are authenticated and authorized.

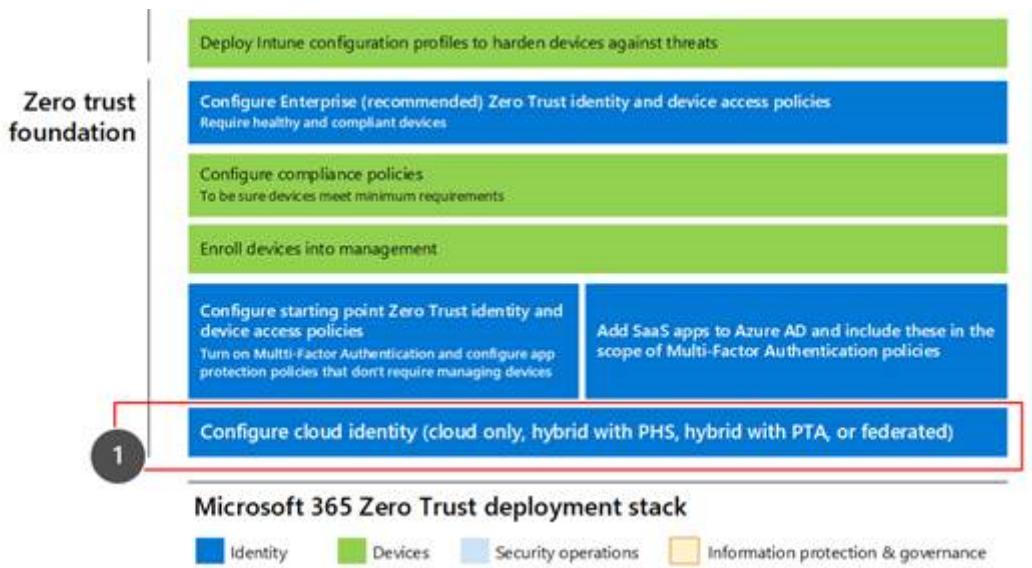
For information about the identity features of each Microsoft 365 for enterprise, the role of Microsoft Entra ID, on-premises and cloud-based components, and the most common authentication configurations, see the [Identity Infrastructure poster](#).



Review this two-page poster to quickly ramp up on identity concepts and configurations for Microsoft 365 for enterprise.

You can [download this poster](#) and can print it in letter, legal, or tabloid (11 x 17) format.

This solution is the first step to build out the Microsoft 365 Zero Trust deployment stack.



For more information, see the [Microsoft 365 Zero Trust deployment plan](#).

What's in this solution

This solution steps you through the deployment of an identity infrastructure for your Microsoft 365 tenant to provide access for your employees and protection against identity-based attacks.



The steps in this solution are:

1. [Determine your identity model](#).
2. [Protect your Microsoft 365 privileged accounts](#).
3. [Protect your Microsoft 365 user accounts](#).
4. [Deploy your identity model](#).

This solution supports the key principles of Zero Trust [↗](#):

- **Verify explicitly:** Always authenticate and authorize based on all available data points.
- **Use least privilege access:** Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.

- **Assume breach:** Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

Unlike conventional intranet access, which trusts everything behind an organization's firewall, Zero Trust treats each sign-in and access as though it originated from an uncontrolled network, whether it's behind the organization firewall or on the Internet. Zero Trust requires protection for the network, infrastructure, identities, endpoints, apps, and data.

Microsoft 365 capabilities and features

Microsoft Entra ID provides a full suite of identity management and security capabilities for your Microsoft 365 tenant.

[\[+\] Expand table](#)

Capability or feature	Description	Licensing
Multifactor 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 stolen credentials can be used to access your environment. Microsoft 365 uses the Microsoft Entra multifactor authentication service for MFA-based sign-ins.	Microsoft 365 E3 or E5
Conditional Access	Microsoft Entra ID evaluates the conditions of the user sign-in and uses Conditional Access policies to determine the allowed 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 their own device and stolen credentials can access your sensitive data. It also protects sensitive data on the devices, because the devices must meet specific requirements for health and security.	Microsoft 365 E3 or E5
Microsoft Entra groups	Conditional Access policies, device management with Intune, and even permissions to files and sites in your organization rely on the assignment to user accounts or Microsoft Entra groups. We recommend you create Microsoft Entra groups that correspond to the levels of protection you're implementing. For example, members of your executive staff are likely higher value targets for hackers. Therefore, it makes sense to add the user accounts of these employees to a Microsoft Entra group and assign	Microsoft 365 E3 or E5

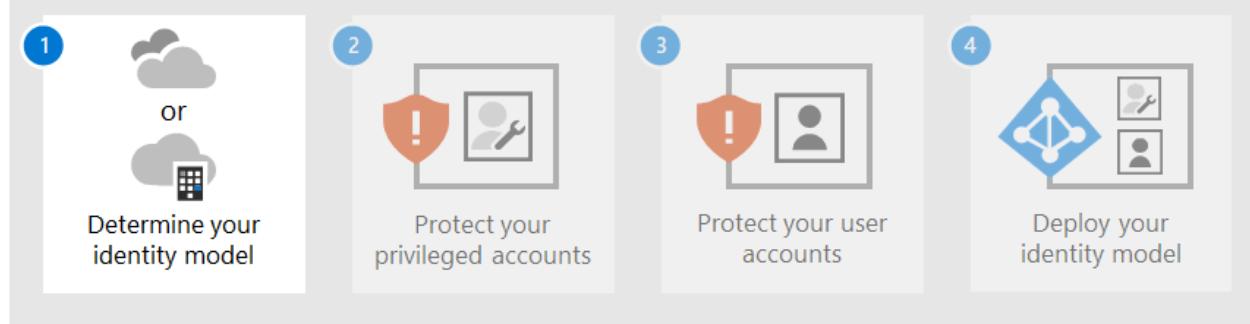
Capability or feature	Description	Licensing
	this group to Conditional Access policies and other policies that enforce a higher level of protection for access.	
Microsoft Entra ID Protection	Enables you to detect potential vulnerabilities affecting your organization's identities and configure automated 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 multifactor 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 365 E5, Microsoft 365 E3 with the E5 Security add-on, EMS E5, or Microsoft Entra ID P2 licenses
Self-service password reset (SSPR)	Allow your users to reset their passwords securely and without help-desk intervention, by providing verification of multiple authentication methods that the administrator can control.	Microsoft 365 E3 or E5
Microsoft Entra password protection	Detect and block known weak passwords and their variants and additional weak terms that are specific to your organization. Default global banned password lists are automatically applied to all users in a Microsoft Entra tenant. You can define additional entries in a custom banned password list. When users change or reset their passwords, these banned password lists are checked to enforce the use of strong passwords.	Microsoft 365 E3 or E5

Next steps

Use these steps to deploy an identity model and authentication infrastructure for your Microsoft 365 tenant:

1. [Determine your cloud identity model.](#)
2. [Protect your Microsoft 365 privileged accounts.](#)
3. [Protect your Microsoft 365 user accounts.](#)
4. Deploy your cloud identity model: [cloud-only](#) or [hybrid](#).

Deploy your identity infrastructure for Microsoft 365



Additional Microsoft cloud identity resources

Manage

To manage your Microsoft cloud identity deployment, see:

- [User accounts](#)
- [Licenses](#)
- [Passwords](#)
- [Groups](#)
- [Governance](#)
- [Directory synchronization](#)

How Microsoft does identity for Microsoft 365

Learn how IT experts at Microsoft [manage identities and secure access](#).

ⓘ Note

This IT Showcase resource is available only in English.

How Contoso did identity for Microsoft 365

For an example of how a fictional but representative multinational organization has deployed a hybrid identity infrastructure for Microsoft 365 cloud services, see [Identity for the Contoso Corporation](#).

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Step 1. Determine your cloud identity model

Article • 12/28/2023

Check out all of our small business content on [Small business help & learning](#).

Microsoft 365 uses Microsoft Entra ID, a cloud-based user identity and authentication service that is included with your Microsoft 365 subscription, to manage identities and authentication for Microsoft 365. Getting your identity infrastructure configured correctly is vital to managing Microsoft 365 user access and permissions for your organization.

Before you begin, watch this video for an overview of identity models and authentication for Microsoft 365.

<https://www.microsoft.com/en-us/videoplayer/embed/RE2Pjwu?postJsllMsg=true>

Your first planning choice is your cloud identity model.

Microsoft cloud identity models

To plan for user accounts, you first need to understand the two identity models in Microsoft 365. You can maintain your organization's identities only in the cloud, or you can maintain your on-premises Active Directory Domain Services (AD DS) identities and use them for authentication when users access Microsoft 365 cloud services.

Here are the two types of identity and their best fit and benefits.

[+] Expand table

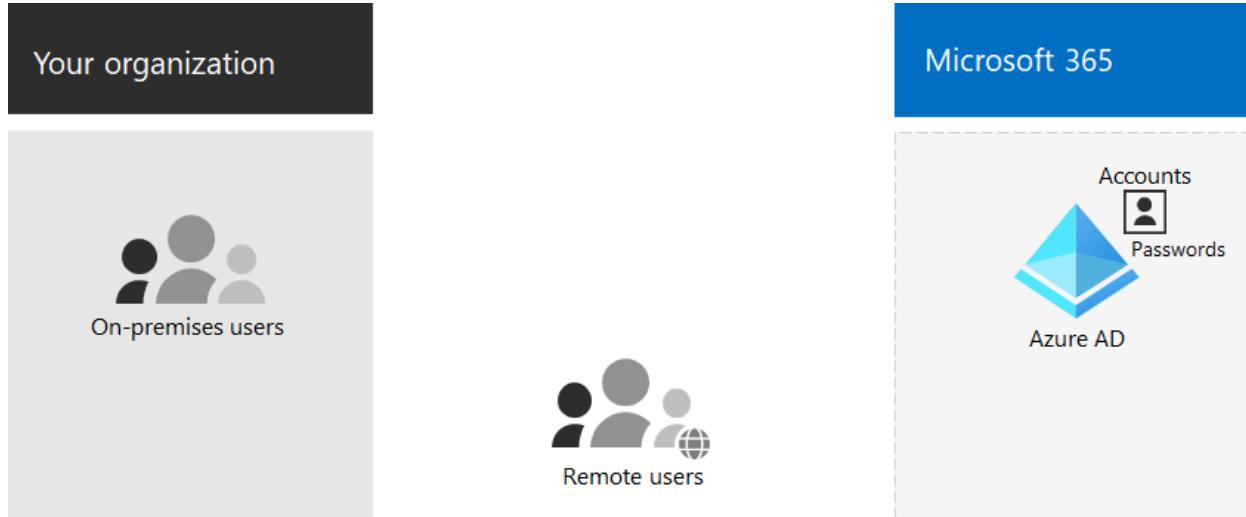
Attribute	Cloud-only identity	Hybrid identity
Definition	User account only exists in the Microsoft Entra tenant for your Microsoft 365 subscription.	User account exists in AD DS and a copy is also in the Microsoft Entra tenant for your Microsoft 365 subscription. The user account in Microsoft Entra ID might also include a hashed version of the already hashed AD DS user account password.
How Microsoft 365 authenticates user credentials	The Microsoft Entra tenant for your Microsoft 365 subscription performs the	The Microsoft Entra tenant for your Microsoft 365 subscription either handles the authentication process or redirects the user to another identity provider.

Attribute	Cloud-only identity	Hybrid identity
	authentication with the cloud identity account.	
Best for	Organizations that do not have or need an on-premises AD DS.	Organizations using AD DS or another identity provider.
Greatest benefit	Simple to use. No extra directory tools or servers required.	Users can use the same credentials when accessing on-premises or cloud-based resources.

Cloud-only identity

A cloud-only identity uses user accounts that exist only in Microsoft Entra ID. Cloud-only identity is typically used by small organizations that do not have on-premises servers or do not use AD DS to manage local identities.

Here are the basic components of cloud-only identity.



Both on-premises and remote (online) users use their Microsoft Entra user accounts and passwords to access Microsoft 365 cloud services. Microsoft Entra authenticates user credentials based on its stored user accounts and passwords.

Administration

Because user accounts are only stored in Microsoft Entra ID, you manage cloud identities with tools such as the [Microsoft 365 admin center](#) and [Windows PowerShell](#).

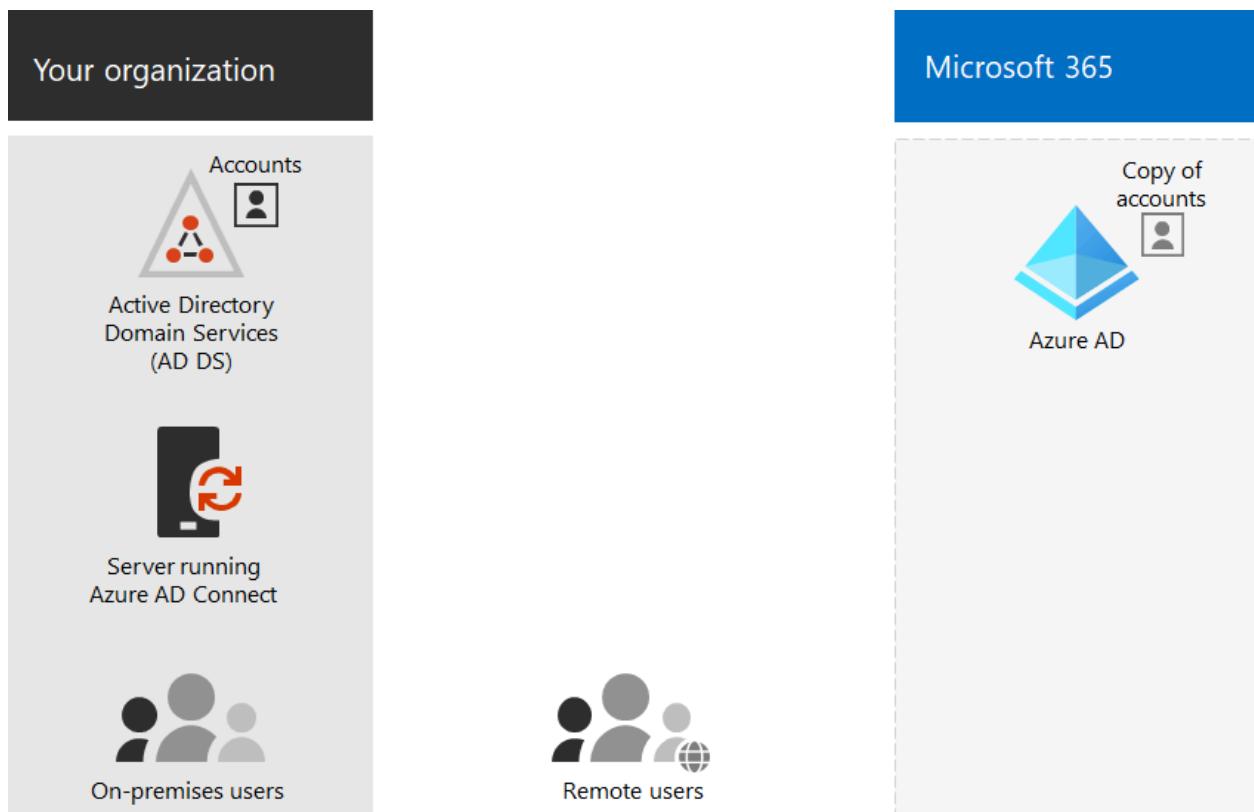
Hybrid identity

Hybrid identity uses accounts that originate in an on-premises AD DS and have a copy in the Microsoft Entra tenant of a Microsoft 365 subscription. Most changes, with the exception of [specific account attributes](#), only flow one way. Changes that you make to AD DS user accounts are synchronized to their copy in Microsoft Entra ID.

Microsoft Entra Connect provides the ongoing account synchronization. It runs on an on-premises server, checks for changes in the AD DS, and forwards those changes to Microsoft Entra ID. Microsoft Entra Connect provides the ability to filter which accounts are synchronized and whether to synchronize a hashed version of user passwords, known as password hash synchronization (PHS).

When you implement hybrid identity, your on-premises AD DS is the authoritative source for account information. This means that you perform administration tasks mostly on-premises, which are then synchronized to Microsoft Entra ID.

Here are the components of hybrid identity.



The Microsoft Entra tenant has a copy of the AD DS accounts. In this configuration, both on-premises and remote users accessing Microsoft 365 cloud services authenticate against Microsoft Entra ID.

ⓘ Note

You always need to use Microsoft Entra Connect to synchronize user accounts for hybrid identity. You need the synchronized user accounts in Microsoft Entra ID to

perform license assignment and group management, configure permissions, and other administrative tasks that involve user accounts.

Hybrid identity and directory synchronization for Microsoft 365

Depending on your business needs and technical requirements, the hybrid identity model and directory synchronization is the most common choice for enterprise customers who are adopting Microsoft 365. Directory synchronization allows you to manage identities in your Active Directory Domain Services (AD DS) and all updates to user accounts, groups, and contacts are synchronized to the Microsoft Entra tenant of your Microsoft 365 subscription.

ⓘ Note

When AD DS user accounts are synchronized for the first time, they are not automatically assigned a Microsoft 365 license and cannot access Microsoft 365 services, such as email. You must first assign them a usage location. Then, assign a license to these user accounts, either individually or dynamically through group membership.

Authentication for hybrid identity

There are two types of authentication when using the hybrid identity model:

- Managed authentication

Microsoft Entra ID handles the authentication process by using a locally-stored hashed version of the password or sends the credentials to an on-premises software agent to be authenticated by the on-premises AD DS.

- Federated authentication

Microsoft Entra ID redirects the client computer requesting authentication to another identity provider.

Managed authentication

There are two types of managed authentication:

- Password hash synchronization (PHS)

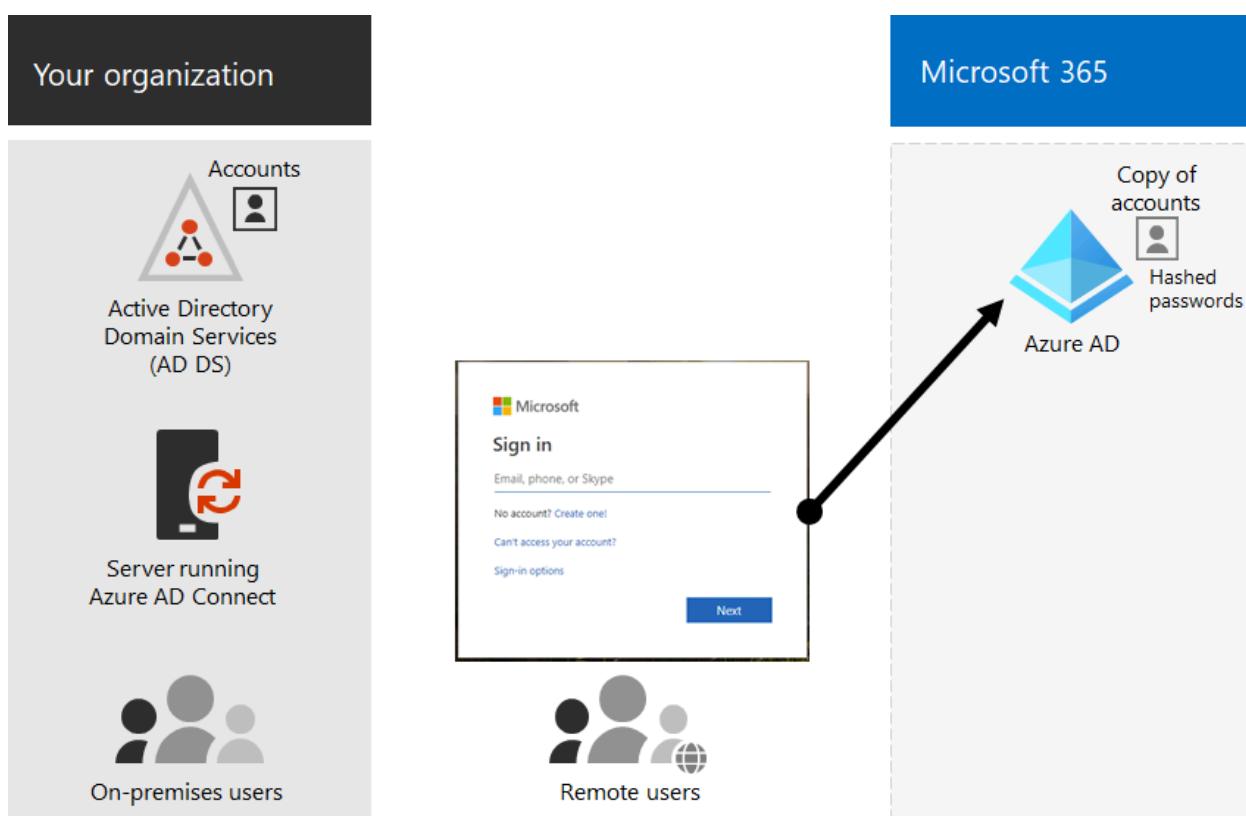
Microsoft Entra ID performs the authentication itself.

- Pass-through authentication (PTA)

Microsoft Entra ID has AD DS perform the authentication.

Password hash synchronization (PHS)

With PHS, you synchronize your AD DS user accounts with Microsoft 365 and manage your users on-premises. Hashes of user passwords are synchronized from your AD DS to Microsoft Entra ID so that the users have the same password on-premises and in the cloud. This is the simplest way to enable authentication for AD DS identities in Microsoft Entra ID.

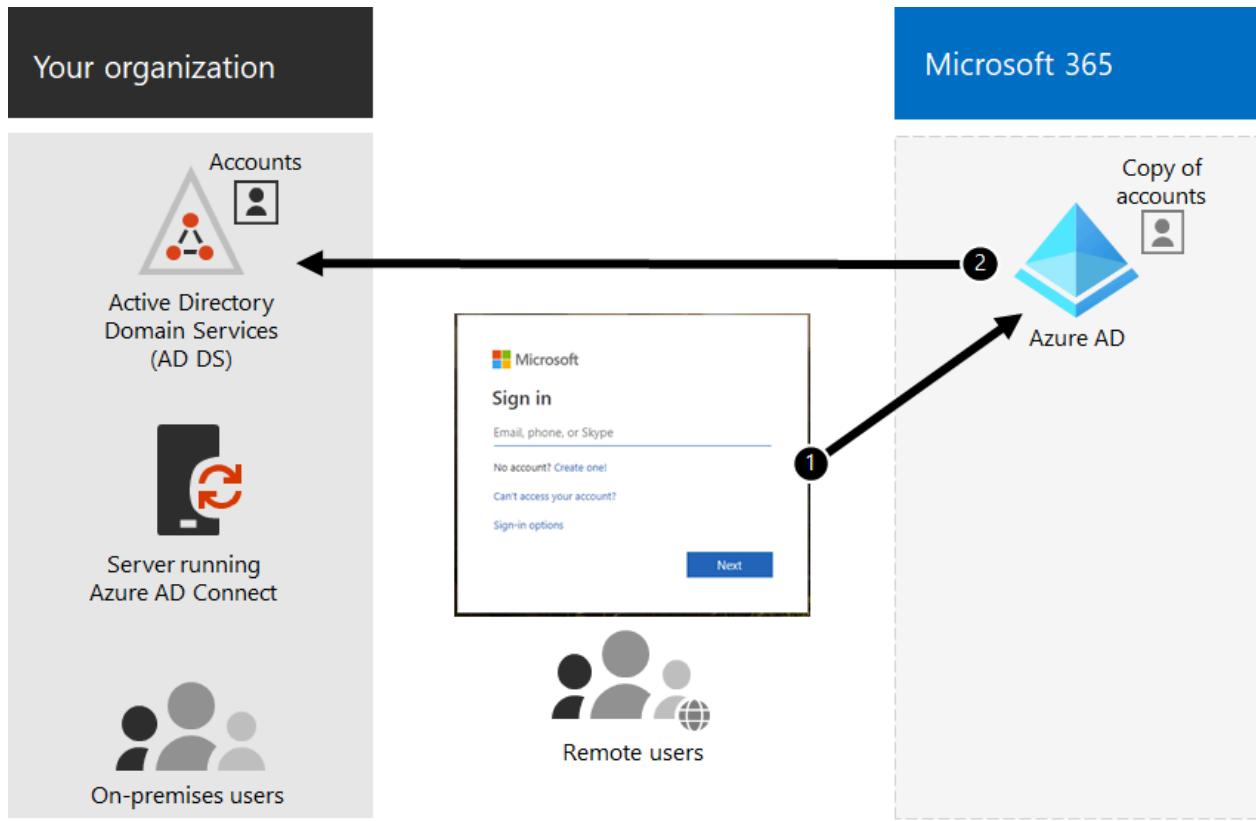


When passwords are changed or reset on-premises, the new password hashes are synchronized to Microsoft Entra ID so that your users can always use the same password for cloud resources and on-premises resources. The user passwords are never sent to Microsoft Entra ID or stored in Microsoft Entra ID in clear text. Some premium features of Microsoft Entra ID, such as Identity Protection, require PHS regardless of which authentication method is selected.

See [choosing the right authentication method](#) to learn more.

Pass-through authentication (PTA)

PTA provides a simple password validation for Microsoft Entra authentication services using a software agent running on one or more on-premises servers to validate the users directly with your AD DS. With PTA, you synchronize AD DS user accounts with Microsoft 365 and manage your users on-premises.



PTA allows your users to sign in to both on-premises and Microsoft 365 resources and applications using their on-premises account and password. This configuration validates users' passwords directly against your on-premises AD DS without storing password hashes in Microsoft Entra ID.

PTA is also for organizations with a security requirement to immediately enforce on-premises user account states, password policies, and logon hours.

See [choosing the right authentication method](#) to learn more.

Federated authentication

Federated authentication is primarily for large enterprise organizations with more complex authentication requirements. AD DS identities are synchronized with Microsoft 365 and users' accounts are managed on-premises. With federated authentication, users have the same password on-premises and in the cloud and they do not have to sign in again to use Microsoft 365.

Federated authentication can support additional authentication requirements, such as smartcard-based authentication or a third-party multi-factor authentication and is

typically required when organizations have an authentication requirement not natively supported by Microsoft Entra ID.

See [choosing the right authentication method](#) to learn more.

For third-party authentication and identity providers, on-premises directory objects may be synchronized to Microsoft 365 and cloud resource access that are primarily managed by a third-party identity provider (IdP). If your organization uses a third-party federation solution, you can configure sign-on with that solution for Microsoft 365 provided that the third-party federation solution is compatible with Microsoft Entra ID.

See the [Microsoft Entra federation compatibility list](#) to learn more.

Administration

Because the original and authoritative user accounts are stored in the on-premises AD DS, you manage your identities with the same tools as you manage your AD DS.

You don't use the Microsoft 365 admin center or PowerShell for Microsoft 365 to manage synchronized user accounts in Microsoft Entra ID.

Next step



Continue with [Step 2](#) to secure your global administrator accounts.

Feedback

Was this page helpful?

Yes

No

[Provide product feedback ↗](#)

Step 2. Protect your Microsoft 365 privileged accounts

Article • 12/28/2023

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Check out all of our small business content on [Small business help & learning](#).

Security breaches of a Microsoft 365 tenant, including information harvesting and phishing attacks, are typically done by compromising the credentials of a Microsoft 365 privileged account. Security in the cloud is a partnership between you and Microsoft:

- Microsoft cloud services are built on a foundation of trust and security. Microsoft provides you security controls and capabilities to help you protect your data and applications.
- You own your data and identities and the responsibility for protecting them, the security of your on-premises resources, and the security of cloud components you control.

Microsoft provides capabilities to help protect your organization, but they're effective only if you use them. If you don't use them, you may be vulnerable to attack. To protect your privileged accounts, Microsoft is here to help you with detailed instructions to:

1. Create dedicated, privileged, cloud-based accounts and use them only when necessary.
2. Configure multi-factor authentication (MFA) for your dedicated Microsoft 365 privileged accounts and use the strongest form of secondary authentication.
3. Protect privileged accounts with Zero Trust identity and device access recommendations.

Note

To secure your privileged roles, check out [Best practices for Microsoft Entra roles](#) to secure privileged access to your tenant.

1. Create dedicated, privileged, cloud-based user accounts and use them only when

necessary

Instead of using everyday user accounts that have been assigned administrator roles, create dedicated user accounts that have the admin roles in Microsoft Entra ID.

From this moment onward, you sign in with the dedicated privileged accounts only for tasks that require administrator privileges. All other Microsoft 365 administration must be done by assigning other administration roles to user accounts.

ⓘ Note

This does require additional steps to sign out as your everyday user account and sign in with a dedicated administrator account. But this only needs to be done occasionally for administrator operations. Consider that recovering your Microsoft 365 subscription after an administrator account breach requires a lot more steps.

You also need to create [emergency access accounts](#) to prevent being accidentally locked out of Microsoft Entra ID.

You can further protect your privileged accounts with Microsoft Entra Privileged Identity Management (PIM) for on-demand, just-in-time assignment of administrator roles.

2. Configure multi-factor authentication for your dedicated Microsoft 365 privileged accounts

Multi-factor authentication (MFA) requires additional information beyond the account name and password. Microsoft 365 supports these extra verification methods:

- The Microsoft Authenticator app
- A phone call
- A randomly generated verification code sent through a text message
- A smart card (virtual or physical) (requires federated authentication)
- A biometric device
- Oauth token

ⓘ Note

For organizations that must adhere to National Institute of Standards and Technology (NIST) standards, the use of a phone call or text message-based

additional verification methods are restricted. Click [here](#) for the details.

If you're a small business that is using user accounts stored only in the cloud (the cloud-only identity model), [set up MFA](#) to configure MFA using a phone call or a text message verification code sent to a smart phone for each dedicated privileged account.

If you're a larger organization that is using a Microsoft 365 hybrid identity model, you have more verification options. If you have the security infrastructure already in place for a stronger secondary authentication method, [set up MFA](#) and configure each dedicated privileged account for the appropriate verification method.

If the security infrastructure for the desired stronger verification method isn't in place and functioning for Microsoft 365 MFA, we strongly recommend that you configure dedicated privileged accounts with MFA using the Microsoft Authenticator app, a phone call, or a text message verification code sent to a smart phone for your privileged accounts as an interim security measure. Don't leave your dedicated privileged accounts without the extra protection provided by MFA.

For more information, see [MFA for Microsoft 365](#).

3. Protect administrator accounts with Zero Trust identity and device access recommendations

To help ensure a secure and productive workforce, Microsoft provides a set of recommendations for [identity and device access](#). For identity, use the recommendations and settings in these articles:

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

Additional protections for enterprise organizations

Use these additional methods to ensure that your privileged account, and the configuration that you perform using it, are as secure as possible.

Privileged access workstation

To ensure that the execution of highly privileged tasks is as secure as possible, use a privileged access workstation (PAW). A PAW is a dedicated computer that is only used for sensitive configuration tasks, such as Microsoft 365 configuration that requires a privileged account. Because this computer isn't used daily for Internet browsing or email, it's better protected from Internet attacks and threats.

For instructions on how to set up a PAW, see [Securing devices as part of the privileged access story](#).

To enable Azure PIM for your Microsoft Entra tenant and 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 Microsoft Entra ID](#).

Privileged Identity Management

Rather than having your privileged accounts be permanently assigned an administrator role, you can use PIM to enable on-demand, just-in-time assignment of the administrator role when it's needed.

Your administrator accounts go from being permanent admins to eligible admins. The administrator role is inactive until someone needs it. You then complete an activation process to add the administrator role to the privileged account for a predetermined amount of time. When the time expires, PIM removes the administrator role from the privileged account.

Using PIM and this process significantly reduces the amount of time that your privileged accounts are vulnerable to attack and use by malicious users.

Using this feature requires either Microsoft Entra ID Governance or Microsoft Entra ID P2 subscriptions. To find the right license for your requirements, see [Compare generally available features of Microsoft Entra ID](#).

For information about licenses for users, see [License requirements to use Privileged Identity Management](#).

For more information, see:

- [Privileged Identity Management](#).
- [Securing privileged access for hybrid and cloud deployments in Microsoft Entra ID](#)

Privileged access management

Privileged access management is enabled by configuring policies that specify just-in-time access for task-based activities in your 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 tenant.

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

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

Privileged access management enables 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 approval policy must request and be granted access approval.

To enable privileged access management, see [Get started with privileged access management](#).

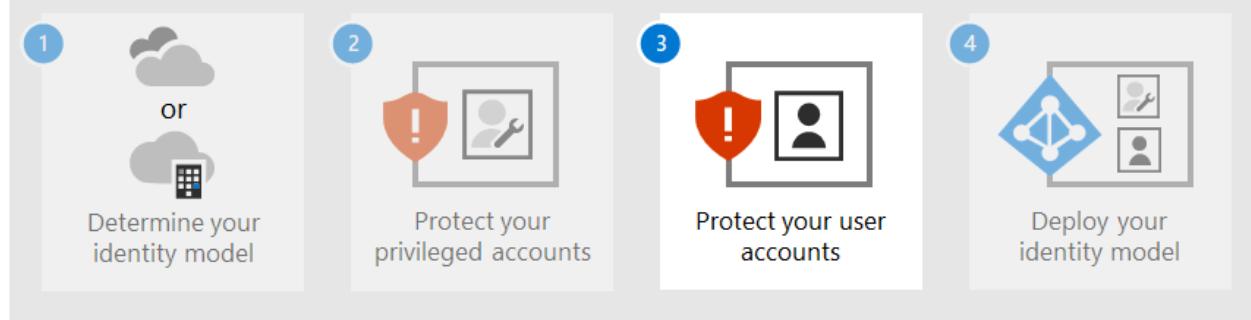
For more information, see [Learn about privileged access management](#).

Security information and event management (SIEM) software for Microsoft 365 logging

SIEM software run on a server performs real-time analysis of security alerts and events created by applications and network hardware. To allow your SIEM server to include Microsoft 365 security alerts and events in its analysis and reporting functions, integrate Microsoft Entra ID into your SEIM. See [Introduction to Azure Log Integration](#).

Next step

Deploy your identity infrastructure for Microsoft 365



Continue with [Step 3](#) to secure your user accounts.

Feedback

Was this page helpful?

Yes

No

[Provide product feedback ↗](#)

Step 3: Protect your Microsoft 365 user accounts

Article • 04/12/2024

Check out all of our small business content on [Small business help & learning](#).

To increase the security of user sign-ins:

- Use Windows Hello for Business
- Use Microsoft Entra Password Protection
- Use multifactor authentication (MFA)
- Deploy identity and device access configurations
- Protect against credential compromise with Microsoft Entra ID Protection

Windows Hello for Business

Windows Hello for Business in Windows 11 Enterprise replaces passwords with strong two-factor authentication when signing on a Windows device. The two factors are a new type of user credential that is tied to a device and a biometric or PIN.

For more information, see [Windows Hello for Business Overview](#).

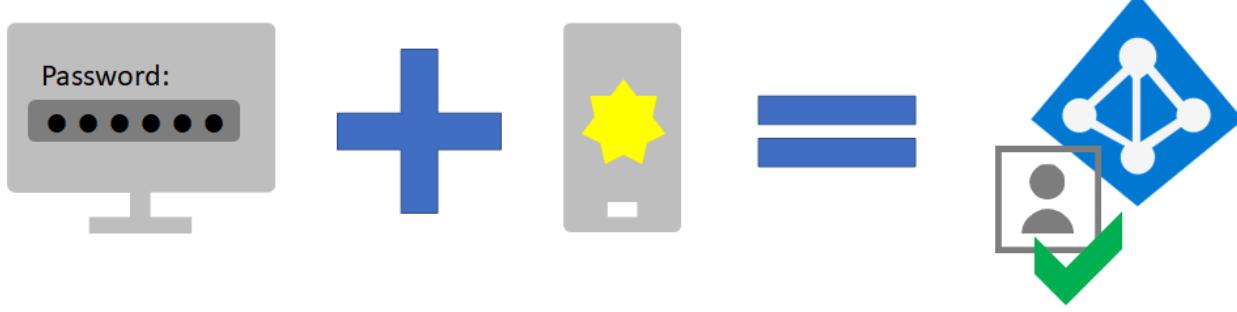
Microsoft Entra Password Protection

Microsoft Entra Password Protection detects and blocks known weak passwords and their variants and can also block additional weak terms that are specific to your organization. Default global banned password lists are automatically applied to all users in a Microsoft Entra tenant. You can define additional entries in a custom banned password list. When users change or reset their passwords, these banned password lists are checked to enforce the use of strong passwords.

For more information, see [Configure Microsoft Entra password protection](#).

MFA

MFA requires that user sign-ins be subject to an additional verification beyond the user account password. Even if a malicious user determines a user account password, they must also be able to respond to an additional verification, such as a text message sent to a smartphone before access is granted.



Your first step in using MFA is to [require it for all administrator accounts](#), also known as privileged accounts. Beyond this first step, Microsoft recommends MFA For all users.

There are three ways to require your users to use MFA based on your Microsoft 365 plan.

[\[\] Expand table](#)

Plan	Recommendation
All Microsoft 365 plans (without Microsoft Entra ID P1 or P2 licenses)	Enable security defaults in Microsoft Entra ID . Security defaults in Microsoft Entra ID include MFA for users and administrators.
Microsoft 365 E3 (includes Microsoft Entra ID P1 licenses)	Use the common Conditional Access policies to configure the following policies: - Require MFA for administrators - Require MFA for all users - Block legacy authentication
Microsoft 365 E5 (includes Microsoft Entra ID P2 licenses)	Taking advantage of Microsoft Entra ID Protection, begin to implement Microsoft's recommended set of Conditional Access and related policies by creating these two policies: - Require MFA when sign-in risk is medium or high - High risk users must change password

Security defaults

Security defaults is a new feature for Microsoft 365 and Office 365 paid or trial subscriptions created after October 21, 2019. These subscriptions have security defaults turned on, which ***requires all of your users to use MFA with the Microsoft Authenticator app***.

Users have 14 days to register for MFA with the Microsoft Authenticator app from their smart phones, which begins from the first time they sign in after security defaults has been enabled. After 14 days have passed, the user won't be able to sign in until MFA registration is completed.

Security defaults ensure that all organizations have a basic level of security for user sign-in that is enabled by default. You can disable security defaults in favor of MFA with Conditional Access policies or for individual accounts.

For more information, see the [overview of security defaults](#).

Conditional Access policies

Conditional Access policies are a set of rules that specify the conditions under which sign-ins are evaluated and access is granted. For example, you can create a Conditional Access policy that states:

- If the user account name is a member of a group for users that are assigned the Exchange, user, password, security, SharePoint, **Exchange admin**, **SharePoint admin**, or **Global admin** roles, require MFA before allowing access.

This policy allows you to require MFA based on group membership, rather than trying to configure individual user accounts for MFA when they're assigned or unassigned from these administrator roles.

You can also use Conditional Access policies for more advanced capabilities, such as requiring that the sign-in is done from a compliant device, such as your laptop running Windows 11.

Conditional Access requires Microsoft Entra ID P1 licenses, which are included with Microsoft 365 E3 and E5.

For more information, see the [overview of Conditional Access](#).

Using these methods together

Keep the following in mind:

- You can't enable security defaults if you have any Conditional Access policies enabled.
- You can't enable any Conditional Access policies if you have security defaults enabled.

If security defaults are enabled, all new users are prompted for MFA registration and the use of the Microsoft Authenticator app.

This table shows the results of enabling MFA with security defaults and Conditional Access policies.

Method	Enabled	Disabled	Additional authentication method
Security defaults	Can't use Conditional Access policies	Can use Conditional Access policies	Microsoft Authenticator app
Conditional Access policies	If any are enabled, you can't enable security defaults	If all are disabled, you can enable security defaults	User specifies during MFA registration

Zero Trust identity and device access configurations

Zero Trust identity and device access settings and policies are recommended prerequisite features and their settings combined with Conditional Access, Intune, and Microsoft Entra ID Protection policies that determine whether a given access request should be granted and under what conditions. This determination is based on the user account of the sign-in, the device being used, the app the user is using for access, the location from which the access request is made, and an assessment of the risk of the request. This capability helps ensure that only approved users and devices can access your critical resources.

ⓘ Note

Microsoft Entra ID Protection requires Microsoft Entra ID P2 licenses, which are included with Microsoft 365 E5.

Identity and device access policies are defined to be used in three tiers:

- Baseline protection is a minimum level of security for your identities and devices that access your apps and data.
- Sensitive protection provides additional security for specific data. Identities and devices are subject to higher levels of security and device health requirements.
- Protection for environments with highly regulated or classified data is for typically small amounts of data that are highly classified, contain trade secrets, or is subject to data regulations. Identities and devices are subject to much higher levels of security and device health requirements.

These tiers and their corresponding configurations provide consistent levels of protection across your data, identities, and devices.

Microsoft highly recommends configuring and rolling out Zero Trust identity and device access policies in your organization, including specific settings for Microsoft Teams, Exchange Online, and SharePoint. For more information, see [Zero Trust identity and device access configurations](#).

Microsoft Entra ID Protection

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. Microsoft Entra ID Protection provides a number of ways to help prevent an attacker from compromising a user account's credentials.

With Microsoft Entra ID Protection, you can:

[+] [Expand table](#)

Capability	Description
Determine and address potential vulnerabilities in your organization's identities	Microsoft Entra ID uses machine learning to detect anomalies and suspicious activity, such as sign-ins and post-sign-in activities. Using this data, Microsoft Entra ID 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 Microsoft Entra ID and Microsoft Intune, can either automatically block access or take corrective actions, including password resets and requiring Microsoft Entra multifactor 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 Microsoft Entra ID Protection.](#)

See the [steps to enable Microsoft Entra ID Protection](#).

Admin technical resources for MFA and secure sign-ins

- MFA for Microsoft 365
- Deploy identity for Microsoft 365
- Azure Academy Microsoft Entra ID training videos ↗
- Configure the Microsoft Entra multifactor authentication registration policy
- Identity and device access configurations

Next step



Continue with Step 4 to deploy the identity infrastructure based on your chosen identity model:

- Cloud-only identity
- Hybrid identity

Feedback

Was this page helpful?

Yes

No

Provide product feedback ↗

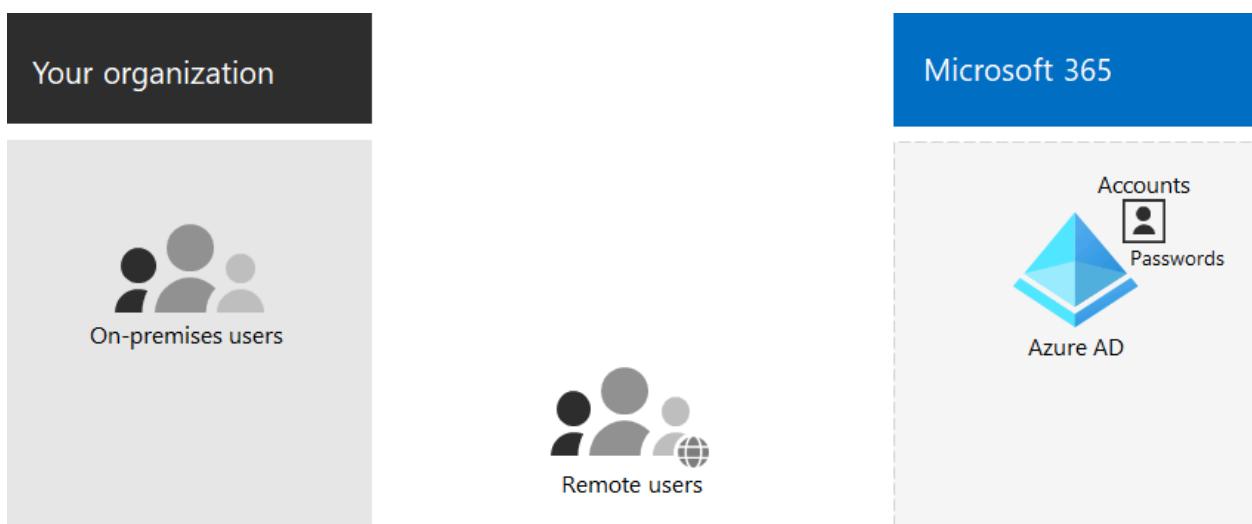
Microsoft 365 cloud-only identity

Article • 12/28/2023

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

If you have chosen the cloud-only identity model, you already have a Microsoft Entra tenant for your Microsoft 365 subscription to store all of your users, groups, and contacts. After setting up protection for administrator accounts in [Step 2](#) and user accounts in [Step 3](#) of this solution, you're now ready to begin creating the new accounts and groups that your organization needs.

Here are the basic components of cloud-only identity.



Users and their user accounts 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 in 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.

You can use groups in Microsoft Entra ID for several purposes that simplify management of your cloud environment. For example, with Microsoft Entra groups, you can:

- Use group-based licensing to assign licenses for Microsoft 365 to your user accounts automatically as soon as they're added as members.
- Add user accounts to specific groups dynamically based on user account attributes, such as department name.
- Automatically provision users for Software as a Service (SaaS) applications and to protect access to those applications with multifactor authentication (MFA) and other Conditional Access policies.
- Provision permissions and levels of access for teams and SharePoint Online team sites.

Next steps for cloud-only identity

- [Manage user accounts](#)
- [Assign licenses to user accounts](#)
- [Manage groups and group membership](#)
- [Manage user account passwords](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Prepare for directory synchronization to Microsoft 365

Article • 12/28/2023

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

If you chose the hybrid identity model and configured protection for administrator accounts in [Step 2](#) and user accounts in [Step 3](#) of this solution, your next task is to deploy directory synchronization. The benefits of directory synchronization for your organization include:

- Reducing the administrative programs in your organization
- Optionally enabling single sign-on scenario
- Automating account changes in Microsoft 365

For more information about the advantages of using directory synchronization, see [hybrid identity with Microsoft Entra ID](#).

However, directory synchronization requires planning and preparation to ensure that your Active Directory Domain Services (AD DS) synchronizes to the Microsoft Entra tenant of your Microsoft 365 subscription with a minimum of errors.

Follow these steps in order for the best results.

ⓘ Note

Non-ASCII characters do not sync for any attributes on the AD DS user account.

AD DS Preparation

To help ensure a seamless transition to Microsoft 365 by using synchronization, you must prepare your AD DS forest before you begin your Microsoft 365 directory synchronization deployment.

Your directory preparation should focus on the following tasks:

- Remove duplicate `proxyAddress` and `userPrincipalName` attributes.
- Update blank and invalid `userPrincipalName` attributes with valid `userPrincipalName` attributes.

- Remove invalid and questionable characters in the `givenName`, `surname` (`sn`), `sAMAccountName`, `displayName`, `mail`, `proxyAddresses`, `mailNickname`, and `userPrincipalName` attributes. For details about preparing attributes, see [List of attributes that are synced by the Azure Active Directory Sync Tool](#).

ⓘ Note

These are the same attributes that Microsoft Entra Connect synchronizes.

Multi-forest deployment considerations

For multiple forests and SSO options, use a [Custom Installation of Microsoft Entra Connect](#).

If your organization has multiple forests for authentication (logon forests), we highly recommend the following:

- **Consider consolidating your forests.** In general, there's more overhead required to maintain multiple forests. Unless your organization has security constraints that dictate the need for separate forests, consider simplifying your on-premises environment.
- **Use only in your primary logon forest.** Consider deploying Microsoft 365 only in your primary logon forest for your initial rollout of Microsoft 365.

If you can't consolidate your multi-forest AD DS deployment or are using other directory services to manage identities, you might be able to synchronize them with the help of Microsoft or a partner.

See [Topologies for Microsoft Entra Connect](#) for more information.

Features that are dependent on directory synchronization

Directory synchronization is required for the following features and functionality:

- Microsoft Entra seamless single sign-on (SSO)
- Skype coexistence
- Exchange hybrid deployment, including:
 - Fully shared global address list (GAL) between your on-premises Exchange environment and Microsoft 365.
 - Synchronizing GAL information from different mail systems.

- The ability to add users to and remove users from Microsoft 365 service offerings. This requires the following:
 - Two-way synchronization must be configured during directory synchronization setup. By default, directory synchronization tools write directory information only to the cloud. When you configure two-way synchronization, you enable write-back functionality so that a limited number of object attributes are copied from the cloud, and then written them back to your local AD DS. Write-back is also referred to as Exchange hybrid mode.
 - An on-premises Exchange hybrid deployment.
 - The ability to move some user mailboxes to Microsoft 365 while keeping other user mailboxes on-premises.
 - Safe senders and blocked senders on-premises are replicated to Microsoft 365.
 - Basic delegation and send-on-behalf-of email functionality.
 - You have an integrated on-premises smart card or multifactor authentication solution.
- Synchronization of photos, thumbnails, conference rooms, and security groups

1. Directory cleanup tasks

Before you synchronize your AD DS to your Microsoft Entra tenant, you need to clean up your AD DS.

ⓘ Important

If you don't perform AD DS cleanup before you synchronize, it can lead to a significant negative impact on the deployment process. It might take days, or even weeks, to go through the cycle of directory synchronization, identifying errors, and re-synchronization.

In your AD DS, complete the following clean-up tasks for each user account that will be assigned a Microsoft 365 license:

1. Ensure a valid and unique email address in the **proxyAddresses** attribute.
2. Remove any duplicate values in the **proxyAddresses** attribute.
3. If possible, ensure a valid and unique value for the **userPrincipalName** attribute in the user's **user** object. For the best synchronization experience, ensure that the AD DS UPN matches the Microsoft Entra UPN. If a user doesn't have a value for the **userPrincipalName** attribute, then the **user** object must contain a valid and unique

value for the **sAMAccountName** attribute. Remove any duplicate values in the **userPrincipalName** attribute.

4. For optimal use of the global address list (GAL), ensure the information in the following attributes of the AD DS user account is correct:

- **givenName**
- **surname**
- **displayName**
- Job Title
- Department
- Office
- Office Phone
- Mobile Phone
- Fax Number
- Street Address
- City
- State or Province
- Zip or Postal Code
- Country or Region

2. Directory object and attribute preparation

Successful directory synchronization between your AD DS and Microsoft 365 requires that your AD DS attributes are properly prepared. For example, you need to ensure that specific characters aren't used in certain attributes that are synchronized with the Microsoft 365 environment. Unexpected characters don't cause directory synchronization to fail but might return a warning. Invalid characters will cause directory synchronization to fail.

Directory synchronization will also fail if some of your AD DS users have one or more duplicate attributes. Each user must have unique attributes.

The attributes that you need to prepare are listed here:

- **displayName**
 - If the attribute exists in the user object, it's synchronized with Microsoft 365.
 - If this attribute exists in the user object, there must be a value for it. That is, the attribute must not be blank.
 - Maximum number of characters: 256
- **givenName**

- If the attribute exists in the user object, it's synchronized with Microsoft 365, but Microsoft 365 doesn't require or use it.
- Maximum number of characters: 64
- **mail**
- The attribute value must be unique within the directory.

 **Note**

If there are duplicate values, the first user with the value is synchronized. Subsequent users will not appear in Microsoft 365. You must modify either the value in Microsoft 365 or modify both of the values in AD DS in order for both users to appear in Microsoft 365.

- **mailNickname** (Exchange alias)

- The attribute value can't begin with a period (.).
- The attribute value must be unique within the directory.

 **Note**

Underscores ("_") in the synchronized name indicates that the original value of this attribute contains invalid characters. For more information on this attribute, see [Exchange alias attribute](#).

- **proxyAddresses**

- Multiple-value attribute
- Maximum number of characters per value: 256
- The attribute value must not contain a space.
- The attribute value must be unique within the directory.
- Invalid characters: < > () ; , [] "
- Letters with diacritical marks, such as umlauts, accents, and tildes, are invalid characters.

The invalid characters apply to the characters following the type delimiter and ":"; such that SMTP:User@contoso.com is allowed, but

SMTP:user:M@contoso.com isn't.

Important

All Simple Mail Transport Protocol (SMTP) addresses should comply with email messaging standards. Remove duplicate or unwanted addresses if they exist.

- **sAMAccountName**

- Maximum number of characters: 20
- The attribute value must be unique within the directory.
- Invalid characters: [\ " | , / : < > + = ; ? *]
- If a user has an invalid **sAMAccountName** attribute but has a valid **userPrincipalName** attribute, the user account is created in Microsoft 365.
- If both **sAMAccountName** and **userPrincipalName** are invalid, the AD DS **userPrincipalName** attribute must be updated.

- **sn** (surname)

- If the attribute exists in the user object, it's synchronized with Microsoft 365, but Microsoft 365 doesn't require or use it.

- **targetAddress**

It's required that the **targetAddress** attribute (for example, SMTP:tom@contoso.com) that's populated for the user must appear in the Microsoft 365 GAL. In third-party messaging migration scenarios, this would require the Microsoft 365 schema extension for the AD DS. The Microsoft 365 schema extension would also add other useful attributes to manage Microsoft 365 objects that are populated by using a directory synchronization tool from AD DS. For example, the **msExchHideFromAddressLists** attribute to manage hidden mailboxes or distribution groups would be added.

- Maximum number of characters: 256
- The attribute value must not contain a space.
- The attribute value must be unique within the directory.
- Invalid characters: \ < > () ; , [] "
- All Simple Mail Transport Protocol (SMTP) addresses should comply with email messaging standards.

- **userPrincipalName**

- The **userPrincipalName** attribute must be in the Internet-style sign-in format where the user name is followed by the at sign (@) and a domain name: for

example, user@contoso.com. All Simple Mail Transport Protocol (SMTP) addresses should comply with email messaging standards.

- The maximum number of characters for the **userPrincipalName** attribute is 113. A specific number of characters are permitted before and after the at sign (@), as follows:
 - Maximum number of characters for the username that is in front of the at sign (@): 64
 - Maximum number of characters for the domain name following the at sign (@): 48
 - Invalid characters: \ % & * + / = ? { } | < > () ; : , [] "
 - Characters allowed: A – Z, a – z, 0 – 9, ' . - _ ! # ^ ~
 - Letters with diacritical marks, such as umlauts, accents, and tildes, are invalid characters.
 - The @ character is required in each **userPrincipalName** value.
 - The @ character can't be the first character in each **userPrincipalName** value.
 - The username can't end with a period (.), an ampersand (&), a space, or an at sign (@).
 - The username can't contain any spaces.
 - Routable domains must be used; for example, local or internal domains can't be used.
 - Unicode is converted to underscore characters.
 - **userPrincipalName** can't contain any duplicate values in the directory.

3. Prepare the **userPrincipalName** attribute

Active Directory is designed to allow the end users in your organization to sign in to your directory by using either **sAMAccountName** or **userPrincipalName**. Similarly, end users can sign in to Microsoft 365 by using the user principal name (UPN) of their work or school account. Directory synchronization attempts to create new users in Microsoft Entra ID by using the same UPN that's in your AD DS. The UPN is formatted like an email address.

In Microsoft 365, the UPN is the default attribute that's used to generate the email address. It's easy to get **userPrincipalName** (in AD DS and in Microsoft Entra ID) and the primary email address in **proxyAddresses** set to different values. When they're set to different values, there can be confusion for administrators and end users.

It's best to align these attributes to reduce confusion. To meet the requirements of single sign-on with Active Directory Federation Services (AD FS) 2.0, you need to ensure that the UPNs in Microsoft Entra ID and your AD DS match and are using a valid domain namespace.

4. Add an alternative UPN suffix to AD DS

You might need to add an alternative UPN suffix to associate the user's corporate credentials with the Microsoft 365 environment. A UPN suffix is the part of a UPN to the right of the @ character. UPNs that are used for single sign-on can contain letters, numbers, periods, dashes, and underscores, but no other types of characters.

For more information on how to add an alternative UPN suffix to Active Directory, see [Prepare for directory synchronization](#).

5. Match the AD DS UPN with the Microsoft 365 UPN

If you've already set up directory synchronization, the user's UPN for Microsoft 365 might not match the user's AD DS UPN that's defined in your AD DS. This condition can occur when a user was assigned a license before the domain was verified. To fix this, use [PowerShell to fix duplicate UPN](#) to update the user's UPN to ensure that the Microsoft 365 UPN matches the corporate user name and domain. If you're updating the UPN in the AD DS and would like it to synchronize with the Microsoft Entra identity, you need to remove the user's license in Microsoft 365 prior to making the changes in AD DS.

Also see [How to prepare a non-routable domain \(such as .local domain\) for directory synchronization](#).

Next steps

After you've completed steps 1 through 5, see [Set up directory synchronization](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Prepare a nonroutable domain for directory synchronization

Article • 05/03/2024

When you synchronize your on-premises directory with Microsoft 365, you have to have a verified domain in Microsoft Entra ID. Only the User Principal Names (UPNs) that are associated with the on-premises Active Directory Domain Services (AD DS) domain are synchronized. However, any UPN that contains a nonroutable domain, such as `.local` (example: billa@contoso.local), is synchronized to an `.onmicrosoft.com` domain (example: billa@contoso.onmicrosoft.com).

If you currently use a `.local` domain for your user accounts in AD DS, we recommend that you change them to use a verified domain. For example, billa@contoso.com, in order to properly synchronize with your Microsoft 365 domain.

What if I only have a `.local` on-premises domain?

You use Microsoft Entra Connect for synchronizing your AD DS to the Microsoft Entra tenant of your Microsoft 365 tenant. For more information, see [Integrating your on-premises identities with Microsoft Entra ID](#).

Microsoft Entra Connect synchronizes your users' UPN and password so that users can sign in with the same credentials they use on-premises. However, Microsoft Entra Connect only synchronizes users to domains that are verified by Microsoft 365. Microsoft Entra ID verifies the domain, as it manages Microsoft 365 identities. In other words, the domain has to be a valid Internet domain (such as, .com, .org, .NET, .us). If your internal AD DS only uses a nonroutable domain (for example, `.local`), this can't possibly match the verified domain you have for your Microsoft 365 tenant. You can fix this issue by either changing your primary domain in your on-premises AD DS, or by adding one or more UPN suffixes.

Change your primary domain

Change your primary domain to a domain you've verified in Microsoft 365, for example, contoso.com. Every user that has the domain `contoso.local` is then updated to contoso.com. This is an involved process, however, and an easier solution is described in the following section.

Add UPN suffixes and update your users to them

You can solve the `.local` problem by registering new UPN suffix or suffixes in AD DS to match the domain (or domains) you verified in Microsoft 365. After you register the new suffix, you update the user UPNs to replace the `.local` with the new domain name, for example, so that a user account looks like billa@contoso.com.

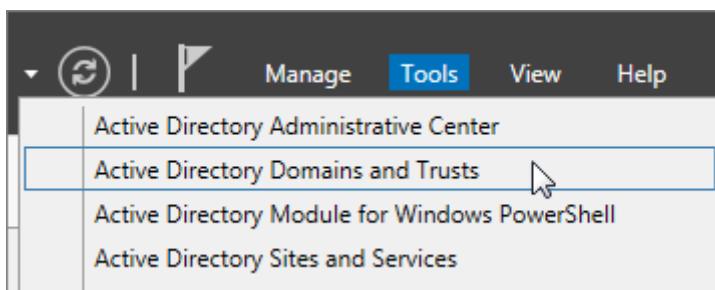
After you update the UPNs to use the verified domain, you're ready to synchronize your on-premises AD DS with Microsoft 365.

Step 1: Add the new UPN suffix

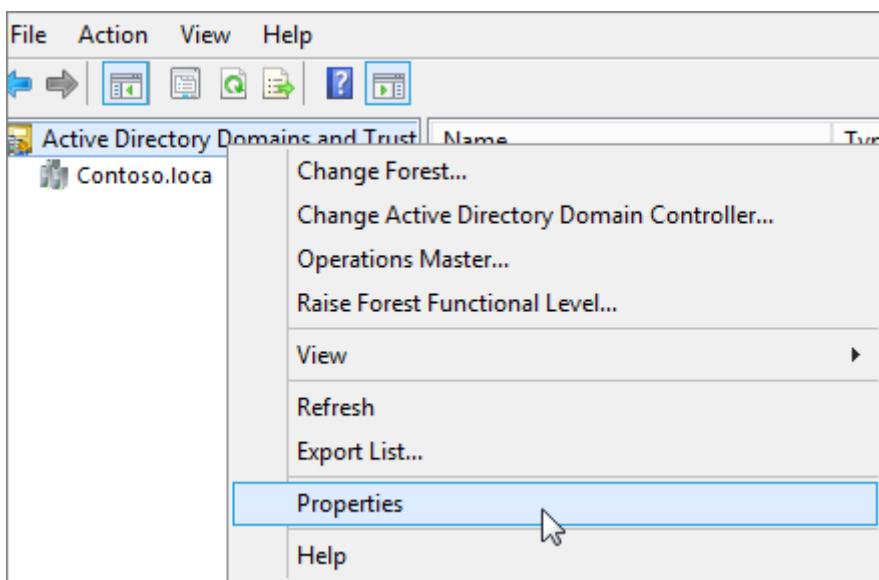
1. On the AD DS domain controller, in the Server Manager choose **Tools > Active Directory Domains and Trusts**.

Or, if you don't have Windows Server 2012

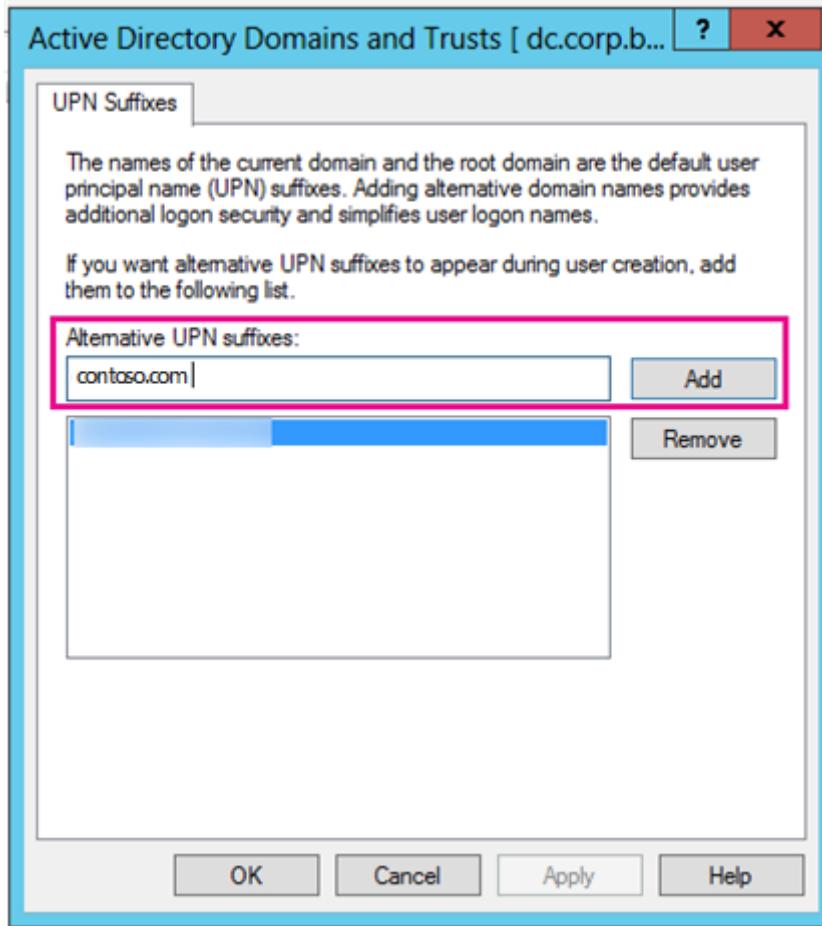
Press **Windows key + R** to open the Run dialog, and then type in `Domain.msc`, and then choose **OK**.



2. In the Active Directory Domains and Trusts window, right-click **Active Directory Domains and Trusts**, and then choose **Properties**.



3. On the UPN Suffixes tab, in the Alternative UPN Suffixes box, type your new UPN suffix or suffixes, and then choose **Add > Apply**.



Choose **OK** when you're done adding suffixes.

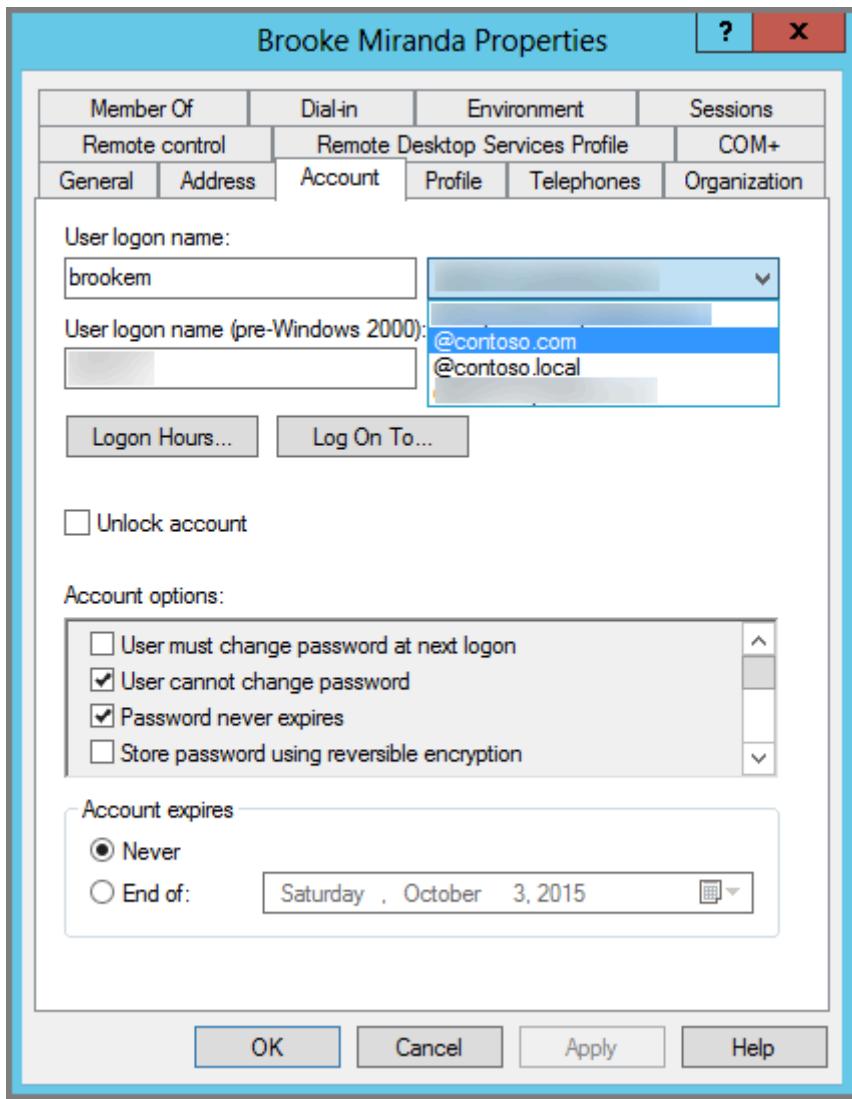
Step 2: Change the UPN suffix for existing users

1. On the AD DS domain controller, in the Server Manager choose **Tools > Active Directory Users and Computers**.

Or, if you don't have Windows Server 2012

Press **Windows key + R** to open the **Run** dialog, and then type in **Dsa.msc**, and then select **OK**

2. Select a user, right-click, and then choose **Properties**.
3. On the **Account** tab, in the UPN suffix drop-down list, choose the new UPN suffix, and then choose **OK**.



4. Complete these steps for every user.

Use PowerShell to change the UPN suffix for all of your users

If you have numerous user accounts to update, it's easier to use PowerShell. The following example uses the cmdlets `Get-ADUser` and `Set-ADUser` to change all `contoso.local` suffixes to `contoso.com` in AD DS.

For example, you could run the following PowerShell commands to update all `contoso.local` suffixes to `contoso.com`:

```
PowerShell

$LocalUsers = Get-ADUser -Filter "UserPrincipalName -like '*contoso.local'"
-Properties userPrincipalName -ResultSetSize $null
$LocalUsers | foreach {$newUpn =
$_ .UserPrincipalName.Replace("@contoso.local", "@contoso.com"); $_ | Set-
ADUser -UserPrincipalName $newUpn}
```

See [Active Directory Windows PowerShell module](#) to learn more about using Windows PowerShell in AD DS.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

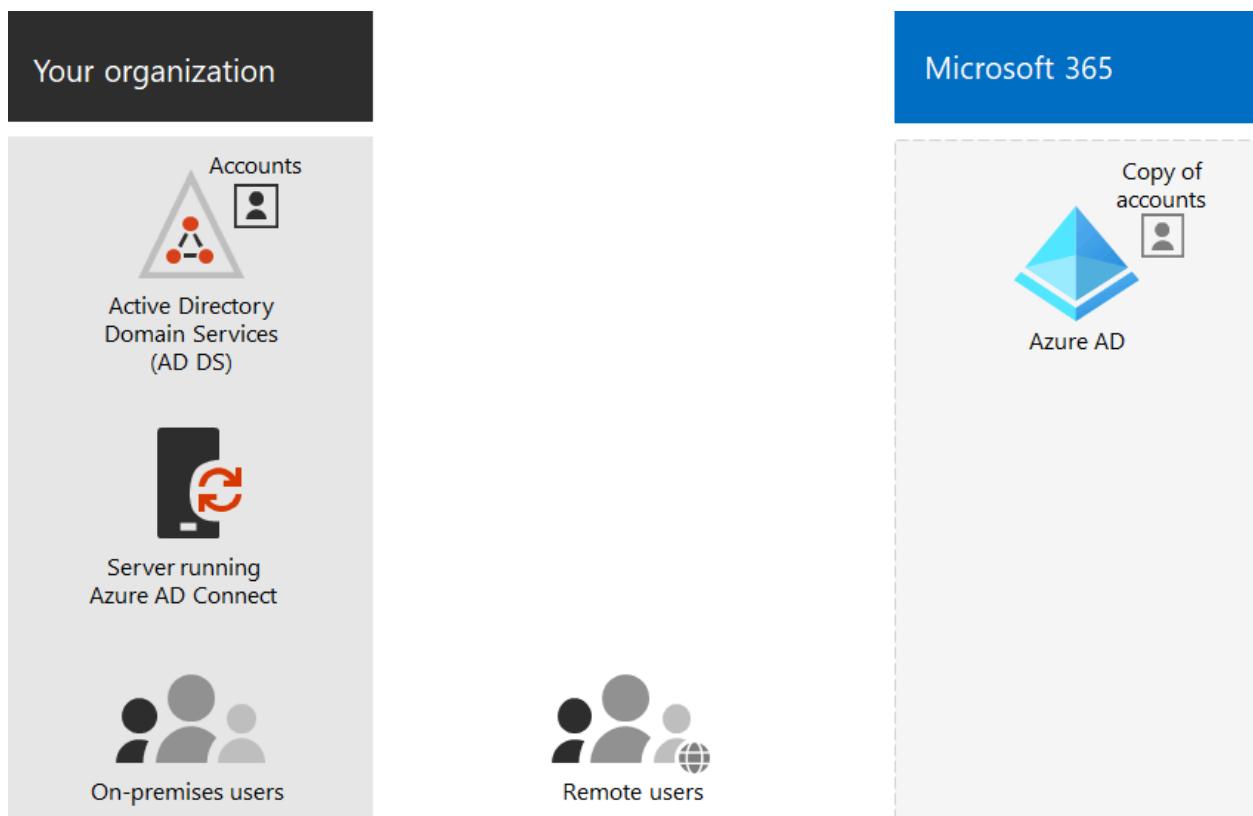
Set up directory synchronization for Microsoft 365

Article • 07/16/2024

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Microsoft 365 uses a Microsoft Entra tenant to store and manage identities for authentication and permissions to access cloud-based resources.

If you have an on-premises Active Directory Domain Services (AD DS) domain or forest, you can synchronize your AD DS user accounts, groups, and contacts with the Microsoft Entra tenant of your Microsoft 365 subscription. This is hybrid identity for Microsoft 365. Here are its components.



Microsoft Entra Connect runs on an on-premises server and synchronizes your AD DS with the Microsoft Entra tenant. Along with directory synchronization, you can also specify these authentication options:

- Password hash synchronization (PHS)

Microsoft Entra ID performs the authentication itself.

- Pass-through authentication (PTA)

Microsoft Entra ID has AD DS perform the authentication.

- Federated authentication

Microsoft Entra ID refers the client computer requesting authentication to another identity provider.

See [Hybrid identities](#) for more information.

1. Review prerequisites for Microsoft Entra Connect

You get a free Microsoft Entra subscription with your Microsoft 365 subscription. When you set up directory synchronization, you'll install Microsoft Entra Connect on one of your on-premises servers.

For Microsoft 365 you'll need to:

- Verify your on-premises domain. The Microsoft Entra Connect wizard guides you through this.
- Obtain the user names and passwords for the admin accounts of your Microsoft 365 tenant and AD DS.

For your on-premises server on which you install Microsoft Entra Connect, you'll need:

[\[\] Expand table](#)

Server OS	Other software
Windows Server 2012 R2 and later	<ul style="list-style-type: none"> - PowerShell is installed by default, no action is required. - Net 4.5.1 and later releases are offered through Windows Update. Make sure you've installed the latest updates to Windows Server in the Control Panel.
Windows Server 2008 R2 with Service Pack 1 (SP1)** or Windows Server 2012	<ul style="list-style-type: none"> - The latest version of PowerShell is available in Windows Management Framework 4.0. Search for it on Microsoft Download Center. - .NET 4.5.1 and later releases are available on Microsoft Download Center.
Windows Server 2008	<ul style="list-style-type: none"> - The latest supported version of PowerShell is available in Windows Management Framework 3.0, available on Microsoft Download Center. - .NET 4.5.1 and later releases are available on Microsoft Download Center.

See [Prerequisites for Microsoft Entra Connect](#) for the details of hardware, software, account and permissions requirements, SSL certificate requirements, and object limits for Microsoft Entra Connect.

You can also review the Microsoft Entra Connect [version release history](#) to see what is included and fixed in each release.

2. Install Microsoft Entra Connect and configure directory synchronization

Before you begin, make sure you have:

- The user name and password of a Microsoft 365 account with the Hybrid Identity Administrator role enabled
- The user name and password of an AD DS domain administrator
- Which authentication method (PHS, PTA, federated)
- Whether you want to use [Microsoft Entra seamless single sign-on \(SSO\)](#)

Follow these steps:

1. Sign in to the [Microsoft 365 admin center](#) (<https://admin.microsoft.com>) and choose **Users > Active Users** on the left navigation.
2. On the **Active users** page, choose **More** (three dots) > **Directory synchronization**.
3. On the **Microsoft Entra preparation** page, select the **Go to the Download center to get the Microsoft Entra Connect tool** link to get started.
4. Follow the steps in [Microsoft Entra Connect and Microsoft Entra Connect Health installation roadmap](#).

3. Finish setting up domains

Follow the steps in [Create DNS records for Microsoft 365 when you manage your DNS records](#) to finish setting up your domains.

Next step

[Assign licenses to user accounts](#)

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Hybrid solutions

Article • 08/27/2024

With Microsoft Azure, you can deploy some Office Server workloads that were typically deployed on-premises in Azure infrastructure services.

For Microsoft 365 identity infrastructure in Azure:

- [Using Microsoft Entra ID for SharePoint Server Authentication](#)
- [Deploy Microsoft 365 Directory Synchronization in Microsoft Azure](#)
- [Connect an on-premises network to a Microsoft Azure virtual network](#)

For SharePoint Server 2013 workloads in Azure:

- [Microsoft Azure Architectures for SharePoint 2013](#)
- [SharePoint Server 2013 Disaster Recovery in Microsoft Azure](#)
- [Internet Sites in Microsoft Azure using SharePoint Server 2013](#)

Related topics

[Microsoft 365 solution and architecture center](#)

[Microsoft cloud for enterprise architects illustrations](#)

[Architectural models for SharePoint, Exchange, Skype for Business, and Lync](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Tutorial: Implement federated authentication between Microsoft Entra ID and SharePoint on-premises

Article • 03/25/2024

Scenario description

In this tutorial, you configure a federated authentication between Microsoft Entra ID and SharePoint on-premises. The goal is to allow users to sign in on Microsoft Entra ID and use their identity to access the SharePoint on-premises sites.

Prerequisites

To perform the configuration, you need the following resources:

- A Microsoft Entra tenant. If you don't have one, you can create a [free account](#).
- A SharePoint 2013 farm or newer.

This article uses the following values:

- Enterprise application name (in Microsoft Entra ID): `SharePoint corporate farm`
- Trust identifier (in Microsoft Entra ID) / realm (in SharePoint): `urn:sharepoint:federation`
- loginUrl (to Microsoft Entra ID): `https://login.microsoftonline.com/dc38a67a-f981-4e24-ba16-4443ada44484/wsfed`
- SharePoint site URL: `https://sp/sites.contoso.local/`
- SharePoint site reply URL: `https://sp/sites.contoso.local/_trust/`
- SharePoint trust configuration name: `MicrosoftEntraTrust`
- UserPrincipalName of the Microsoft Entra test user: `AzureUser1@demo1984.onmicrosoft.com`

Configure an enterprise application in Microsoft Entra ID

To configure the federation in Microsoft Entra ID, you need to create a dedicated Enterprise application. Its configuration is simplified using the pre-configured template `SharePoint on-premises` that can be found in the application gallery.

Create the enterprise application

1. Sign in to the [Microsoft Entra admin center](#) as at least a `Cloud Application Administrator`.
2. Browse to `Identity > Applications > Enterprise applications > New application`.
3. In the search box, enter `SharePoint on-premises`. Select `SharePoint on-premises` from the result pane.
4. Specify a name for your application (in this tutorial, it is `SharePoint corporate farm`), and click `Create` to add the application.
5. In the new enterprise application, select `Properties`, and check the value for `User assignment required?`. For this scenario, set its value to `No` and click `Save`.

Configure the enterprise application

In this section, you configure the SAML authentication and define the claims that will be sent to SharePoint upon successful authentication.

1. In the Overview of the Enterprise application `SharePoint corporate farm`, select `2. Set up single sign-on` and choose the `SAML` in the next dialog.
2. On the `Set up Single Sign-On with SAML` page, select the `Edit` icon in the `Basic SAML Configuration` pane.
3. In the `Basic SAML Configuration` section, follow these steps:
 - a. In the `Identifier` box, ensure that this value is present: `urn:sharepoint:federation`.

- b. In the **Reply URL** box, enter a URL by using this pattern: `https://spsites.contoso.local/_trust/`.
 - c. In the **Sign on URL** box, enter a URL by using this pattern: `https://spsites.contoso.local/`.
 - d. Select **Save**.
4. In the **User Attributes & Claims** section, delete the following claim types, which are useless since they won't be used by SharePoint to grant permissions:

- `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`
- `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname`
- `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname`

5. The settings should now look like this:

The screenshot shows two configuration panels side-by-side.

Basic SAML Configuration

Identifier (Entity ID)	urn:sharepoint:federation
Reply URL (Assertion Consumer Service URL)	<code>https://spsites.contoso.local/_trust/</code>
Sign on URL	<code>https://spsites.contoso.local/</code>
Relay State	<i>Optional</i>
Logout Url	<i>Optional</i>

User Attributes & Claims

name	<code>user.userprincipalname</code>
Unique User Identifier	<code>user.userprincipalname</code>

6. Copy the information that you'll need later in SharePoint:

- In the **SAML Signing Certificate** section, **Download the Certificate (Base64)**. This is the public key of the signing certificate used by Microsoft Entra ID to sign the SAML token. SharePoint will need it to verify the integrity of the incoming SAML tokens.
- In the **Set up SharePoint corporate farm** section, copy the **Login URL** in a notepad and replace the trailing string `/saml2` with `/wsfed`.

Important

Make sure to replace `/saml2` with `/wsfed` to ensure that Microsoft Entra ID issues a SAML 1.1 token, as required by SharePoint.

- In the **Set up SharePoint corporate farm** section, copy the **Logout URL**

Configure SharePoint to trust Microsoft Entra ID

Create the trust in SharePoint

In this step, you create a `SPTrustedLoginProvider` to store the configuration that SharePoint needs to trust Microsoft Entra ID. For that, you need the information from Microsoft Entra ID that you copied above. Note that using Windows PowerShell may make some commands to fail. Start the SharePoint Management Shell and run the following script to create it:

```
PowerShell

# Path to the public key of the Microsoft Entra SAML signing certificate (self-signed), downloaded from the
Enterprise application in the Azure portal
$signingCert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("C:\Microsoft Entra
app\SharePoint corporate farm.cer")
# Unique realm (corresponds to the "Identifier (Entity ID)" in the Microsoft Entra enterprise application)
$realm = "urn:sharepoint:federation"
# Login URL copied from the Microsoft Entra enterprise application. Make sure to replace "saml2" with "wsfed" at
the end of the URL:
```

```

$loginUrl = "https://login.microsoftonline.com/dc38a67a-f981-4e24-ba16-4443ada44484/wsfed"

# Define the claim types used for the authorization
$userIdentifier = New-SPClaimTypeMapping -IncomingClaimType
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name" -IncomingClaimTypeDisplayName "name" -LocalClaimType
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"
$role = New-SPClaimTypeMapping "http://schemas.microsoft.com/ws/2008/06/identity/claims/role" -
IncomingClaimTypeDisplayName "Role" -SameAsIncoming

# Let SharePoint trust the Microsoft Entra signing certificate
New-SPTtrustedRootAuthority -Name "Microsoft Entra signing certificate" -Certificate $signingCert

# Create a new SPTrustedIdentityTokenIssuer in SharePoint
$trust = New-SPTtrustedIdentityTokenIssuer -Name "MicrosoftEntraTrust" -Description "Microsoft Entra ID" -Realm
$realm -ImportTrustCertificate $signingCert -ClaimsMappings $userIdentifier, $role -SignInUrl $loginUrl -
IdentifierClaim $userIdentifier.InputClaimType

```

Configure the SharePoint web application

In this step, you configure a web application in SharePoint to trust the Microsoft Entra Enterprise application created above. There are important rules to have in mind:

- The default zone of the SharePoint web application must have Windows authentication enabled. This is required for the Search crawler.
- The SharePoint URL that will use Microsoft Entra authentication must be set with HTTPS.

1. Create or extend the web application. This article describes two possible configurations:

- If you create a new web application that uses both Windows and Microsoft Entra authentication in the Default zone:
 - a. Start the **SharePoint Management Shell** and run the following script:

```

PowerShell

# This script creates a new web application and sets Windows and Microsoft Entra authentication on the
Default zone
# URL of the SharePoint site federated with Microsoft Entra
$trustedSharePointSiteUrl = "https://spsites.contoso.local/"
$applicationPoolManagedAccount = "Contoso\spapppool1"

$winAp = New-SPAuthenticationProvider -UseWindowsIntegratedAuthentication -DisableKerberos:$true
$sptrust = Get-SPTtrustedIdentityTokenIssuer "MicrosoftEntraTrust"
$trustedAp = New-SPAuthenticationProvider -TrustedIdentityTokenIssuer $sptrust

New-SPWebApplication -Name "SharePoint - Microsoft Entra" -Port 443 -SecureSocketsLayer -URL
$trustedSharePointSiteUrl -ApplicationPool "SharePoint - Microsoft Entra" -ApplicationPoolAccount (Get-
SPManagedAccount $applicationPoolManagedAccount) -AuthenticationProvider $winAp, $trustedAp

```

b. Open the **SharePoint Central Administration** site.

c. Under **System Settings**, select **Configure Alternate Access Mappings**. The **Alternate Access Mapping Collection** box opens.

d. Filter the display with the new web application and confirm that you see something like this:

Internal URL	Zone	Public URL for Zone
https://spsites.contoso.local	Default	https://spsites.contoso.local

- If you extend an existing web application to use Microsoft Entra authentication on a new zone:

a. Start the **SharePoint Management Shell** and run the following script:

```

PowerShell

# This script extends an existing web application to set Microsoft Entra authentication on a new zone
# URL of the default zone of the web application
$webAppDefaultZoneUrl = "http://spsites/"
# URL of the SharePoint site federated with ADFS
$trustedSharePointSiteUrl = "https://spsites.contoso.local/"
$sptrust = Get-SPTtrustedIdentityTokenIssuer "MicrosoftEntraTrust"

```

```
$ap = New-SPAuthenticationProvider -TrustedIdentityTokenIssuer $sptrust
$wa = Get-SPWebApplication $webAppDefaultZoneUrl

New-SPWebApplicationExtension -Name "SharePoint - Microsoft Entra" -Identity $wa -SecureSocketsLayer -
Zone Internet -Url $trustedSharePointSiteUrl -AuthenticationProvider $ap
```

- b. Open the SharePoint Central Administration site.
- c. Under **System Settings**, select **Configure Alternate Access Mappings**. The **Alternate Access Mapping Collection** box opens.
- d. Filter the display with the web application that was extended and confirm that you see something like this:

Internal URL	Zone	Public URL for Zone
http://spsites	Default	http://spsites
https://spsites.contoso.local	Internet	https://spsites.contoso.local

Once the web application is created, you can create a root site collection and add your Windows account as the primary site collection administrator.

1. Create a certificate for the SharePoint site

Since SharePoint URL uses HTTPS protocol (<https://spsites.contoso.local/>), a certificate must be set on the corresponding Internet Information Services (IIS) site. Follow those steps to generate a self-signed certificate:

Important

Self-signed certificates are suitable only for test purposes. In production environments, we strongly recommend that you use certificates issued by a certificate authority instead.

- a. Open the Windows PowerShell console.
- b. Run the following script to generate a self-signed certificate and add it to the computer's MY store:

```
PowerShell

New-SelfSignedCertificate -DnsName "spsites.contoso.local" -CertStoreLocation "cert:\LocalMachine\My"
```

2. Set the certificate in the IIS site

- a. Open the Internet Information Services Manager console.
- b. Expand the server in the tree view, expand **Sites**, select the site **SharePoint - Microsoft Entra ID**, and select **Bindings**.
- c. Select **https binding** and then select **Edit**.
- d. In the TLS/SSL certificate field, choose the certificate to use (for example, **spsites.contoso.local** created above) and select **OK**.

Note

If you have multiple Web Front End servers, you need to repeat this operation on each.

The basic configuration of the trust between SharePoint and Microsoft Entra ID is now finished. Let's see how to sign in to the SharePoint site as a Microsoft Entra user.

Sign in as a member user

Microsoft Entra ID has [two type of users](#): Guest users and Member users. Let's start with a member user, which is merely a user that is homed in your organization.

Create a member user in Microsoft Entra ID

1. Sign in to the [Microsoft Entra admin center](#) as at least a [User Administrator](#).

2. Browse to **Identity > Users > All users**.
3. Select **New user > Create new user**, at the top of the screen.
4. In the **User properties**, follow these steps:
 - a. In the **Display name** field, enter **B.Simon**.
 - b. In the **User principal name** field, enter the **username@companydomain.extension**. For example, **B.Simon@contoso.com**.
 - c. Select the **Show password** check box, and then write down the value that's displayed in the **Password** box.
 - d. Select **Review + create**.
5. Select **Create**.
6. You can share the site with this user and permit access to it.

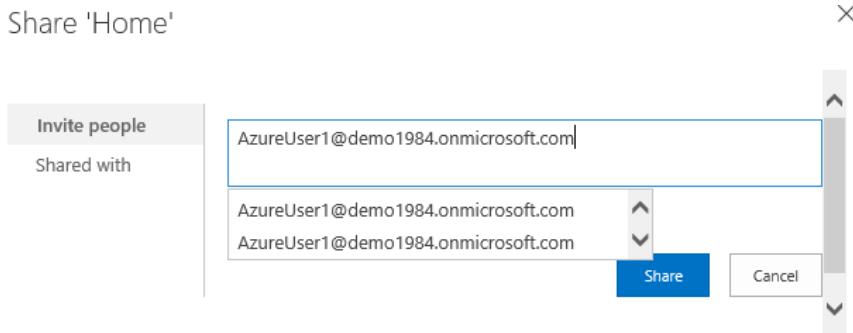
Grant permissions to the Microsoft Entra user in SharePoint

Sign in to the SharePoint root site collection as your Windows account (site collection administrator) and click **Share**.

In the dialog, you need to type the exact value of the **userprincipalname**, for example **AzureUser1@demo1984.onmicrosoft.com**, and be careful to select the **name** claim result (move your mouse on a result to see its claim type)

Important

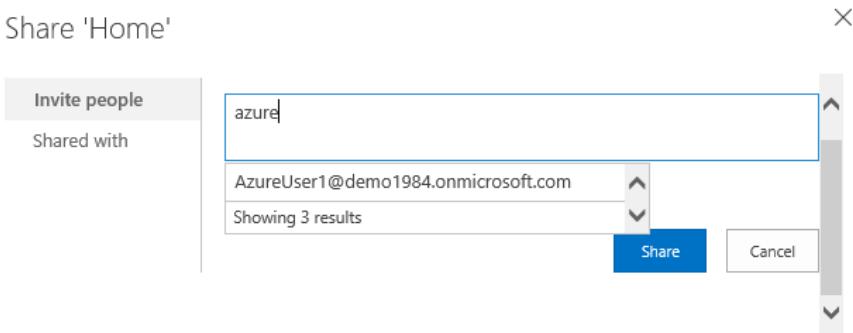
Be careful to type the exact value of the user you want to invite, and choose the appropriate claim type in the list, otherwise the sharing will not work.



This limitation is because SharePoint does not validate the input from the people picker, which can be confusing and lead to misspellings or users accidentally choosing the wrong claim type.

To fix this scenario, an open-source solution called [EntraCP](#) can be used to connect SharePoint 2019 / 2016 / 2013 with Microsoft Entra ID and resolve the input against your Microsoft Entra tenant. For more information, see [EntraCP](#).

Below is the same search with EntraCP configured: SharePoint returns actual users based on the input:



Important

EntraCP isn't a Microsoft product and isn't supported by Microsoft Support. To download, install, and configure EntraCP on the on-premises SharePoint farm, see the [EntraCP](#) website.

Microsoft Entra user **AzureUser1@demo1984.onmicrosoft.com** can now use his/her identity to sign in to the SharePoint site <https://sp/sites.contoso.local/>.

Grant permissions to a security group

Add the group claim type to the enterprise application

1. In the Overview of the Enterprise application `SharePoint corporate farm`, select 2. Set up single sign-on.

2. In the **User Attributes & Claims** section, follow these steps if there is no group claim present:

- a. Select **Add a group claim**, select **Security groups**, make sure that **Source Attribute** is set to **Group ID**
- b. Check **Customize the name of the group claim**, then check **Emit groups as role claims** and click **Save**.
- c. The **User Attributes & Claims** should look like this:

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for... ...]

Additional claims

Claim name	Value
http://schemas.microsoft.com/ws/2008/06/identity/claims/role	user.groups [SecurityGroup] ...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ...

Create a security group in Microsoft Entra ID

Let's create a security group.

1. Browse to **Identity > Groups**.

2. Select **New group**.

3. Fill in the **Group type** (Security), **Group name** (for example, `AzureGroup1`), and **Membership type**. Add the user you created above as a member and click select **Create**:

Group type * ⓘ

Security

Group name * ⓘ

AzureGroup1

Group description ⓘ

Enter a description for the group

Azure AD roles can be assigned to the group (Preview) ⓘ

Yes No

Membership type * ⓘ

Assigned

Owners

No owners selected

Members

1 member selected

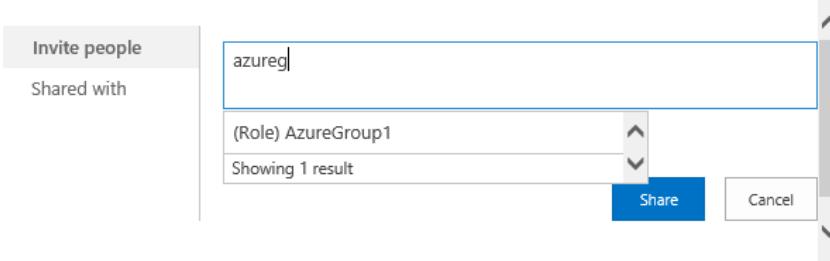
Grant permissions to the security group in SharePoint

Microsoft Entra security groups are identified with their attribute `Id`, which is a GUID (for example, `00aa00aa-bb11-cc22-dd33-44ee44ee44ee`).

Without a custom claims provider, users need to type the exact value (`Id`) of the group in the people picker, and select the corresponding claim type. This is not user-friendly nor reliable.

To avoid this, this article uses third-party claims provider [EntraCP](#) to find the group in a friendly way in SharePoint:

Share 'Home'



Manage Guest users access

There are two types of guest accounts:

- B2B guest accounts: Those users are homed in an external Microsoft Entra tenant
- MSA guest accounts: Those users are homed in a Microsoft identity provider (Hotmail, Outlook) or a social account provider (Google or similar)

By default, Microsoft Entra ID sets both the "Unique User Identifier" and the claim "name" to the attribute `user.userprincipalname`. Unfortunately, this attribute is ambiguous for guest accounts, as the table below shows:

Source attribute set in Microsoft Entra ID	Actual property used by Microsoft Entra ID for B2B guests	Actual property used by Microsoft Entra ID for MSA guests	Property that SharePoint can rely on to validate the identity
<code>user.userprincipalname</code>	mail, for example: <code>guest@PARTNERTENANT</code>	<code>userprincipalname</code> , for example: <code>guest_outlook.com#EXT#@TENANT.onmicrosoft.com</code>	ambiguous
<code>user.localuserprincipalname</code>	<code>userprincipalname</code> , for example: <code>guest_PARTNERTENANT#EXT#@TENANT.onmicrosoft.com</code>	<code>userprincipalname</code> , for example: <code>guest_outlook.com#EXT#@TENANT.onmicrosoft.com</code>	<code>userprincipalname</code>

As a conclusion, to ensure that guest accounts are all identified with the same attribute, the identifier claims of the enterprise application should be updated to use the attribute `user.localuserprincipalname` instead of `user.userprincipalname`.

Update the application to use a consistent attribute for all guest users

1. In the Overview of the Enterprise application `SharePoint corporate farm`, select **2. Set up single sign-on**.
2. On the **Set up Single Sign-On with SAML** page, select the **Edit** icon in the **User Attributes & Claims** pane.
3. In the **User Attributes & Claims** section, follow these steps:
 - a. Select **Unique User Identifier (Name ID)**, change its **Source Attribute** property to `user.localuserprincipalname`, and click **Save**.
 - b. Select `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name`, change its **Source Attribute** property to `user.localuserprincipalname`, and click **Save**.
 - c. The **User Attributes & Claims** should look like this:

Required claim	
Claim name	Value
Unique User Identifier (Name ID)	user.localuserprincipalname [namei... ...]
Additional claims	
Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.localuserprincipalname ...

Invite guest users in SharePoint

Note

This section assumes that claims provider EntraCP is used

In the section above, you updated the enterprise application to use a consistent attribute for all guest accounts.

Now, the configuration of EntraCP needs to be updated to reflect that change and use the attribute `userprincipalname` for guest accounts:

1. Open the [SharePoint Central Administration site](#).
2. Under [Security](#), select [EntraCP global configuration](#).
3. In the section [User identifier property](#): Set the [User identifier for 'Guest' users](#): to `UserPrincipalName`.
4. Click [Ok](#)

User identifier property

Set the properties that identify users in Azure Active Directory.

AzureCP automatically maps them to the identity claim type you set in the `SPTrustIdentityTokenIssuer`.

Be cautious: Changing it may make existing Azure AD user permissions invalid.

User identifier for 'Member' users: `UserPrincipalName`

User identifier for 'Guest' users: `UserPrincipalName`

You can now invite any guest user in the SharePoint sites.

Configure the federation for multiple web applications

The configuration works for a single web application, but additional configuration is needed if you intend to use the same trusted identity provider for multiple web applications. For example, assume you have a separate web application

<https://otherwebapp.contoso.local/> and you now want to enable Microsoft Entra authentication on it. To do this, configure SharePoint to pass the SAML WReply parameter, and add the URLs in the enterprise application.

Configure SharePoint to pass the SAML WReply parameter

1. On the SharePoint server, open the SharePoint 201x Management Shell and run the following commands. Use the same name for the trusted identity token issuer as you used previously.

PowerShell

```
$t = Get-SPTrustIdentityTokenIssuer "MicrosoftEntraTrust"
$t.UseWReplyParameter = $true
$t.Update()
```

Add the URLs in the enterprise application

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Cloud Application Administrator](#).

2. Browse to **Identity > Applications > Enterprise applications** > Select the previously created enterprise application, and select **Single sign-on**.

3. On the **Set up Single Sign-On with SAML** page, edit **Basic SAML Configuration**.

4. In the section **Reply URL (Assertion Consumer Service URL)**, add the URL (for example, <https://otherwebapp.contoso.local/>) of all additional web applications that need to sign in users with Microsoft Entra ID and click **Save**.

Reply URL (Assertion Consumer Service URL) * ⓘ

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

	Default
<input checked="" type="checkbox"/> https://sp/sites.contoso.local/_trust/	
<input type="checkbox"/> https://otherwebapp.contoso.local/	
<input checked="" type="checkbox"/> https://onemoreapp.contoso.local/	
<input type="checkbox"/>	

Configure the lifetime of the security token

By default, Microsoft Entra ID creates a SAML token that is valid for 1 hour, that cannot be customized in the Azure portal or using a Conditional Access policy.

However, it is possible to create a [custom token lifetime policy](#), and assign it to the enterprise application you created for SharePoint Server.

You can run the script below to achieve this:

PowerShell

```
Install-Module Microsoft.Graph
Connect-MgGraph -Scopes "Policy.ReadWrite.ApplicationConfiguration","Policy.Read.All","Application.ReadWrite.All"

$appDisplayName = "SharePoint corporate farm"
$sp = Get-MgServicePrincipal -Search DisplayName:$appDisplayName -ConsistencyLevel eventual

$oldPolicy = Get-MgServicePrincipalTokenLifetimePolicy -ServicePrincipalId $sp.Id
if ($null -ne $oldPolicy) {
    # There can be only 1 TokenLifetimePolicy associated to the service principal (or 0, as by default)
    Remove-MgServicePrincipalAppManagementPolicy -AppManagementPolicyId $oldPolicy.Id -ServicePrincipalId $sp.Id
}

# Get / create a custom token lifetime policy
$policyDisplayName = "WebPolicyScenario"
$policy = Get-MgPolicyTokenLifetimePolicy -Filter "DisplayName eq '$policyDisplayName'"
if ($null -eq $policy) {
    $params = @{
        Definition = @('{"TokenLifetimePolicy":{"Version":1,"AccessTokenLifetime":"4:00:00"}}')
        DisplayName = $policyDisplayName
        IsOrganizationDefault = $false
    }
    $policy = New-MgPolicyTokenLifetimePolicy -BodyParameter $params
}

# Assign the token lifetime policy to an app
$body = @{
    "@odata.id" = "https://graph.microsoft.com/v1.0/policies/tokenLifetimePolicies/($policy.Id)"
}
Invoke-GraphRequest -Uri ('https://graph.microsoft.com/v1.0/servicePrincipals/{0}/tokenLifetimePolicies/$ref' -f $sp.Id) -Method POST -Body $body
```

Feedback

Was this page helpful?

Yes

No

Provide product feedback ↗

Connect an on-premises network to a Microsoft Azure virtual network

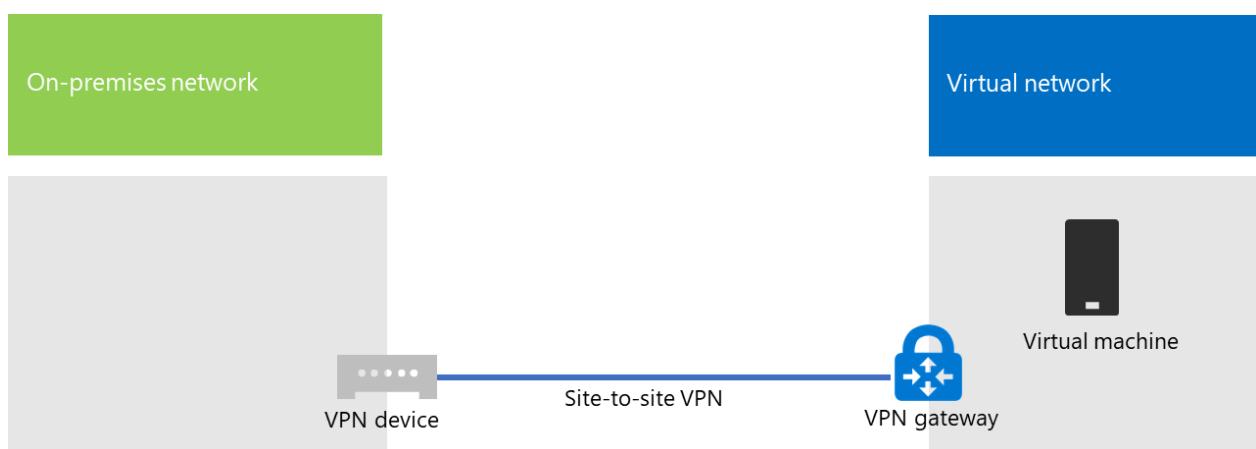
Article • 12/18/2023

A cross-premises Azure virtual network is connected to your on-premises network, extending your network to include subnets and virtual machines hosted in Azure infrastructure services. This connection lets computers on your on-premises network to directly access virtual machines in Azure and vice versa.

For example, a directory synchronization server running on an Azure virtual machine needs to query your on-premises domain controllers for changes to accounts and synchronize those changes with your Microsoft 365 subscription. This article shows you how to set up a cross-premises Azure virtual network using a site-to-site virtual private network (VPN) connection that is ready to host Azure virtual machines.

Configure a cross-premises Azure virtual network

Your virtual machines in Azure don't have to be isolated from your on-premises environment. To connect Azure virtual machines to your on-premises network resources, you must configure a cross-premises Azure virtual network. The following diagram shows the required components to deploy a cross-premises Azure virtual network with a virtual machine in Azure.



In the diagram, there are two networks connected by a site-to-site VPN connection: the on-premises network and the Azure virtual network. The site-to-site VPN connection is:

- Between two endpoints that are addressable and located on the public Internet.
- Terminated by a VPN device on the on-premises network and an Azure VPN gateway on the Azure virtual network.

The Azure virtual network hosts virtual machines. Network traffic originating from virtual machines on the Azure virtual network gets forwarded to the VPN gateway, which then forwards the traffic across the site-to-site VPN connection to the VPN device on the on-premises network. The routing infrastructure of the on-premises network then forwards the traffic to its destination.

Note

You can also use [ExpressRoute](#), which is a direct connection between your organization and Microsoft's network. Traffic over ExpressRoute does not travel over the public Internet. This article does not describe the use of ExpressRoute.

To set up the VPN connection between your Azure virtual network and your on-premises network, follow these steps:

1. **On-premises:** Define and create an on-premises network route for the address space of the Azure virtual network that points to your on-premises VPN device.
2. **Microsoft Azure:** Create an Azure virtual network with a site-to-site VPN connection.
3. **On premises:** Configure your on-premises hardware or software VPN device to terminate the VPN connection, which uses Internet Protocol security (IPsec).

After you establish the site-to-site VPN connection, you add Azure virtual machines to the subnets of the virtual network.

Plan your Azure virtual network

Prerequisites

- An Azure subscription. For information about Azure subscriptions, go to the [How To Buy Azure page](#).
- An available private IPv4 address space to assign to the virtual network and its subnets, with sufficient room for growth to accommodate the number of virtual machines needed now and in the future.
- An available VPN device in your on-premises network to terminate the site-to-site VPN connection that supports the requirements for IPsec. For more information, see [About VPN devices for site-to-site virtual network connections](#).
- Changes to your routing infrastructure so that traffic routed to the address space of the Azure virtual network gets forwarded to the VPN device that hosts the site-to-site VPN connection.

- A web proxy that gives computers that are connected to the on-premises network and the Azure virtual network access to the Internet.

Solution architecture design assumptions

The following list represents the design choices that have been made for this solution architecture.

- This solution uses a single Azure virtual network with a site-to-site VPN connection. The Azure virtual network hosts a single subnet that can contain multiple virtual machines.
- You can use the Routing and Remote Access Service (RRAS) in Windows Server 2016 or Windows Server 2012 to establish an IPsec site-to-site VPN connection between the on-premises network and the Azure virtual network. You can also use other options, such as Cisco or Juniper Networks VPN devices.
- The on-premises network might still have network services like Active Directory Domain Services (AD DS), Domain Name System (DNS), and proxy servers. Depending on your requirements, it might be beneficial to place some of these network resources in the Azure virtual network.

For an existing Azure virtual network with one or more subnets, determine whether there's remaining address space for an additional subnet to host your needed virtual machines, based on your requirements. If you don't have remaining address space for an additional subnet, create an additional virtual network that has its own site-to-site VPN connection.

Plan the routing infrastructure changes for the Azure virtual network

You must configure your on-premises routing infrastructure to forward traffic destined for the address space of the Azure virtual network to the on-premises VPN device that is hosting the site-to-site VPN connection.

The exact method of updating your routing infrastructure depends on how you manage routing information, which can be:

- Routing table updates based on manual configuration.
- Routing table updates based on routing protocols, such as Routing Information Protocol (RIP) or Open Shortest Path First (OSPF).

Consult with your routing specialist to make sure that traffic destined for the Azure virtual network is forwarded to the on-premises VPN device.

Plan for firewall rules for traffic to and from the on-premises VPN device

If your VPN device is on a perimeter network that has a firewall between the perimeter network and the Internet, you might have to configure the firewall for the following rules to allow the site-to-site VPN connection.

- Traffic to the VPN device (incoming from the Internet):
 - Destination IP address of the VPN device and IP protocol 50
 - Destination IP address of the VPN device and UDP destination port 500
 - Destination IP address of the VPN device and UDP destination port 4500
- Traffic from the VPN device (outgoing to the Internet):
 - Source IP address of the VPN device and IP protocol 50
 - Source IP address of the VPN device and UDP source port 500
 - Source IP address of the VPN device and UDP source port 4500

Plan for the private IP address space of the Azure virtual network

The private IP address space of the Azure virtual network must be able to accommodate addresses used by Azure to host the virtual network and with at least one subnet that has enough addresses for your Azure virtual machines.

To determine the number of addresses needed for the subnet, count the number of virtual machines that you need now, estimate for future growth, and then use the following table to determine the size of the subnet.

[\[+\] Expand table](#)

Number of virtual machines needed	Number of host bits needed	Size of the subnet
1-3	3	/29
4-11	4	/28
12-27	5	/27
28-59	6	/26
60-123	7	/25

Planning worksheet for configuring your Azure virtual network

Before you create an Azure virtual network to host virtual machines, you must determine the settings needed in the following tables.

For the settings of the virtual network, fill in Table V.

Table V: Cross-premises virtual network configuration

 Expand table

Item	Configuration element	Description	Value
1.	Virtual network name	A name to assign to the Azure virtual network (example DirSyncNet).	_____
2.	Virtual network location	The Azure datacenter that will contain the virtual network (such as West US).	_____
3.	VPN device IP address	The public IPv4 address of your VPN device's interface on the Internet. Work with your IT department to determine this address.	_____
4.	Virtual network address space	The address space (defined in a single private address prefix) for the virtual network. Work with your IT department to determine this address space. The address space should be in Classless Interdomain Routing (CIDR) format, also known as network prefix format. An example is 10.24.64.0/20.	_____
5.	IPsec shared key	A 32-character random, alphanumeric string that will be used to authenticate both sides of the site-to-site VPN connection. Work with your IT or security department to determine this key value and then store it in a secure location. Alternately, see Create a random string for an IPsec preshared key .	_____

Fill in Table S for the subnets of this solution.

- For the first subnet, determine a 28-bit address space (with a /28 prefix length) for the Azure gateway subnet. See [Calculating the gateway subnet address space for Azure virtual networks](#) for information about how to determine this address space.
- For the second subnet, specify a friendly name, a single IP address space based on the virtual network address space, and a descriptive purpose.

Work with your IT department to determine these address spaces from the virtual network address space. Both address spaces should be in CIDR format.

Table S: Subnets in the virtual network

[Expand table](#)

Item	Subnet name	Subnet address space	Purpose
1.	GatewaySubnet	_____	The subnet used by the Azure gateway.
2.	_____	_____	_____

For the on-premises DNS servers that you want the virtual machines in the virtual network to use, fill in Table D. Give each DNS server a friendly name and a single IP address. This friendly name does not need to match the host name or computer name of the DNS server. Note that two blank entries are listed, but you can add more. Work with your IT department to determine this list.

Table D: On-premises DNS servers

[Expand table](#)

Item	DNS server friendly name	DNS server IP address
1.	_____	_____
2.	_____	_____

To route packets from the Azure virtual network to your organization network across the site-to-site VPN connection, you must configure the virtual network with a local network. This local network has a list of the address spaces (in CIDR format) for all of the locations on your organization's on-premises network that the virtual machines in the virtual network must reach. This can be all of the locations on the on-premises network or a subset. The list of address spaces that define your local network must be unique and must not overlap with the address spaces used for this virtual network or your other cross-premises virtual networks.

For the set of local network address spaces, fill in Table L. Note that three blank entries are listed but you will typically need more. Work with your IT department to determine this list.

Table L: Address prefixes for the local network

Item	Local network address space
1.	_____
2.	_____
3.	_____

Deployment roadmap

Creating the cross-premises virtual network and adding virtual machines in Azure consists of three phases:

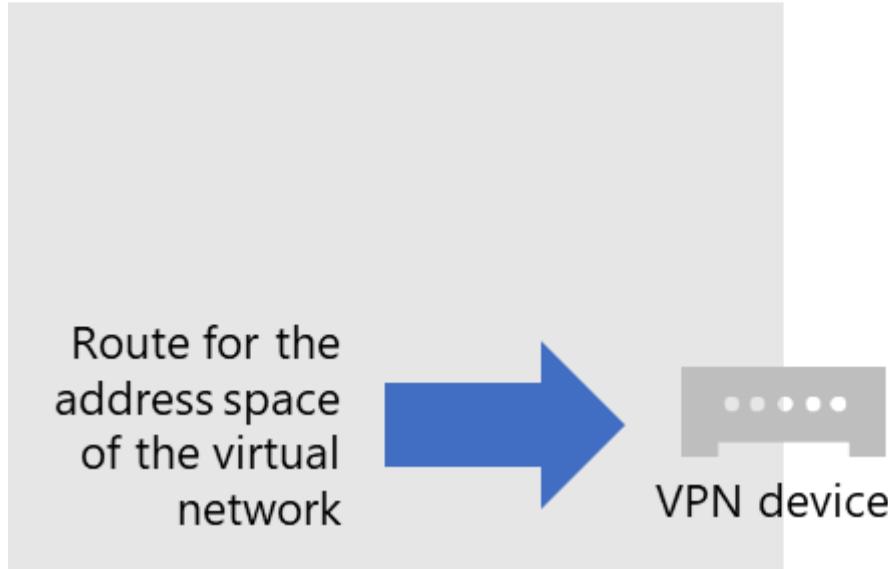
- Phase 1: Prepare your on-premises network.
- Phase 2: Create the cross-premises virtual network in Azure.
- Phase 3 (Optional): Add virtual machines.

Phase 1: Prepare your on-premises network

You must configure your on-premises network with a route that points to and ultimately delivers traffic destined for the address space of the virtual network to the router on the edge of the on-premises network. Consult with your network administrator to determine how to add the route to the routing infrastructure of your on-premises network.

Here is your resulting configuration.

On-premises network



Phase 2: Create the cross-premises virtual network in Azure

First, open an Azure PowerShell prompt. If you have not installed Azure PowerShell, see [Get started with Azure PowerShell](#).

Next, login to your Azure account with this command.

```
PowerShell
```

```
Connect-AzAccount
```

Get your subscription name using the following command.

```
PowerShell
```

```
Get-AzSubscription | Sort SubscriptionName | Select SubscriptionName
```

Set your Azure subscription with these commands. Replace everything within the quotes, including the < and > characters, with the correct subscription name.

```
PowerShell
```

```
$subscrName=<subscription name>
Select-AzSubscription -SubscriptionName $subscrName
```

Next, create a new resource group for your virtual network. To determine a unique resource group name, use this command to list your existing resource groups.

PowerShell

```
Get-AzResourceGroup | Sort ResourceGroupName | Select ResourceGroupName
```

Create your new resource group with these commands.

PowerShell

```
$rgName=<resource group name>
$locName=<Table V - Item 2 - Value column>
New-AzResourceGroup -Name $rgName -Location $locName
```

Next, you create the Azure virtual network.

PowerShell

```
# Fill in the variables from previous values and from Tables V, S, and D
$rgName=<name of your new resource group>
$locName=<Azure location of your new resource group>
$vnetName=<Table V - Item 1 - Value column>
$vnetAddrPrefix=<Table V - Item 4 - Value column>
$gwSubnetPrefix=<Table S - Item 1 - Subnet address space column>
$subnetName=<Table S - Item 2 - Subnet name column>
$subnetPrefix=<Table S - Item 2 - Subnet address space column>
$dnsServers=@( "<Table D - Item 1 - DNS server IP address column>, "<Table
D - Item 2 - DNS server IP address column>" )
$locShortName=(Get-AzResourceGroup -Name $rgName).Location

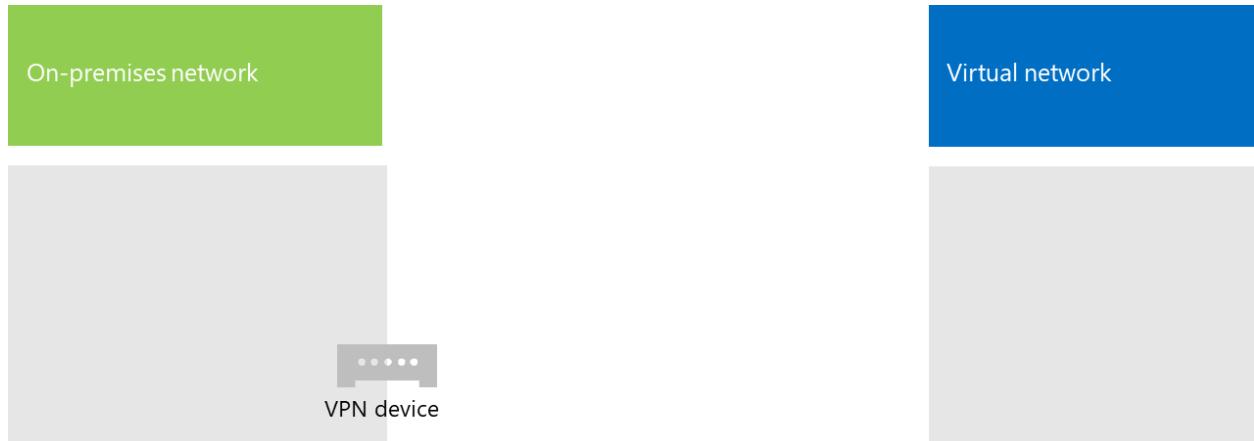
# Create the Azure virtual network and a network security group that allows
incoming remote desktop connections to the subnet that is hosting virtual
machines
$gatewaySubnet=New-AzVirtualNetworkSubnetConfig -Name "GatewaySubnet" -
AddressPrefix $gwSubnetPrefix
$vmSubnet=New-AzVirtualNetworkSubnetConfig -Name $subnetName -AddressPrefix
$subnetPrefix
New-AzVirtualNetwork -Name $vnetName -ResourceGroupName $rgName -Location
$locName -AddressPrefix $vnetAddrPrefix -Subnet $gatewaySubnet,$vmSubnet -
DNSServer $dnsServers
$rule1=New-AzNetworkSecurityRuleConfig -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-AzNetworkSecurityGroup -Name $subnetName -ResourceGroupName $rgName -
```

```

Location $locShortName -SecurityRules $rule1
$vnet=Get-AzVirtualNetwork -ResourceGroupName $rgName -Name $vnetName
$nsg=Get-AzNetworkSecurityGroup -Name $SubnetName -ResourceGroupName $rgName
Set-AzVirtualNetworkSubnetConfig -VirtualNetwork $vnet -Name $SubnetName -
AddressPrefix $SubnetPrefix -NetworkSecurityGroup $nsg
$vnet | Set-AzVirtualNetwork

```

Here is your resulting configuration.



Next, use these commands to create the gateways for the site-to-site VPN connection.

PowerShell

```

# Fill in the variables from previous values and from Tables V and L
$vnetName=<Table V - Item 1 - Value column>
$localGatewayIP=<Table V - Item 3 - Value column>
$localNetworkPrefix=@( <comma-separated, double-quote enclosed list of the
local network address prefixes from Table L, example: "10.1.0.0/24",
"10.2.0.0/24"> )
$vnetConnectionKey=<Table V - Item 5 - Value column>
$vnet=Get-AzVirtualNetwork -Name $vnetName -ResourceGroupName $rgName
# Attach a virtual network gateway to a public IP address and the gateway
subnet
$publicGatewayVipName="PublicIPAddress"
$vnetGatewayIpConfigName="PublicIPConfig"
New-AzPublicIpAddress -Name $vnetGatewayIpConfigName -ResourceGroupName
$rgName -Location $locName -AllocationMethod Dynamic
$publicGatewayVip=Get-AzPublicIpAddress -Name $vnetGatewayIpConfigName -
ResourceGroupName $rgName
$vnetGatewayIpConfig>New-AzVirtualNetworkGatewayIpConfig -Name
$vnetGatewayIpConfigName -PublicIpAddressId $publicGatewayVip.Id -SubnetId
$vnet.Subnets[0].Id
# Create the Azure gateway
$vnetGatewayName="AzureGateway"
$vnetGateway>New-AzVirtualNetworkGateway -Name $vnetGatewayName -
ResourceGroupName $rgName -Location $locName -GatewayType Vpn -VpnType
RouteBased -IpConfigurations $vnetGatewayIpConfig
# Create the gateway for the local network
$localGatewayName="LocalNetGateway"
$localGateway>New-AzLocalNetworkGateway -Name $localGatewayName -

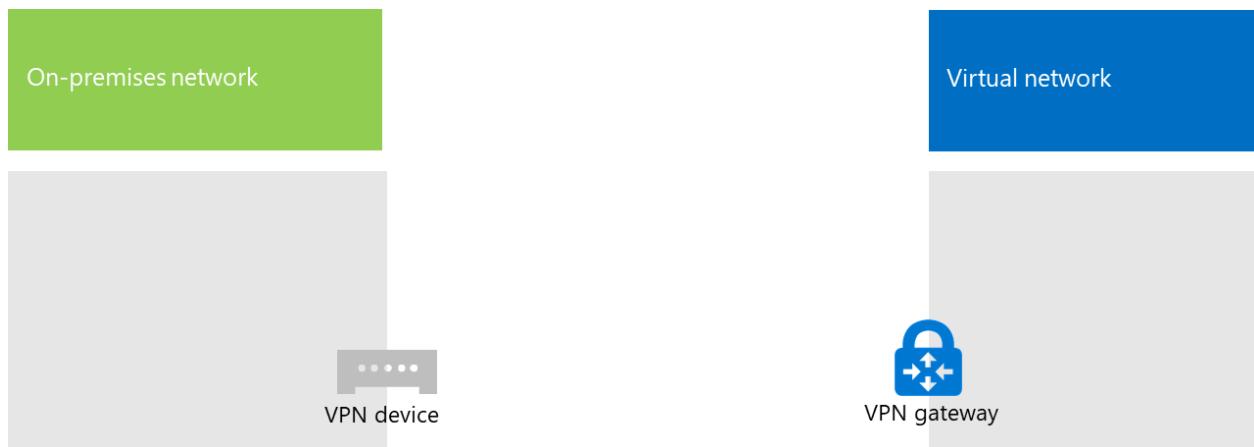
```

```

ResourceGroupName $rgName -Location $locName -GatewayIpAddress
$localGatewayIP -AddressPrefix $localNetworkPrefix
# Create the Azure virtual network VPN connection
$vnetConnectionName="S2SConnection"
$vnetConnection=New-AzVirtualNetworkGatewayConnection -Name
$vnetConnectionName -ResourceGroupName $rgName -Location $locName -
ConnectionType IPsec -SharedKey $vnetConnectionKey -VirtualNetworkGateway1
$vnetGateway -LocalNetworkGateway2 $localGateway

```

Here is your resulting configuration.

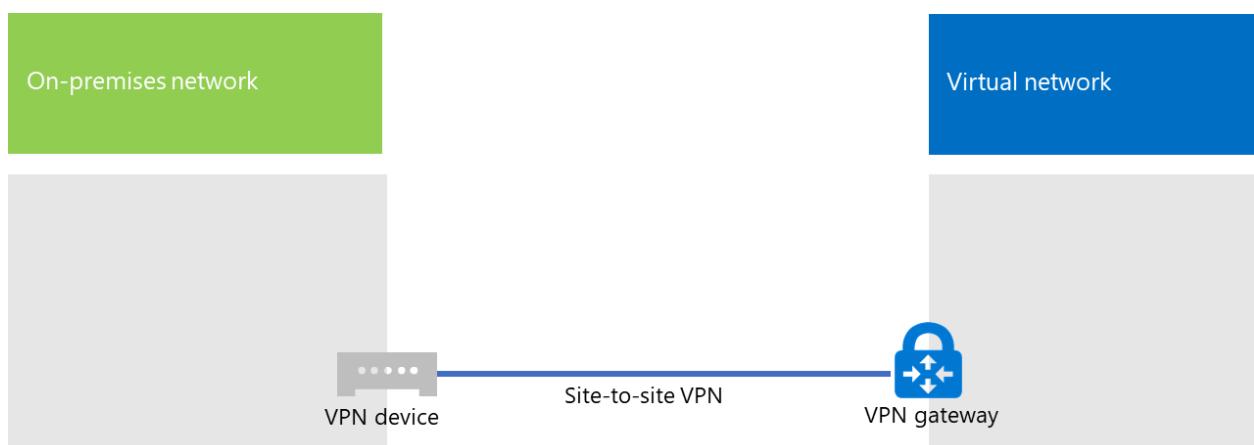


Next, configure your on-premises VPN device to connect to the Azure VPN gateway. For more information, see [About VPN Devices for site-to-site Azure Virtual Network connections](#).

To configure your VPN device, you will need the following:

- The public IPv4 address of the Azure VPN gateway for your virtual network. Use the `Get-AzPublicIpAddress -Name $vnetGatewayIpConfigName -ResourceGroupName $rgName` command to display this address.
- The IPsec pre-shared key for the site-to-site VPN connection (Table V- Item 5 - Value column).

Here is your resulting configuration.



Phase 3 (Optional): Add virtual machines

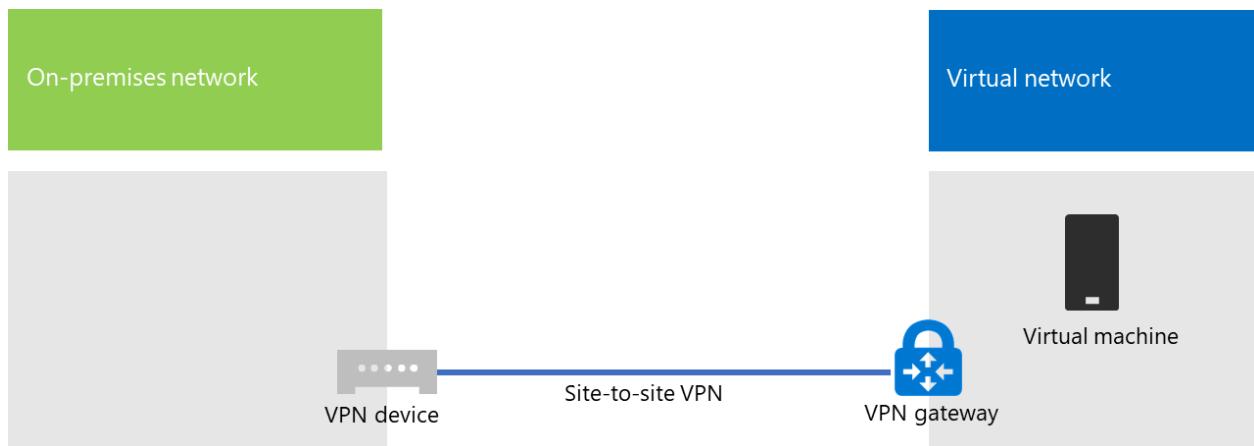
Create the virtual machines you need in Azure. For more information, see [Create a Windows virtual machine with the Azure portal](#).

Use the following settings:

- On the **Basics** tab, select the same subscription and resource group as your virtual network. You will need these later to sign in to the virtual machine. In the **Instance details** section, choose the appropriate virtual machine size. Record the administrator account user name and password in a secure location.
- On the **Networking** tab, select the name of your virtual network and the subnet for hosting virtual machines (not the GatewaySubnet). Leave all other settings at their default values.

Verify that your virtual machine is using DNS correctly by checking your internal DNS to ensure that Address (A) records were added for your new virtual machine. To access the Internet, your Azure virtual machines must be configured to use your on-premises network's proxy server. Contact your network administrator for additional configuration steps to perform on the server.

Here is your resulting configuration.



Next step

[Deploy Microsoft 365 Directory Synchronization in Microsoft Azure](#)

Feedback

Was this page helpful?

Yes

No

Provide product feedback ↗

Deploy Microsoft 365 Directory Synchronization in Microsoft Azure

Article • 03/21/2024

Microsoft Entra Connect (formerly known as the Directory Synchronization tool, Directory Sync tool, or the DirSync.exe tool) is an application that you install on a domain-joined server to synchronize your on-premises Active Directory Domain Services (AD DS) users to the Microsoft Entra tenant of your Microsoft 365 subscription.

Microsoft 365 uses Microsoft Entra ID for its directory service. Your Microsoft 365 subscription includes a Microsoft Entra tenant. This tenant can also be used for management of your organization's identities with other cloud workloads, including other SaaS applications and apps in Azure.

You can install Microsoft Entra Connect on an on-premises server, but you can also install it on a virtual machine in Azure for these reasons:

- You can provision and configure cloud-based servers faster, making the services available to your users sooner.
- Azure offers better site availability with less effort.
- You can reduce the number of on-premises servers in your organization.

This solution requires connectivity between your on-premises network and your Azure virtual network. For more information, see [Connect an on-premises network to a Microsoft Azure virtual network](#).

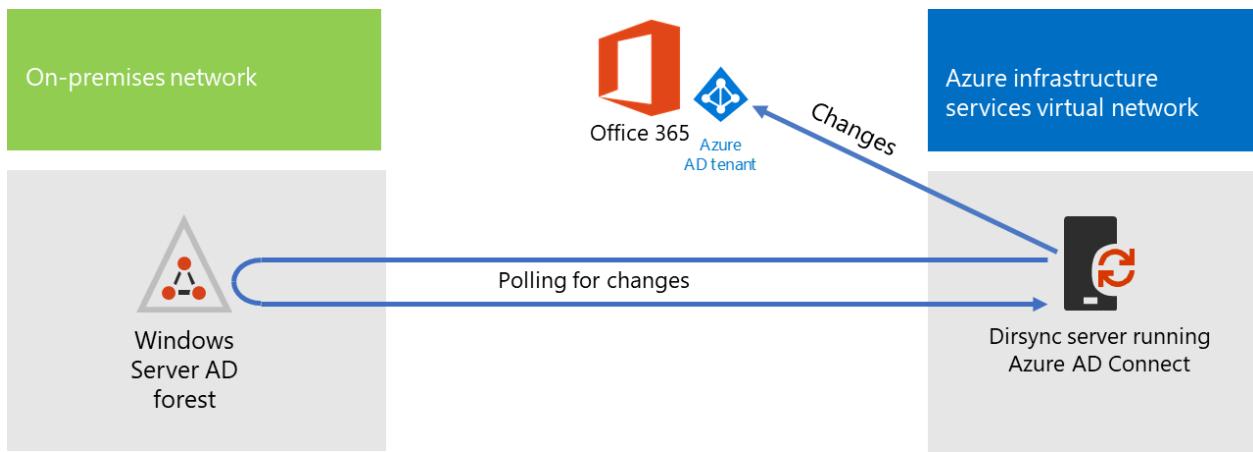
ⓘ Note

This article describes synchronization of a single domain in a single forest.

Microsoft Entra Connect synchronizes all AD DS domains in your Active Directory forest with Microsoft 365. If you have multiple Active Directory forests to synchronize with Microsoft 365, see [Multi-forest Directory Sync with Single Sign-On Scenario](#).

Overview of deploying Microsoft 365 directory synchronization in Azure

The following diagram shows Microsoft Entra Connect running on a virtual machine in Azure (the directory sync server) that synchronizes an on-premises AD DS forest to a Microsoft 365 subscription.



In the diagram, there are two networks connected by a site-to-site VPN or ExpressRoute connection. There's an on-premises network where AD DS domain controllers are located, and there's an Azure virtual network with a directory sync server, which is a virtual machine running [Microsoft Entra Connect](#). There are two main traffic flows originating from the directory sync server:

- Microsoft Entra Connect queries a domain controller on the on-premises network for changes to accounts and passwords.
- Microsoft Entra Connect sends the changes to accounts and passwords to the Microsoft Entra instance of your Microsoft 365 subscription. Because the directory sync server is in an extended portion of your on-premises network, these changes are sent through the on-premises network's proxy server.

! Note

This solution describes synchronization of a single Active Directory domain, in a single Active Directory forest. Microsoft Entra Connect synchronizes all Active Directory domains in your Active Directory forest with Microsoft 365. If you have multiple Active Directory forests to synchronize with Microsoft 365, see [Multi-forest Directory Sync with Single Sign-On Scenario](#).

There are two major steps when you deploy this solution:

1. Create an Azure virtual network and establish a site-to-site VPN connection to your on-premises network. For more information, see [Connect an on-premises network to a Microsoft Azure virtual network](#).
2. Install [Microsoft Entra Connect](#) on a domain-joined virtual machine in Azure, and then synchronize the on-premises AD DS to Microsoft 365. This involves:
 - Creating an Azure Virtual Machine to run Microsoft Entra Connect.
 - Installing and configuring [Microsoft Entra Connect](#).

Configuring Microsoft Entra Connect requires the credentials (user name and password) of a Microsoft Entra administrator account and an AD DS enterprise administrator account. Microsoft Entra Connect runs immediately and on an ongoing basis to synchronize the on-premises AD DS forest to Microsoft 365.

Before you deploy this solution in production, you can use the instructions in [The simulated enterprise base configuration](#) to set up this configuration as a proof of concept, for demonstrations, or for experimentation.

Important

When Microsoft Entra Connect configuration completes, it does not save the AD DS enterprise administrator account credentials.

Note

This solution describes synchronizing a single AD DS forest to Microsoft 365. The topology discussed in this article represents only one way to implement this solution. Your organization's topology might differ based on your unique network requirements and security considerations.

Plan for hosting a directory sync server for Microsoft 365 in Azure

Prerequisites

Before you begin, review the following prerequisites for this solution:

- Review the related planning content in [Plan your Azure virtual network](#).
- Ensure that you meet all [Prerequisites](#) for configuring the Azure virtual network.
- Have a Microsoft 365 subscription that includes the Active Directory integration feature. For information about Microsoft 365 subscriptions, go to the [Microsoft 365 subscription page](#).
- Provision one Azure Virtual Machine that runs Microsoft Entra Connect to synchronize your on-premises AD DS forest with Microsoft 365.

You must have the credentials (names and passwords) for an AD DS enterprise administrator account and a Microsoft Entra Administrator account.

Solution architecture design assumptions

The following list describes the design choices made for this solution.

- This solution uses a single Azure virtual network with a site-to-site VPN connection. The Azure virtual network hosts a single subnet that has one server, the directory sync server that is running Microsoft Entra Connect.
- On the on-premises network, a domain controller and DNS servers exist.
- Microsoft Entra Connect performs password hash synchronization instead of single sign-on. You don't have to deploy an Active Directory Federation Services (AD FS) infrastructure. To learn more about password hash synchronization and single sign-on options, see [Choosing the right authentication method for your Microsoft Entra hybrid identity solution](#).

There are other design choices that you might consider when you deploy this solution in your environment. These include the following:

- If there are existing DNS servers in an existing Azure virtual network, determine whether you want your directory sync server to use them for name resolution instead of DNS servers on the on-premises network.
- If there are domain controllers in an existing Azure virtual network, determine whether configuring Active Directory Sites and Services might be a better option for you. The directory sync server can query the domain controllers in the Azure virtual network for changes in accounts and passwords instead of domain controllers on the on-premises network.

Deployment roadmap

Deploying Microsoft Entra Connect on a virtual machine in Azure consists of three phases:

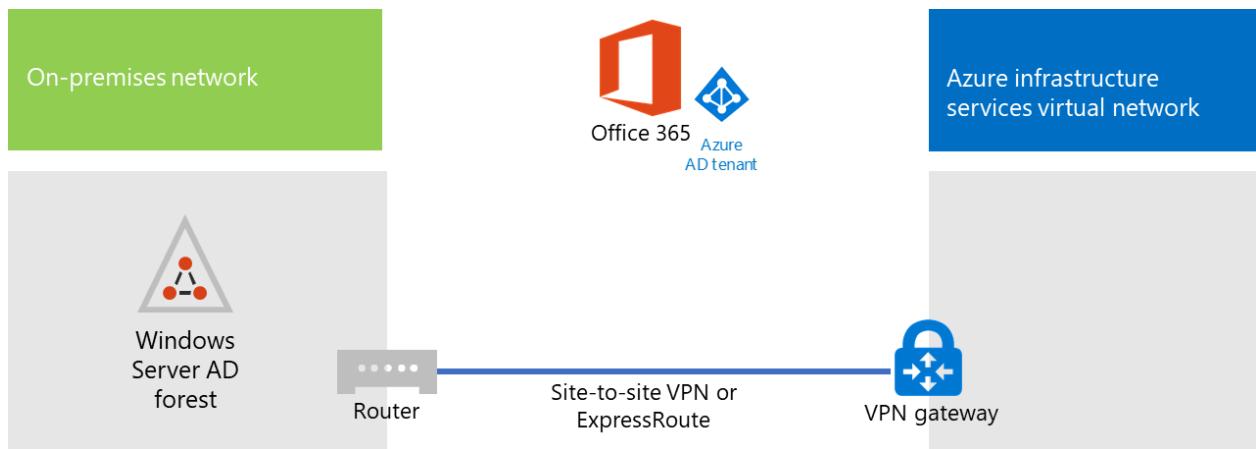
- Phase 1: Create and configure the Azure virtual network
- Phase 2: Create and configure the Azure virtual machine
- Phase 3: Install and configure Microsoft Entra Connect

After deployment, you must also assign locations and licenses for the new user accounts in Microsoft 365.

Phase 1: Create and configure the Azure virtual network

To create and configure the Azure virtual network, complete [Phase 1: Prepare your on-premises network](#) and [Phase 2: Create the cross-premises virtual network in Azure](#) in the deployment roadmap of [Connect an on-premises network to a Microsoft Azure virtual network](#).

This is your resulting configuration.



This figure shows an on-premises network connected to an Azure virtual network through a site-to-site VPN or ExpressRoute connection.

Phase 2: Create and configure the Azure virtual machine

Create the virtual machine in Azure using the instructions [Create your first Windows virtual machine in the Azure portal](#). Use the following settings:

1. On the **Basics** pane, select the same subscription, location, and resource group as your virtual network. Record the user name and password in a secure location. You'll need these later to connect to the virtual machine.
2. On the **Choose a size** pane, choose the **A2 Standard** size.
3. On the **Settings** pane, in the **Storage** section, select the **Standard** storage type. In the **Network** section, select the name of your virtual network and the subnet for hosting the directory sync server (not the GatewaySubnet). Leave all other settings at their default values.

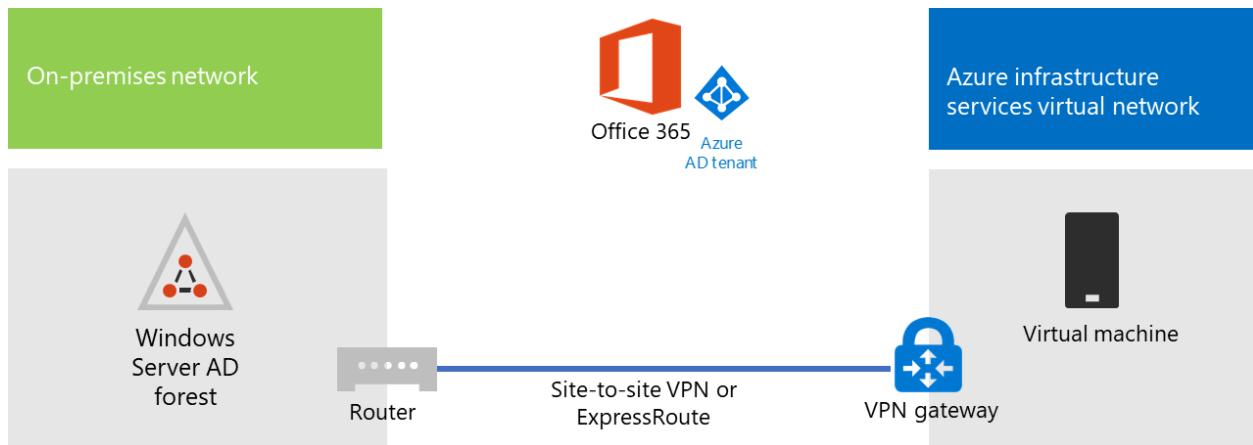
Verify that your directory sync server is using DNS correctly by checking your internal DNS to make sure that an Address (A) record was added for the virtual machine with its

IP address.

Use the instructions in [Connect to the virtual machine and sign on](#) to connect to the directory sync server with a Remote Desktop Connection. After signing in, join the virtual machine to the on-premises AD DS domain.

For Microsoft Entra Connect to gain access to Internet resources, you must configure the directory sync server to use the on-premises network's proxy server. You should contact your network administrator for any additional configuration steps to perform.

This is your resulting configuration.



This figure shows the directory sync server virtual machine in the cross-premises Azure virtual network.

Phase 3: Install and configure Microsoft Entra Connect

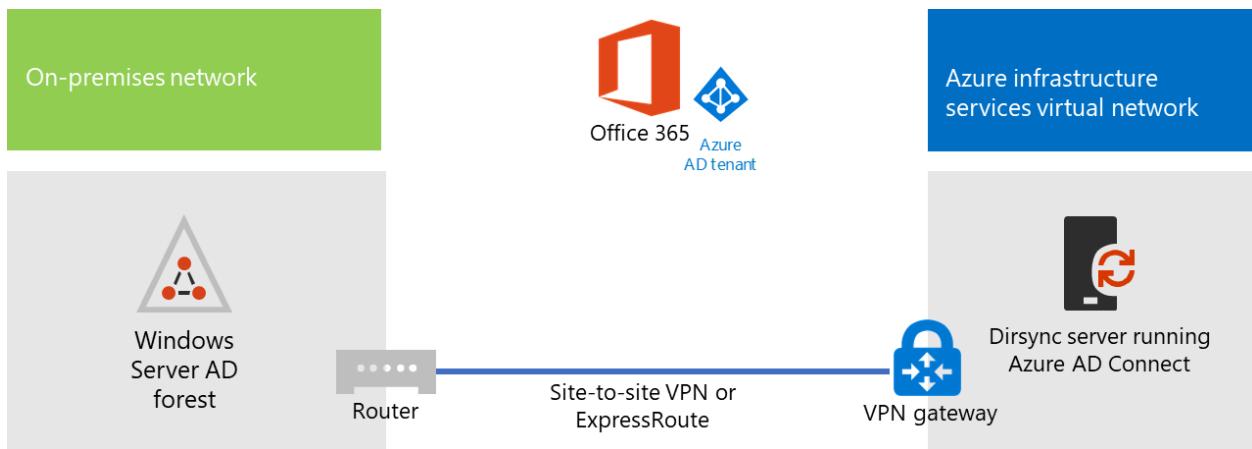
Complete the following procedure:

1. Connect to the directory sync server using a Remote Desktop Connection with an AD DS domain account that has local administrator privileges. See [Connect to the virtual machine and sign on](#).
2. From the directory sync server, open the [Set up directory synchronization for Microsoft 365](#) article and follow the directions for directory synchronization with password hash synchronization.

⊗ Caution

Setup creates the **AAD_xxxxxxxxxxxxxx** account in the Local Users organizational unit (OU). Do not move or remove this account or synchronization will fail.

This is your resulting configuration.



This figure shows the directory sync server with Microsoft Entra Connect in the cross-premises Azure virtual network.

Assign locations and licenses to users in Microsoft 365

Microsoft Entra Connect adds accounts to your Microsoft 365 subscription from the on-premises AD DS, but in order for users to sign in to Microsoft 365 and use its services, the accounts must be configured with a location and licenses. Use these steps to add the location and activate licenses for the appropriate user accounts:

1. Sign in to the [Microsoft 365 admin center](#), and then click **Admin**.
2. In the left navigation, click **Users > Active users**.
3. In the list of user accounts, select the check box next to the user you want to activate.
4. On the page for the user, click **Edit for Product licenses**.
5. On the **Product licenses** page, select a location for the user for **Location**, and then enable the appropriate licenses for the user.
6. When complete, click **Save**, and then click **Close** twice.
7. Go back to step 3 for additional users.

See also

[Microsoft 365 solution and architecture center](#)

[Connect an on-premises network to a Microsoft Azure virtual network](#)

[Download Microsoft Entra Connect](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Manage Microsoft 365 user accounts

Article • 12/27/2023

You can manage Microsoft 365 user accounts in several different ways, depending on your configuration. You can manage user accounts in the [Microsoft 365 admin center](#), [PowerShell](#), in Active Directory Domain Services (AD DS), or in the Microsoft Entra admin center.

As soon as you purchase Microsoft 365, the [Microsoft 365 admin center](#) and PowerShell can be used to manage accounts. When managing cloud identities, every person in your organization has a separate user account name and password. If you want to integrate with your on-premises infrastructure and have user accounts synchronized with Microsoft 365, you can use Microsoft Entra Connect to provide synchronization of identities and passwords for single sign-on (SSO) functionality.

Plan for where and how you will manage your user accounts

Where and how you can manage your user accounts depends on the identity model you want to use for your Microsoft 365. The two overall models are cloud-only and hybrid.

Cloud-only

You create and manage users in the [Microsoft 365 admin center](#). You can also use PowerShell or the Microsoft Entra admin center.

Hybrid

User accounts are synchronized with Microsoft 365 from AD DS, so you must use on-premises AD DS tools to manage user accounts.

Managing Accounts

When deciding which way your organization will create and manage accounts, consider the following requirements:

- The directory synchronization software needs to be installed on servers within your on-premises environment to connect the identities between Microsoft 365 and your AD DS.

- Any directory synchronization option, including SSO options, requires that your AD DS attributes meet standards. The specifics of what attributes are used in your directory and what cleanup (if any) is needed are described in [Prepare for directory synchronization to Microsoft 365](#).
- Plan how you are going to create Microsoft 365 accounts.

The following table lists the different account management tools.

[\[+\] Expand table](#)

Tool	Notes
Microsoft 365 admin center	<p>Add users individually or in bulk</p> <p>Provides a simple web interface to add and change user accounts.</p> <p>Can't be used to change users if directory synchronization is enabled (location and license assignment can be set).</p> <p>Can't be used with SSO options.</p>
Windows PowerShell	<p>Manage Microsoft 365 with Windows PowerShell</p> <p>Allows you to add users in bulk users by using a Windows PowerShell script.</p> <p>Can be used to assign location and licenses to accounts, regardless of how the accounts are created.</p>
Bulk import	<p>Add several users at the same time</p> <p>Allows you to import a CSV file to add a group of users to Microsoft 365.</p> <p>Can't be used with SSO options.</p>
Microsoft Entra ID	<p>You get a free edition of Microsoft Entra ID with your Microsoft 365 subscription. You can perform functions like self-service password reset for cloud users, and customization of the Sign-in and Access Panel pages by using the free edition. To get enhanced functionality, you can upgrade to the basic edition, Microsoft Entra ID P1, or Microsoft Entra ID P2. See Microsoft Entra editions for the list of supported features.</p>
Directory synchronization	<p>Integrating your on-premises identities with Microsoft Entra ID</p> <p>For directory synchronization with or without password synchronization, use Microsoft Entra Connect with express settings.</p> <p>For multiple forests and SSO options, use Custom Installation of Microsoft Entra Connect.</p> <p>Provides the infrastructure that's necessary to enable SSO.</p> <p>Required for many hybrid scenarios such as staged migration and hybrid Exchange</p> <p>Synchronizes security and mail-enabled groups from your AD DS.</p>

- Regardless of how you intend to add the user accounts to Microsoft 365, you need to manage several account features, such as assigning licenses, specifying location,

and so on. These features can be managed long-term from the [Microsoft 365 admin center](#) or you can also [create user accounts with PowerShell](#).

If you choose to add and manage all your users through the admin center, you will specify the location and assign licenses at the same time as creating the Microsoft 365 account. As a result, not much planning is required.

Important

Creating accounts in Microsoft 365 without assigning a license (to SharePoint Online, for example) means that the account owner can view the Microsoft 365 center but can't access any of the services within your company's subscription. After you assign a location and the license, the account is replicated to the service or services that you assigned. The user can sign in to their account and use the services that you assigned to them.

See also

[Microsoft 365 admin center Manage user accounts and licenses with Microsoft 365 PowerShell](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Add several users at the same time to Microsoft 365 - Admin Help

Article • 10/30/2023

Each person on your team needs a user account before they can sign in and access Microsoft 365 services, such as email and the Microsoft 365 apps. If you have a lot of people, you can add their accounts all at once from an Excel spreadsheet or other file saved in CSV format. [Not sure what CSV format is?](#)

Add multiple users in the Microsoft 365 admin center

1. Sign in to Microsoft 365 with your work or school account.
2. In the admin center, choose **Users > Active users**.
3. Select **Add multiple users**.
4. On the **Import multiple users** panel, you can optionally download a sample CSV file with or without sample data filled in.

Your spreadsheet needs to include the **exact same column headings** as the sample one (User Name, First Name, and so on). If you use the template, open it in a text editing tool, like Notepad, and consider leaving all the data in row 1 alone, and only entering data in rows 2 and below.

Your spreadsheet also needs to include values for the user name (like bob@contoso.com) and a display name (like Bob Kelly) for each user.

Console
User Name,First Name,Last Name,Display Name,Job Title,Department,Office Number,Office Phone,Mobile Phone,Fax,Alternate email address,Address,City,State or Province,ZIP or Postal Code,Country or Region chris@contoso.com,Chris,Green,Chris Green,IT Manager,Information Technology,123451,123-555-1211,123-555-6641,123-555-6700,chris@contoso.com,1 Microsoft way,Redmond,Wa,98052,United States ben@contoso.com,Ben,Andrews,Ben Andrews,IT Manager,Information Technology,123452,123-555-1212,123-555-6642,123-555-6700,chris@contoso.com,1 Microsoft way,Redmond,Wa,98052,United States david@contoso.com,David,Longmuir,David Longmuir,IT Manager,Information Technology,123453,123-555-1213,123-555-6643,123-555-6700,chris@contoso.com,1 Microsoft way,Redmond,Wa,98052,United States

cynthia@contoso.com,Cynthia,Carey,Cynthia Carey,IT Manager,Information Technology,123454,123-555-1214,123-555-6644,123-555-6700,chris@contoso.com,1 Microsoft way,Redmond,Wa,98052,United States melissa@contoso.com,Melissa,MacBeth,Melissa MacBeth,IT Manager,Information Technology,123455,123-555-1215,123-555-6645,123-555-6700,chris@contoso.com,1 Microsoft way,Redmond,Wa,98052,United States

5. Enter a file path into the box, or choose **Browse** to browse to the CSV file location, then choose **Verify**.

If there are problems with the file, the problem is displayed in the panel. You can also download a log file.

6. On the **Set user options** dialog you can set the sign-in status and choose the product license that will be assigned to all users.
7. On the **View your result** dialog you can choose to send the results to either yourself or other users (passwords will be in plain text) and you can see how many users were created, and if you need to purchase more licenses to assign to some of the new users.

Next steps

- Now that these people have accounts, they need to [Download and install or reinstall Microsoft 365 or Office 2016 on a PC or Mac](#). Each person on your team can install Microsoft 365 on up to 5 PCs or Macs.
- Each person can also [Set up Office apps and email on a mobile device](#) on up to 5 tablets and 5 phones, such as iPhones, iPads, and Android phones and tablets. This way they can edit Office files from anywhere.

See [Set up Microsoft 365 for business](#) for an end-to-end list of the setup steps.

More information about how to add users to Microsoft 365

Not sure what CSV format is?

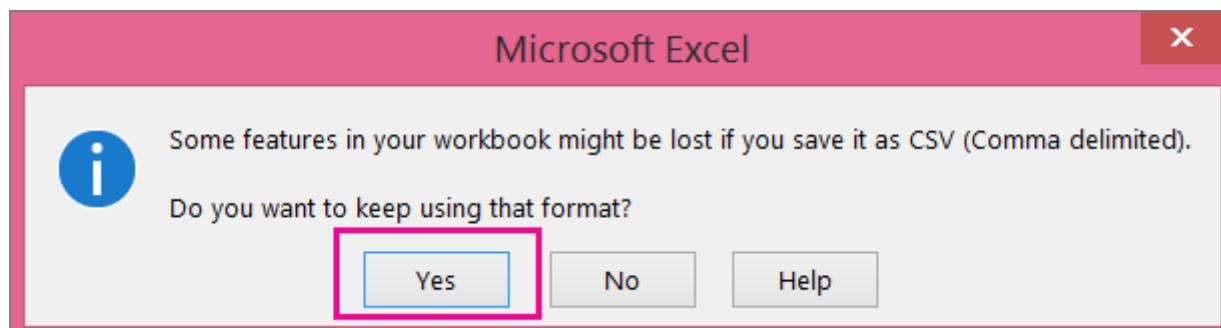
A CSV file is a file with comma separated values. You can create or edit a file like this with any text editor or spreadsheet program, such as Excel.

You can download [this sample spreadsheet](#) as a starting point. Remember that Microsoft 365 requires column headings in the first row so don't replace them with something else.

Save the file with a new name, and specify CSV format.



When you save the file, you'll probably get a prompt that some features in your workbook will be lost if you save the file in CSV format. This is okay. Click Yes to continue.



Tips for formatting your spreadsheet

- **Do I need the same column headings as in the sample spreadsheet?** Yes. The sample spreadsheet contains column headings in the first row. These headings are required. For each user you want to add to Microsoft 365, create a row under the heading. If you add, change, or delete any of the column headings, Microsoft 365 might not be able to create users from the information in the file.
- **What if I don't have all the information required for each user?** The user name and display name are required, and you cannot add a new user without this information. If you don't have some of the other information, such as the fax, you can use a space plus a comma to indicate that the field should remain blank.
- **How small or large can the spreadsheet be?** The spreadsheet must have at least two rows. One is for the column headings (the user data column label) and one for the user. You cannot have more than 250 rows. If you need to import more than 249 users, you can create more than one spreadsheet.
- **What languages can I use?** When you create your spreadsheet, you can enter user data column labels in any language or characters, but you must not change the order of the labels, as shown in the sample. You can then make entries into the

fields, using any language or characters, and save your file in a Unicode or UTF-8 format.

- **What if I'm adding users from different countries or regions?** Create a separate spreadsheet for each area. You'll need to step through the Bulk add users wizard which each spreadsheet, giving a single location of all users included in the file that you're working with.
- **Is there a limit to the number of characters I can use?** The following table shows the user data column labels and the maximum character length for each in the sample spreadsheet.

User data column label	Maximum character length
User Name (Required)	79 including the at sign (@), in the format name@domain.<extension>. The user's alias cannot exceed 50 characters, and the domain name cannot exceed 48 characters.
First Name	64
Last Name	64
Display Name (required)	256
Job Title	64
Department	64
Office Number	128
Office Phone	64
Mobile Phone	64
Fax	64
Address	1023
City	128
State or Province	128
ZIP or Postal Code	40
Country or Region	128

Still having problems when adding users to Microsoft 365?

- **Double-check that the spreadsheet is formatted correctly.** Check the column headings to make sure they match the headings in the sample file. Make sure you're following the rules for character lengths and that each field is separated by a comma.
- **If you don't see the new users in Microsoft 365 right away, wait a few minutes.** It can take a little while for changes to go across all the services in Microsoft 365.

Related articles

[Add users individually or in bulk to Microsoft 365](#)

Assign Microsoft 365 licenses to user accounts

Article • 04/15/2024

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

For the cloud-only identity model, you can assign Microsoft 365 licenses to user accounts as they're created, depending on how you create them.

For the hybrid identity model, when Active Directory Domain Services (AD DS) user accounts are synchronized for the first time, they aren't automatically assigned a location or a Microsoft 365 license. **You must configure each user account with a user location prior to or along with assigning a license.**

In either case, you must assign a license to user accounts so your users can access Microsoft 365 services, such as email and Microsoft Teams.

You can assign licenses to user accounts either individually or automatically through group membership.

To assign Microsoft 365 licenses to individual user accounts, you can use:

- [The Microsoft 365 admin center](#)
- [PowerShell](#)
- The Microsoft Entra admin center

Group-based licensing

You can configure security groups in Microsoft Entra ID 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 unassigned from the user account.

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.

For more information, see [group-based licensing in Microsoft Entra ID](#).

Next steps

With the appropriate set of user accounts that have been assigned licenses, you're now ready to:

- Implement security
- Deploy client software, such as Microsoft 365 Apps
- Set up device management
- Configure services and applications

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Manage Microsoft 365 user account passwords

Article • 01/24/2024

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

You can manage Microsoft 365 user account passwords in several different ways, depending on your identity configuration. You can manage user accounts in the [Microsoft 365 admin center](#), in Active Directory Domain Services (AD DS), or in the Microsoft Entra admin center.

Plan for where and how you will manage your user account passwords

Where and how you can manage your user accounts depends on the identity model you want to use for your Microsoft 365. The two models are cloud-only and hybrid.

Cloud-only

You manage user account passwords in:

- [The Microsoft 365 admin center](#)
- The Microsoft Entra admin center

Hybrid

With hybrid identity, passwords are stored in AD DS so you must use on-premises AD DS tools to manage user account passwords. Even when using Password Hash Synchronization (PHS), in which Microsoft Entra ID stores a hashed version of the already hashed version in AD DS, you and users must manage their passwords in AD DS.

With [password writeback](#), your users can change their AD DS passwords through Microsoft Entra ID.

Prevent bad passwords

All your users should be using [Microsoft's password guidance](#) to create their user account passwords.

To prevent users from creating an easily-determined password, use Microsoft Entra password protection, which uses both a global banned password list and an optional custom banned password list that you specify. For example, you can specify terms that are specific to your organization, such as:

- Brand names
- Product names
- Locations (for example, such as company headquarters)
- Company-specific internal terms
- Abbreviations that have specific company meaning

You can ban bad passwords [in the cloud](#) and for your [on-premises AD DS](#).

Simplify user sign-in

Microsoft Entra seamless single sign-on (Microsoft Entra seamless SSO) works with PHS and Pass-Through Authentication (PTA), to allow your users to sign in to services that use Microsoft Entra 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 configure Microsoft Entra seamless SSO with the Microsoft Entra Connect tool. See the [instructions to configure Microsoft Entra seamless SSO](#).

Simplify password updates to AD DS

With password writeback, you can allow users to reset their passwords through Microsoft Entra ID, which is then replicated to AD DS. Users don't need to access their on-premises AD DS to update their passwords. 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 Microsoft Entra ID Protection 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 [Microsoft Entra SSPR with password writeback](#).

 **Note**

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

Simplify password resets

Self-service password reset (SSPR) allows 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. You must enable [password writeback](#) before you can deploy password resets.

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

Feedback

Was this page helpful?



[Provide product feedback](#) ↗

Manage Microsoft 365 groups

Article • 02/20/2024

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

You can manage Microsoft 365 groups in several different ways, depending on your configuration. You can manage user accounts in the [Microsoft 365 admin center](#), PowerShell, in Active Directory Domain Services (AD DS), or in the [Microsoft Entra admin center](#).

Plan for where and how you'll manage your groups

Where and how you can manage your user accounts depends on the identity model you want to use for your Microsoft 365. The two overall models are cloud-only and hybrid.

Cloud-only

You create and manage groups with:

- [The Microsoft 365 admin center](#)
- PowerShell
 - [Manage Microsoft 365 groups with PowerShell](#)
- [Microsoft Entra admin center](#)

Hybrid

To manage hybrid groups, you can use the same tools you use for cloud-only groups. AD DS groups are synchronized with Microsoft 365 from AD DS, so you must use on-premises AD DS tools to manage these groups.

You can also create and manage Microsoft Entra groups that are separate from AD DS groups but can contain users and groups from AD DS.

Allow users to create and manage their own groups

Microsoft Entra ID allows groups that can be managed by group owners instead of IT administrators. Known as *self-service group management*, this feature allows group

owners who aren't 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 Microsoft Entra security and Microsoft 365 groups. It is not available for mail-enabled groups, distribution lists, or any group that has been synchronized from AD DS.

For more information, see the [instructions to configure a Microsoft Entra group for self-service management](#).

Set up dynamic group membership

Microsoft Entra ID supports configuring a series of rules that automatically add or remove user accounts as members of a Microsoft Entra 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's 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 Microsoft Entra group, based on the user account attribute Department set to "Sales".

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

Set up automatic licensing

You can configure security groups in Microsoft Entra ID 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 unassigned from the user account.

For Microsoft 365 Enterprise, you'll configure Microsoft Entra security groups to assign the appropriate Microsoft 365 Enterprise license.

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.

For more information, see [Group-based licensing basics in Microsoft Entra ID](#).

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

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Manage Microsoft 365 identity governance

Article • 07/26/2024

Identity governance is all about protecting, monitoring, and auditing access to critical assets while ensuring employee productivity. For example, with identity governance, you can ensure that the right users have the right access to the right resources and determine if that access changes over time.

For more information, See this [overview of identity governance for Microsoft Entra ID](#).

Set up Microsoft Entra access reviews

Microsoft Entra access reviews allow you to review a user's access to ensure only the right people have continued access. For example:

- As a new employee joins your organization, you need to ensure they have the right access to be productive.
- As that employee moves to other teams, locations, or departments, you need to ensure that their access to previous teams, locations, or departments are removed as needed.
- When that employee or a guest leaves your organization, you need to ensure their access is removed.

This is especially important if your organization is subject to security audits to determine if user accounts have too much access, which could result in fines if in violation of industry or regional regulations.

For more information, see the [overview of access reviews](#).

See these articles to configure different types of access reviews:

- [Groups and apps](#)
- [Microsoft Entra roles](#)
- [Azure resource roles](#)

Set up Microsoft Entra entitlement management

With Microsoft Entra entitlement management, you can manage the identity and access lifecycle at scale by automating access request workflows, access assignments, reviews, and expiration.

Your employees need access to various groups, applications, and sites to perform their job. Managing this access can be challenging because requirements change, new applications are added, or users need additional access rights. When you collaborate with other organizations, you may not know who in the other organization needs access to your organization's resources, and outside users won't know what applications, groups, or sites your organization is using.

Microsoft Entra entitlement management can help you more efficiently manage access to groups, applications, and SharePoint sites for internal and outside users.

For more information, see the [overview of Microsoft Entra entitlement management](#).

Feedback

Was this page helpful?



[Provide product feedback](#) ↗

View directory synchronization status in Microsoft 365

Article • 12/18/2023

If you have integrated your on-premises Active Directory Domain Services (AD DS) with Microsoft Entra ID by synchronizing your on-premises environment with Microsoft 365, you can also check the status of your synchronization.

View directory synchronization status

- Sign in to the [Microsoft 365 admin center](#) and choose **DirSync Status** on the home page.
- Alternately, you can go to **Users > Active users**, and on the **Active users** page, select the **Ellipsis > Directory synchronization**. On the **Directory Synchronization** pane, choose **Go to DirSync management**.

Information on the Manage directory synchronization page

The following table lists the features you can get information about on the page.

If there's a problem with your directory synchronization, the errors are listed on this page as well. For more information about different errors you might encounter, see [Identify directory synchronization errors in Microsoft 365](#).

[] [Expand table](#)

Item	What it's for
Domains verified	Number of domains in your Microsoft 365 tenant that you have verified you own.
Domains not verified	Domains you have added, but not verified.
Directory sync enabled	True or False. Specifies whether you have enabled directory sync.
Latest directory sync	Last time directory sync ran. Will display a warning and a link to a troubleshooting tool if the last sync was more than three days ago.

Item	What it's for
Password sync enabled	True or False. Specifies whether you have password hash sync between our on-premises and your Microsoft 365 tenant.
Last Password Sync	Last time password hash sync ran. Will display a warning and a link to a troubleshooting tool if the last sync was more than three days ago.
Directory sync client version	Contains a download link if a new version of Microsoft Entra Connect has been released.
Directory sync service account	Displays the name of your Microsoft 365 directory sync service account.

Monitor synchronization health

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

The key design decision of how to use Microsoft Entra Connect Health is based on how you're using Microsoft Entra Connect:

- If you're using the **managed authentication** option, start with [Using Microsoft Entra Connect Health with sync](#) to understand and configure Microsoft Entra 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 Microsoft Entra Connect Health with AD FS](#) to understand and configure Microsoft Entra Connect Health.

When complete, you'll have:

- The Microsoft Entra Connect Health agent installed on your on-premises identity provider servers.
- The Microsoft Entra Connect Health portal displaying the current state of your on-premises infrastructure and synchronization activities with the Microsoft Entra tenant for your Microsoft 365 subscription.

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

View directory synchronization errors in Microsoft 365

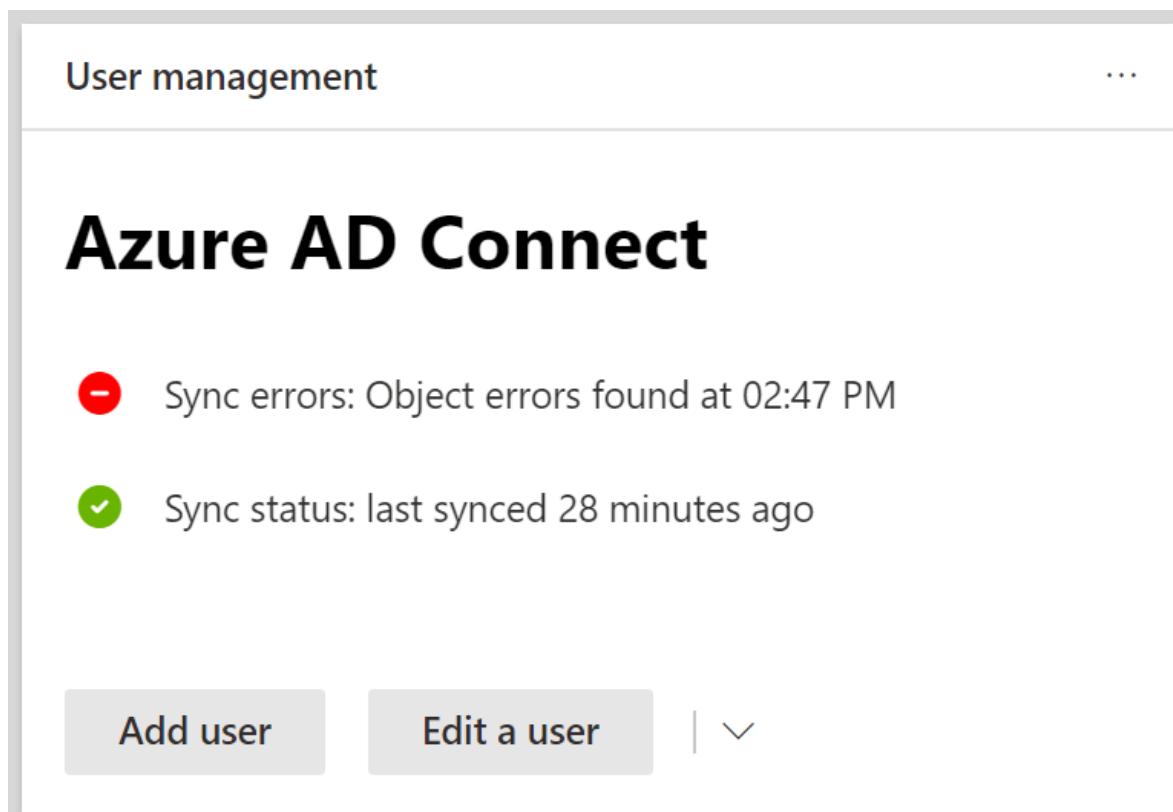
Article • 07/17/2024

You can view directory synchronization errors in the [Microsoft 365 admin center](#). Only the User object errors are displayed. To view errors with PowerShell, see [Identify objects with DirSyncProvisioningErrors](#).

View directory synchronization errors in the Microsoft 365 admin center

To view any errors in the Microsoft 365 admin center:

1. Sign in to the [Microsoft 365 admin center](#) with a Hybrid Identity Administrator account.
2. On the Home page, you'll see the **User management** card.



3. On the card, choose **Sync errors** under Microsoft Entra Connect to see the errors on the **Directory sync errors** page.

The screenshot shows the Microsoft 365 admin center interface. On the left, there's a navigation sidebar with categories like Home, Users, Groups, Roles, Billing, Support, Settings, and Reports. Under 'Settings', 'DirSync errors' is selected. The main content area is titled 'Directory sync errors' and contains a message about identifying objects from on-premises Active Directory that have unique UserPrincipalName and ProxyAddress attributes. It includes a link to 'Learn more about Azure AD Connect sync'. Below this, a table lists 'Duplicated attribute' entries for 'Proxy address' with values 'SMTP:DList2@fdx.exchcloud.com' and 'Display name' 'DList2' and 'Object type' 'Group'. A search bar and a refresh button are at the top right.

4. Choose any of the errors to display the details pane with information about the error and tips on how to fix it.

This screenshot shows the same 'Directory sync errors' page after selecting one of the errors. The main content area now displays a detailed view of the 'Proxy address' entry. It includes sections for 'Delete duplicate attributes' and 'Group:DList2'. The 'Delete duplicate attributes' section provides instructions to decide which group should use the attribute or remove it from both. The 'Group:DList2' section lists various properties: Last sync time (2019-11-01T15:45:16Z), Source anchor (IkysnD8qQy50l9ANWxA7A==), Source (On-premises Active Directory), Date created (Sun, 29 Oct 2017 16:40:46 GMT), and a long list of proxy addresses. The list of proxy addresses includes 'SMTP:DList2@fdx.exchcloud.com (Removed automatically)', 'smtp:DList2@fdx.exchcloud.com', 'smtp:DList2@FDK.onmicrosoft.com', and 'smtp:DList2@Grp@FDK.onmicrosoft.com'. A 'Delete this group' button is also present.

After viewing, see [fixing problems with directory synchronization for Microsoft 365](#) to correct any identified issues.

Feedback

Was this page helpful?

Yes

No

[Provide product feedback ↗](#)

Fixing problems with directory synchronization for Microsoft 365

Article • 07/22/2024

With directory synchronization, you can continue to manage users and groups on-premises and synchronize additions, deletions, and changes to the cloud. But setup is a little complicated and it can sometimes be difficult to identify the source of problems. We have resources to help you identify potential issues and fix them.

How do I know if something is wrong?

The first indication that something is wrong is when the DirSync Status tile in the Microsoft 365 admin center indicates there's a problem.

You'll also receive a mail (to the alternate email and to your admin email) from Microsoft 365 that indicates your tenant has encountered directory synchronization errors. For details see [Identify directory synchronization errors in Microsoft 365](#).

How do I get Microsoft Entra Connect tool?

In the [Microsoft 365 admin center](#), navigate to **Users > Active users**. Click the More menu (three dots) and select **Directory synchronization**.

Follow the [instructions in the wizard](#) to download Microsoft Entra Connect.

If you're still using Azure Active Directory (Azure AD) Sync (DirSync), take a look at [How to troubleshoot Azure Active Directory Sync Tool installation and Configuration Wizard error messages in Microsoft 365](#) for information about the system requirements to install dirsync, the permissions you need, and how to troubleshoot common errors.

To update from Azure AD Sync to Microsoft Entra Connect, see [the upgrade instructions](#).

Resolving common causes of problems with directory synchronization in Microsoft 365

Synchronized objects aren't appearing or updating online, or I'm getting synchronization error reports from the Service.

- Identity synchronization and duplicate attribute resiliency

I have an alert in the admin center, or am receiving automated emails that there hasn't been a recent synchronization event

- Troubleshoot connectivity issues with Microsoft Entra Connect
- Microsoft Entra Connect Accounts and permissions
- Microsoft Entra Connect Sync: How to manage the Microsoft Entra service account
- Directory synchronization to Microsoft Entra ID stops or you're warned that sync hasn't registered in more than a day ↗

Password hashes aren't synchronizing, or I'm seeing an alert in the admin center that there hasn't been a recent password hash synchronization

- Implementing password hash synchronization with Microsoft Entra Connect Sync

I'm seeing an alert that Object quota exceeded

- We have a built-in object quota to help protect the service. If you have too many objects in your directory that need to sync to Microsoft 365, you have to [Contact support for business products](#) ↗ to increase your quota.

I need to know which attributes are synchronized

- You can find a list of all the attributes that are synced between on-premises and the cloud [right here](#) ↗.

I can't manage or remove objects that were synchronized to the cloud

- Are you ready to manage objects in the cloud only? Or is there an object that was deleted on-premises, but is stuck in the cloud? Take a look at this [Troubleshooting Errors during synchronization](#) and [support article](#) for guidance on how to resolve these issues.

I got an error message that my company has exceeded the number of objects that can be synchronized

- You can read more about this issue [here](#).

Other resources

- Script to fix duplicate user principal names
 - How to prepare a nonroutable domain (such as .local domain) for directory synchronization
 - Script to count total synchronized objects
 - Use PowerShell to fix duplicate UPN ↗
 - Use PowerShell to fix duplicate email addresses ↗
-

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Turn off directory synchronization for Microsoft 365

Article • 07/16/2024

You can use PowerShell to turn off directory synchronization and convert your synchronized users to cloud-only. However, it isn't recommended that you turn off directory synchronization as a troubleshooting step. If you need assistance with troubleshooting directory synchronization, see the [Fixing problems with directory synchronization for Microsoft 365](#) article.

Contact support  if you need help with this procedure.

Turn off directory synchronization

To turn off Directory synchronization:

1. First, install the required software and connect to your Microsoft 365 subscription.

For instructions, see [Connect with the Microsoft Graph PowerShell module for Windows PowerShell](#).

2. Use **Update-MgBetaOrganization** to disable directory synchronization:

PowerShell

```
# Install v1.0 and beta Microsoft Graph PowerShell modules
Install-Module Microsoft.Graph -Force
Install-Module Microsoft.Graph.Beta -AllowClobber -Force

# Connect With Hybrid Identity Administrator Account
Connect-MgGraph -scopes
"Organization.ReadWrite.All,Directory.ReadWrite.All"

# Verify the current status of the DirSync Type
Get-MgOrganization | Select OnPremisesSyncEnabled

# Store the Tenant ID in a variable named organizationId
$organizationId = (Get-MgOrganization).Id

# Store the False value for the DirSyncEnabled Attribute
$params = @{
    onPremisesSyncEnabled = $false
}

# Perform the update
Update-MgBetaOrganization -OrganizationId $organizationId -BodyParameter
$params
```

```
# Check that the command worked  
Get-MgOrganization | Select OnPremisesSyncEnabled
```

ⓘ Note

If you use this command, you must wait 72 hours before you can turn directory synchronization back on. Visit [Update-MgBetaOrganization](#) for more detailed information on cmdlet usage and switches. This process will clear the following on-premises properties:

- DnsDomainName
- NetBiosName
- OnPremisesDistinguishedName
- OnPremisesSamAccountName
- OnpremisesUserPrincipalName

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Compliance for Microsoft 365 for enterprise

Article • 05/13/2024

Most organizations have business or legal requirements that govern how data is used, shared, and retained. Some organizations also have data residency requirements or regulatory requirements that restrict communication between certain users and groups.

[Microsoft Compliance](#) contains a plethora of information to help organizations understand how we as a cloud service provider can satisfy those requirements. See the [comprehensive list of compliance offerings](#) for information detailing how Microsoft complies with national, regional, and industry-specific requirements governing the collection and use and data.

Shared responsibility model

Security and compliance in the cloud is a [shared responsibility](#) and the division of those responsibilities between the cloud service provider and customer depends on the cloud offering utilized. Microsoft works to ensure that we are compliant with industry and international standards, and customers are responsible for ensuring their data within the [Microsoft Cloud](#) is protected in a manner that is compliant with the standards and regulations imposed on the customer.

Inheritance of compliance features and settings

Microsoft 365 apps, depending on the app, inherit compliance features and settings from Microsoft Teams, Exchange Online, SharePoint Online, Azure, and Viva Engage. In addition, all Microsoft 365 services are built on the [Microsoft Graph API](#).

For detailed information on each service, see:

[Microsoft 365 Plan for security and compliance](#)

[Microsoft Teams Overview of security and compliance in Microsoft Teams](#)

[Microsoft SharePoint Plan compliance requirements for SharePoint and OneDrive](#)

[Microsoft Graph Use the Microsoft Graph compliance and privacy APIs](#)

[Viva Engage Overview of security and compliance in Viva Engage](#)

[Microsoft Entra ID](#) Microsoft Entra security baseline for Microsoft Entra ID

[Azure](#) [Azure](#), Dynamics 365, Microsoft 365, and Power Platform compliance offerings

General Data Protection Regulation (GDPR)

All Microsoft 365 apps and services support compliance with EU General Data Protection Regulation (GDPR) requirements. For detailed information, see [the GDPR Overview](#).

Data residency

Multi-Geo is Microsoft 365 feature that allows organizations to span their storage over multiple geo locations and specify where to store users' data. For multinational customers with data residency requirements, you can use this feature to ensure that each user's data is stored in the geo location necessary for compliance. For more info about this feature, see [Multi-Geo Capabilities in OneDrive and SharePoint](#).

For more information about Microsoft 365 Multi-Geo, see [Microsoft 365 Multi-Geo](#).

Microsoft Purview

[Microsoft Purview](#) is a family of data governance, risk, and compliance solutions that can help your organization govern, protect, and manage your entire data estate.

Data lifecycle management

Use data lifecycle management capabilities in Microsoft Purview to govern your OneDrive and SharePoint content for compliance or regulatory requirements. The following table describes the capabilities to help you keep the content you need and delete what you don't need.

[] Expand table

Capability	What problems does it solve?	Get started
Retention policies and retention labels Learn about retention for SharePoint and OneDrive	Retain or delete content with policy management for SharePoint and OneDrive documents	Create and configure retention policies Create retention labels for exceptions to your retention policies

Deleted users' data

When a user leaves your organization and you've deleted that user's account, what happens to the user's data? When considering data retention compliance, determine what needs to happen with the deleted user's data. For some organizations, retaining deleted user data could be important continuity and preventing critical data loss.

If a user's Microsoft 365 account is deleted, their OneDrive files are preserved for 30 days. To change this setting, [Set the OneDrive retention for deleted users](#).

By default, when a user is deleted, the user's manager is automatically given access to the user's OneDrive. To change this, see [OneDrive retention and deletion](#).

Information protection

Microsoft Purview Information Protection capabilities help you discover, classify, and protect sensitive information in OneDrive and SharePoint. The following table describes these capabilities. Consider if you want to implement any of these capabilities as part of your OneDrive and SharePoint rollout.

[] [Expand table](#)

Capability	What problems does it solve?	Get started
Sensitive information types	Identifies sensitive data by using built-in or custom regular expressions or a function. Corroborative evidence includes keywords, confidence levels, and proximity.	Customize a built-in sensitive information type
Trainable classifiers	Identifies sensitive data by using examples of the data you're interested in rather than identifying elements in the item (pattern matching). You can use built-in classifiers or train a classifier with your own content.	Get started with trainable classifiers
Sensitivity labels	A single solution across apps, services, and devices to label and protect your data as it travels inside and outside your organization. Sensitivity labels can be used to protect files themselves or individual SharePoint sites and teams.	Enable sensitivity labels for Office files in SharePoint and OneDrive Use sensitivity labels to protect content in Microsoft Teams, Microsoft 365 Groups, and SharePoint sites
Data loss	Helps prevent unintentional sharing of sensitive	Get started with the default

Capability	What problems does it solve?	Get started
prevention	items.	DLP policy

File sync

The OneDrive sync app has policies that you can use to help you maintain a compliant environment. Consider configuring these policies before you roll out SharePoint and OneDrive.

[\[+\] Expand table](#)

Policy	Windows GPO	Mac
Allow syncing OneDrive accounts for only specific organizations	AllowTenantList	AllowTenantList
Block syncing OneDrive accounts for specific organizations	BlockTenantList	BlockTenantList
Prevent users from syncing libraries and folders shared from other organizations	BlockExternalSync	BlockExternalSync
Prevent users from syncing personal OneDrive accounts	DisablePersonalSync	DisablePersonalSync
Exclude specific kinds of files from being uploaded	EnableODIgnoreListFromGPO	EnableODIgnore

Information barriers

Microsoft Purview Information Barriers is a compliance solution that allows you to restrict two-way communication and collaboration between groups and users in Microsoft Teams, SharePoint, and OneDrive. Often used in highly regulated industries, information barriers can help to avoid conflicts of interest and safeguard internal information between users and organizational areas.

When information barrier policies are in place, users who shouldn't communicate or share files with other specific users won't be able to find, select, chat, or call those users. Information barrier policies automatically put checks in place to detect and prevent unauthorized communication and collaboration among defined groups and users.

If your business requires information barriers, see [Learn about information barriers](#) and [Use information barriers with SharePoint](#) to get started.

Related articles

[Implement compliance in Microsoft 365](#)

[Compliance in Microsoft Teams](#)

[Compliance in Microsoft Viva](#)

[Compliance in SharePoint and OneDrive](#)

[Compliance in Microsoft Cloud for Retail](#)

[Windows Privacy Compliance Guide](#)

[Microsoft Purview Compliance Portal](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Security for Microsoft 365 for enterprise

Article • 05/13/2024

Microsoft 365 for enterprise follows all the security best practices and procedures such as service-level security through defense-in-depth, customer controls within the services, security hardening, and operational best practices. For full details, see the [Microsoft Trust Center](#) and [Microsoft Compliance](#).

Trustworthy by design

Microsoft 365 is designed and developed in compliance with the Microsoft Trustworthy Computing Security Development Lifecycle (SDL), which is described at [Microsoft Security Development Lifecycle \(SDL\)](#). The first step in creating a more secure unified communications, collaboration, and productivity system was to design threat models and test each feature as it was designed. Multiple security-related improvements were built into the coding process and practices. Build-time tools detect buffer overruns and other potential security threats before the code is checked in to the final product. It's impossible to design against all unknown security threats. No system can guarantee complete security. However, because product development embraced secure design principles from the start, Microsoft 365 incorporates industry standard security technologies as a fundamental part of its architecture.

Security Framework for Microsoft 365

Microsoft 365 endorses security ideas like Zero Trust, and principles of Least Privilege access. This section gives an overview of fundamental elements that form a security framework for Microsoft 365.

Core elements include:

- Microsoft Entra ID, which provides a single trusted back-end repository for user accounts. User profile information is stored in Microsoft Entra ID through the actions of Microsoft Graph.
 - There might be multiple tokens issued which you might see if tracing your network traffic.
- Transport Layer Security (TLS) encrypts the channel in motion. Authentication takes place using either mutual TLS (MTLS), based on certificates, or using Service-to-Service authentication based on Microsoft Entra ID.
- Point-to-point audio, video, and application sharing streams are encrypted and integrity checked using Secure Real-Time Transport Protocol (SRTP).

- You'll see OAuth traffic in your trace, particularly around token exchanges and negotiating permissions while switching between tabs in Teams, for example to move from Posts to Files. For an example of the OAuth flow for tabs, [see this document](#).
- Microsoft 365 uses industry-standard protocols for user authentication, wherever possible.

Microsoft Entra ID

Microsoft Entra ID functions as the directory service for Microsoft 365 and Office 365. It stores all user and application directory information and policy assignments.

Encryption in Microsoft 365

There are multiple layers of encryption at work within Microsoft 365 to protect your organization's content. For an overview of encryption in Microsoft 365, see [Encryption in Microsoft 365](#).

User and Client Authentication

A trusted user is one whose credentials have been authenticated by Microsoft Entra ID in Microsoft 365 or Office 365.

Authentication is the provision of user credentials to a trusted server or service. Microsoft 365 uses the following authentication protocols, depending on the status and location of the user.

- **Modern Authentication (MA)** is the Microsoft implementation of OAUTH 2.0 for client to server communication. It enables security features such as multifactor authentication and Conditional Access. To use MA, both the online tenant and the clients need to be enabled for MA. The Microsoft 365 clients across PC and mobile, and the web clients, all support MA.

Note

If you want more information on Microsoft Entra authentication and authorization methods, this article's Introduction and 'Authentication basics in Microsoft Entra ID' sections will help.

Microsoft 365 authentication is accomplished through Microsoft Entra ID and OAuth. The process of authentication can be simplified to:

- User sign in > token issuance > next request use issued token.

Requests from clients to cloud services are authenticated and authorized by Microsoft Entra ID with the use of OAuth. Users with valid credentials issued by a federated partner are trusted and pass through the same process as native users. However, further restrictions can be put into place by administrators.

For media authentication, the ICE and TURN protocols also use the Digest challenge as described in the IETF TURN RFC.

Endpoint security

Microsoft is unifying user-facing Microsoft 365 apps and services to a single and consistent domain: `**cloud.microsoft**`.

The growth of Microsoft cloud services led to the expansion of the domain space they occupy, resulting in hundreds of domains. This fragmentation is a challenge for end user navigation, administrative simplicity, and the development of cross-app experiences.

The `*.microsoft*` top-level domain is exclusive to Microsoft. The new domain doesn't have traditional suffixes such as .com or .net in the end. This is by design.

`cloud.microsoft` resides under the `.microsoft` top-level domain, for which Microsoft is a registry operator and the sole registrant. This domain allows for extra security, privacy, and protection against spoofing when you interact with apps within that domain. You can trust that any website or app that ends with `cloud.microsoft` is an official Microsoft product or service.

For more information, see [Unified `cloud.microsoft` domain for Microsoft 365 apps](#).

Related articles

[Top 12 tasks for security teams to support working from home](#)

[Microsoft Trust Center](#)

[Optimize Microsoft 365 or Office 365 connectivity for remote users using VPN split tunneling](#)

[Understand how security works in Microsoft Viva](#)

[Security guide for Microsoft Teams overview](#)

[Security in Microsoft Teams](#)

[Windows operating system security](#)

[Dynamics 365 security](#)

[Security in Microsoft Cloud for Retail](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Privacy for Microsoft 365 for enterprise

Article • 05/13/2024

When an organization is considering relying on Microsoft 365 for communication and collaboration, privacy is something that needs to be addressed at every level. The topics we discuss in this article should address your privacy concerns when planning your Microsoft 365 implementation, or at any point during Microsoft 365 usage.

What personal data does Microsoft 365 collect and for what purposes does Microsoft 365 use this data?

Microsoft processes the personal data in Microsoft 365 to deliver the services and for the purposes outlined in the [Product Terms](#) and the [Microsoft Online Services Data Protection Addendum \(DPA\)](#). Microsoft 365, as an integrated set of cloud-based services, processes various types of personal data as part of delivering the services.

To the extent Microsoft 365 processes personal data with Microsoft's legitimate business operations, Microsoft is an independent data controller for such use and is responsible for complying with all applicable laws and controller obligations.

Legal Basis of Processing

Our customers are controllers for the data provided to Microsoft, as set forth in the [Product Terms](#) and the [Microsoft Online Services Data Protection Addendum \(DPA\)](#), and they determine legal basis of processing. Microsoft, in turn, processes the data on the customers' instructions, as a processor.

What third parties have access to personal data?

Microsoft won't disclose personal data except:

1. as the customer directs (including as required to complete phone calls);
2. as described in the Online Service Terms (such as the use of authorized subcontractors to provide certain components of services);
3. as required by law.

If law enforcement contacts Microsoft with a demand, Microsoft will attempt to redirect the law enforcement agency to request that personal data directly from the customer. If compelled to disclose personal data to law enforcement, Microsoft will promptly notify the customer and provide a copy of the demand unless legally prohibited from doing so. For more information about data that we disclose in response to requests from law enforcement and other government agencies, please see our [Law Enforcement Requests Report](#).

Where does Microsoft 365 transfer and store personal data?

Personal data is transferred and stored as set forth in the [Online Service Terms](#), the [Product Terms](#) and the [Microsoft Online Services Data Protection Addendum \(DPA\)](#).

We have information on the [Microsoft 365 Data Residency overview and definitions](#) if you need to learn more.

How long does Microsoft 365 retain personal data?

Microsoft 365 retains your data for the minimum amount of time necessary to deliver the service.

Because this data is required to provide the service, this typically means that we retain personal data until the user stops using Microsoft 365, or until the user deletes personal data. If a user (or an administrator on the user's behalf) deletes the data, Microsoft will ensure that all copies of the personal data are deleted within 30 days.

If a company terminates service with Microsoft, corresponding personal data will all be deleted between 90 and 180 days of service termination.

In some circumstances, local laws require that Microsoft 365 retains telephone records (for billing purposes) for a specific period of time, in those circumstances Microsoft 365 follows the law for each region.

Additionally, if a company requests that Microsoft 365 holds a user's data to support a legal obligation, Microsoft will respect the company administrator's request.

Right to withdraw consent

If Microsoft 365 processes any personal data based on consent, you may have the right to withdraw your consent at any time. You should direct your request to withdraw consent to your administrator, where your administrator is the controller of the personal data at issue.

Contact Details of Microsoft's Data Protection Officer

If you have a privacy concern, complaint or question for the Microsoft Chief Privacy Officer and EU Data Protection Officer, contact us by using [our web form](#). Our EU Data Protection Officer is located at Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland. Telephone: +353 1 706 3117. You can also raise a concern or lodge a complaint with a data protection authority or other official with jurisdiction.

Related articles

[Windows Privacy Compliance Guide](#)

[Understand how privacy works in Microsoft Viva](#)

[Microsoft Teams privacy](#)

[Overview of privacy controls for Microsoft 365 Apps for enterprise](#)

[Online Service Terms](#)

[Product Terms](#)

[Microsoft Online Services Data Protection Addendum \(DPA\)](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Cloud services roadmap for Microsoft 365

Article • 08/28/2024

To get the creativity, teamwork, and productivity benefits of Microsoft 365 for enterprise, deploy the cloud services that best fit your organization's needs.

Deploy

To deploy your cloud services:

- [Get your services ready](#)
- [Migrate your on-premises data to Microsoft 365](#)
- Get your cloud services set up for your users
 - [Exchange Online](#)
 - [SharePoint](#)
 - [Microsoft Teams](#)
 - [Viva Engage ↗](#)
- [Train your users](#)

Manage

To manage your cloud services:

- [Check your service health](#)
- [Understand your support options](#)
- Administer your cloud services
 - [Exchange Online](#)
 - [SharePoint ↗](#)
 - [Skype for Business](#)
 - [Teams](#)
 - [Viva Engage ↗](#)

How Microsoft does cloud services for Microsoft 365

For information about how Microsoft IT has deployed or is managing Microsoft 365 cloud services:

1. Go to Microsoft IT Showcase .
2. Select **Search content**.
3. Under **Refine results**, select **IT Pro** under **Audience**, and then under **Product**, select a cloud service.

Next step

Start your cloud services implementation. For guidance, see [Configure Microsoft 365 Enterprise services and applications](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback !\[\]\(1211315d3f8f154a702f4c244ae46241_img.jpg\)](#)

Configure Microsoft 365 Enterprise services and applications

Article • 07/24/2024

Our [basic set up instructions](#) help you get everyone using your Microsoft 365 services and applications in the shortest time possible. Sometimes getting things configured before everyone starts using them is preferred. For example if you want to configure mail routing, file storage, or sharing policies.

If you want help getting Microsoft 365 set up, use [FastTrack](#) or the [Setup guides for Microsoft 365 and Office 365 services](#).

 [Expand table](#)

Services & applications	Resources
Microsoft 365 Suite	<ul style="list-style-type: none">- Add your company branding to Microsoft 365 Sign In Page- Add customized help desk info to the Microsoft 365 help pane- Add integration with Microsoft Entra ID and other applications.- Activate and use mobile device management in Microsoft 365- Monitor Microsoft 365 connectivity
Email (Exchange Online)	<ul style="list-style-type: none">- Use the Exchange migration advisor to get customized setup guidance- Set up Exchange Online Protection
Sites (SharePoint)	<ul style="list-style-type: none">- Configure hybrid functionality for SharePoint Server- Use the SharePoint Planning Guide or the SharePoint deployment advisor to plan and configure additional features
IM and online meetings (Teams)	<ul style="list-style-type: none">- Microsoft Teams deployment overview- Meetings and conferencing in Microsoft Teams- Plan your Teams voice solution
File storage & sharing (OneDrive and SharePoint)	<ul style="list-style-type: none">- Set up Microsoft 365 file storage and sharing: Learn when you should use OneDrive to store files and when you should use SharePoint team sites- Use the OneDrive setup guide to get customized setup guidance
Microsoft 365 applications	<ul style="list-style-type: none">- Microsoft 365 administrators should use the Microsoft 365 Apps deployment documentation to get help planning a Microsoft 365 Apps for enterprise deployment or upgrade.- Power BI for Microsoft 365 admin center- Get started with Project for the web.- Microsoft Intune deployment advisor

**Services &
applications**

Resources

**Enterprise Social
(Viva Engage)**

- [Introducing Microsoft Viva Engage](#)
- Use the [Viva Engage Enterprise setup guide](#) to get customized setup guidance

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

IT Admins - Overview of external collaboration options in Microsoft 365

Article • 01/17/2024

With Microsoft 365, your users can collaborate with people outside your organization in a variety of ways. Users can share files, invite guests to teams, have meetings with external participants, and chat with people from other organizations. This article covers the external collaboration options available and links to the content you need to configure each.

The following table shows the primary ways people from outside your organization can access your Microsoft 365 resources:

[Expand table](#)

Activity	Account type	Default setting
Authenticated file and folder sharing	Guest account	Enabled
Site sharing	Guest account	Enabled
Team sharing	Guest account	Enabled
Cross-cloud sharing	Guest account	Disabled
Multitenant organization sharing	Guest account	Disabled
Shared channel in Teams	Existing Microsoft 365 external account	Disabled
External chat and meetings	Existing Microsoft 365 external account	Enabled
Cross-cloud meetings	Existing Microsoft 365 external account	Disabled
Anonymous meeting join	None	Enabled
Unauthenticated file and folder sharing	None	Enabled

People outside your organization don't have access unless a user in your organization initiates one of these activities. You can disable any of these settings if you don't want to allow that activity in your organization.

If you have business processes or requirements around allowing collaboration with external organizations, see [Onboard trusted vendors to collaborate in Microsoft 365](#).

Document, site, and team sharing with guest accounts

Sharing documents, sites, and teams with people outside your organization uses *guest accounts*. Guest accounts are a type of account in Microsoft Entra ID that is managed through [Microsoft Entra B2B collaboration](#). They can be used to share resources in your organization with anyone who has an email address, including people in [other Microsoft 365 cloud environments](#). You can manage guest accounts the same way you manage users in your organization. Guests don't require a license for most features of collaboration.

Guests can only access resources that you specifically share with them.

If the guest has a work or school account in another organization, or a Microsoft account, they can log in with their regular username and password. If they have a different type of account - such as a Gmail account - they can log in by using a one-time passcode that is sent to their email address.

With guests you can:

- Invite them to Microsoft 365 groups, teams, or SharePoint sites where they can collaborate with people in your organization.
- Share a single file or a folder with them which they can view or edit depending on the permissions you give them.

For information about how to plan for collaboration with guests in Microsoft 365, see the following references:

- [Plan external collaboration](#)
- [Set up secure file sharing and collaboration with Microsoft Teams](#)

For information about how to set up Microsoft 365 for collaboration with guests, see the following references:

- [Collaborate with guests on a document](#)
- [Collaborate with guests in a site](#)
- [Collaborate with guests in a team](#)

Shared channels

Shared channels are a type of Teams channel that allows you to share with people outside the team, including people in other Microsoft 365 organizations. While shared channels is turned on by default in Teams, external collaboration with shared channels is disabled by default. External collaboration with shared channels uses [Microsoft Entra B2B direct connect](#) which allows you to add people from other Microsoft 365 organizations to Teams channels without the need for creating a guest account.

Shared channels have a particular advantage over guest accounts in that they don't require external participants to switch accounts in the Teams desktop client or log into your organization. They can use their regular work or school account and access the channel directly.

Sharing channels with people outside your organization requires that your organization and the external organization both configure an organizational relationship in Microsoft Entra B2B Direct Connect.

For information about how to set up Microsoft 365 for external collaboration with shared channels, see the following references:

- [Plan external collaboration](#)
- [Shared channels in Microsoft Teams](#)
- [Collaborate with external participants in a channel](#)

External chat and meetings

Users in your organization can chat, add users to meetings, and use audio or video conferencing in Teams with users in external Microsoft 365 organizations. By default, users in your organization can communicate in these ways with all other Microsoft 365 domains. People in other organizations can communicate in these ways with your users if they know the user's email address. You can allow or block specific domains or block all domains if you want to disable the feature.

You can also allow users in your organization to communicate with people from outside your organization who are using Teams accounts that aren't managed by an organization, as well as Skype for Business (online and on-premises) and Skype users.

Guest accounts aren't used as part of external chat and meetings. External participants remain signed in to their organization or to Skype and can communicate directly with people in your organization. They don't have access to your teams or channels.

For information about how to set up Microsoft 365 for external chat and meetings, see the following references:

- [Use guest access and external access to collaborate with people outside your organization](#)
- [Manage external access in Microsoft Teams.](#)

Anonymous meeting join

People from outside your organization can join meetings in the following ways:

- If they're logged in to your organization with a guest account, they join meetings as a guest.
- If they're logged in to a different organization with a work or school account, and both organizations trust each other in [external access](#) or are part of [cross-cloud meeting connection](#), they join meetings as an external participant.
- If they're not a guest or external participant, they must join meetings anonymously.

If the anonymous join setting is enabled for your organization, anonymous users can join a meeting using a meeting link that has been shared with them (such as a link in the meeting invitation). They're prompted to enter a display name of their choosing when joining the meeting anonymously. Depending on the lobby settings, the anonymous user may be automatically admitted to the meeting, or be added to a lobby where the meeting organizer (or meeting participants with the presenter role) can allow or deny access to the meeting.

It is not possible to verify the identity of anonymous users before, during or after the meeting.

You can control anonymous users' ability to join meetings at the organization level and through meeting policy settings. For information about configuring anonymous join for meetings, see [Manage anonymous participant access to Teams meetings](#).

Unauthenticated file and folder access

In Microsoft 365, files and folders in Teams, SharePoint, and OneDrive can be shared using unauthenticated - or *Anyone* - links. Anyone links give access to the shared item to anyone who has the link. Anyone links can be shared with others, giving those people access to the file or folder.

People using an Anyone link don't have to authenticate, and their access can't be audited. File and folder owners can revoke access at any time by deleting the link.

Anyone links can't be used with files in a Teams shared channel site.

For information about working with anonymous file and folder sharing, see the following references:

- [Manage sharing settings](#)
- [Best practices for sharing files and folders with unauthenticated users](#)

Cross-cloud sharing and meetings

You can collaborate with users in other Microsoft Azure cloud environments (such as between Microsoft Azure Commercial and Microsoft Azure Government) in the following ways:

- **Cross-cloud guest access** - You can share documents, sites, and teams with organizations that are in other Microsoft Azure cloud environments.
- **Cross-cloud meetings** - You can meet with people in other Microsoft Azure cloud environments with an authenticated meeting experience that doesn't require guest accounts.

Both options require that you enable connections to the other cloud environment and set up an organizational relationship with the specific organization with which you want to collaborate.

For information about setting up cross-cloud guest access, see [Collaborate with guests from other Microsoft 365 cloud environments](#).

For information about setting up cross-cloud meetings, see [Meet with people in other Microsoft 365 cloud environments](#).

Multitenant organizations

If your organization manages multiple Microsoft 365 tenants, you can set up a multitenant organization in Microsoft 365 to facilitate collaboration and resource access between tenants. Multitenant organizations synchronize users between tenants using Microsoft Entra B2B collaboration users. With the new Microsoft Teams desktop client, users can search for users in other tenants, receive real-time notifications from all the

tenants in the multitenant organization, and participate in chats, meetings, and calls across all of the tenants without needing to switch tenants.

For information about how to set up a multitenant organization, see [Plan for multitenant organizations in Microsoft 365](#) and [Set up a multitenant org in Microsoft 365](#).

Related articles

[Intro to file collaboration in Microsoft 365](#)

[File collaboration in SharePoint with Microsoft 365](#)

[Use guest access and external access to collaborate with people outside your organization](#)

[Limit organizations where users can have guest accounts](#)

[Control who can bypass the meeting lobby in Microsoft Teams](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Exchange Online

Article • 05/08/2024

Microsoft Exchange Online is a cloud based messaging platform that delivers email, calendar, contacts, and tasks. Users connect to Exchange Online using apps like Outlook, Outlook on the web, or Outlook mobile app to access email and collaboration functionality, including shared mailboxes, shared calendars and global address lists.

Exchange is included when you sign up for Microsoft 365 Business or Microsoft 365 for enterprise subscriptions. You can also buy standalone Exchange Online plans for your organization. For a full list of subscription options for Exchange, see the [Exchange Online service descriptions](#).

Manage Exchange Online

As an administrator for your organization, you manage Exchange using both the Microsoft 365 admin center and the Exchange admin center (EAC). Use the Microsoft 365 admin center for user, group, and resource management tasks. Use the EAC for more specific tasks related to Exchange line mail flow, migration, and mobile devices. Learn more at [Exchange admin center](#).

To access EAC:

1. [Sign in](#) to Microsoft 365 using your work or school account that has administrator rights.
2. In the Microsoft 365 admin center navigation, choose ...[Show all*](#) to see the full list.
3. Under Admin centers*, choose **Exchange**.

You can also access EAC directly at <https://admin.exchange.microsoft.com>.

EAC access requires the [Exchange administrator role](#). For more information about assigning administrator roles, see [Assign admin roles in the Microsoft 365 admin center](#).

Tip

When you assign someone to the Exchange administrator role, we recommend also assigning them to the Service Support administrator role. This way they can see important information in the Microsoft 365 admin center, such as the health of the Exchange service, as well as change and release notifications.

Introduction to SharePoint and OneDrive in Microsoft 365 for administrators

Article • 03/28/2024

SharePoint and OneDrive in Microsoft 365 are cloud-based services that help organizations share and manage content, knowledge, and applications to:

- Empower teamwork
- Quickly find information
- Seamlessly collaborate across the organization

The resources on this page are designed to get you started. Depending on the needs of your organization, you may want to read about [migration](#) and [governance](#) options before you start rolling SharePoint and OneDrive out to your users.

If you're ready to get started with SharePoint and OneDrive, read [Plan for SharePoint and OneDrive in Microsoft 365](#) and follow the planning and rollout articles that are listed in that article.

If you're just starting out with SharePoint and OneDrive, learn about the [FastTrack onboarding and adoption services](#), [find a SharePoint certified partner](#), or [visit the SharePoint community](#).

Once you're using SharePoint and OneDrive, get the [OneDrive sync app](#) and the [mobile app](#).

Migration

If you have files that you need to move to SharePoint and OneDrive, the resources in this section can help you get started.

[+] Expand table

If you're looking for this information:	Go to this resource:
Learn how to include migration as part of your plan to roll out SharePoint and OneDrive	Migration planning for SharePoint and OneDrive rollout
How to migrate content from file shares or other cloud providers using Migration Manager	Migrate your content to Microsoft 365

If you're looking for this information:	Go to this resource:
How to migrate SharePoint Server sites and content	Overview of the SharePoint Migration Tool (SPMT)

Governance

If your organization has legal or other requirements that govern the handling of data, or if you have sensitive or confidential information that you want to protect, these references can help you configure SharePoint for your governance standards and policies.

[Expand table](#)

If you're looking for this information:	Go to this resource:
How to plan your compliance requirements for SharePoint and OneDrive	Plan compliance requirements for SharePoint and OneDrive
How to ensure that you retain files for a specified period of time, or delete them on a specified schedule	Overview of retention policies OneDrive retention and deletion
How to classify documents based on the sensitivity of the information	Overview of sensitivity labels Enable sensitivity labels for Office files in SharePoint and OneDrive
How to prevent the loss or exfiltration of important data in documents emails	Learn data loss prevention
Search for in-place items such as email, documents, and instant messaging conversations	Content Search in Microsoft 365

If you use OneDrive in your organization and you want to protect important files by saving them to the cloud, govern how much storage space users get, or govern how users sync file, these references will help you configure your policies.

[Expand table](#)

If you're looking for this information:	Go to this resource:
Protect important files on users' desktops or in their Documents folder	Redirect and move Windows known folders to OneDrive and Redirect and move macOS Desktop and Documents folders to OneDrive

If you're looking for this information:	Go to this resource:
Control how users sync files to their devices	Use Group Policy to control OneDrive sync settings and Deploy and configure the OneDrive sync app for Mac
Configure the amount of storage space users have in OneDrive	Set the default storage space for OneDrive users

Microsoft Teams

SharePoint is deeply integrated into Teams. Files that are stored in Teams are stored in SharePoint sites. When you administer SharePoint sites in the SharePoint admin center, you may find that many of them are connected to teams. Use these resources to understand how SharePoint and Teams are integrated.

[\[\] Expand table](#)

If you're looking for this information:	Go to this resource:
Learn about how Teams and SharePoint work together	Overview of Teams and SharePoint integration
Learn how to manage settings and permissions when Teams and SharePoint are integrated together	Manage settings and permissions when SharePoint and Teams are integrated

Collaboration

SharePoint and OneDrive provide a rich collaboration environment where people inside and outside your organization can work together, coauthoring documents. Microsoft 365 provides a variety of options to help you create a secure and productive file collaboration environment that meets the needs of your organization. Use these resources to get started.

[\[\] Expand table](#)

If you're looking for this information:	Go to this resource:
Learn about secure collaboration in Microsoft 365	Set up secure collaboration with Microsoft 365
Learn about file collaboration and how to plan your implementation	Intro to file collaboration in Microsoft 365

If you're looking for this information:	Go to this resource:
	File collaboration in SharePoint with Microsoft 365
Learn about collaborating with people outside your organization	External sharing overview Collaborate with guests
Use the security and compliance features in Microsoft 365 to help secure your guest sharing environment	Create a secure guest sharing environment

Modern intranet

SharePoint provides a rich set of tools to help you create and maintain your organization's intranet. Use these resources to get started.

[] [Expand table](#)

If you're looking for this information:	Go to this resource:
Learn about the different types of SharePoint sites	Plan your SharePoint site ↗
Select whether to allow users to create their own sites	Manage site creation
Learn how to plan an intelligent intranet for your organization	Plan an intelligent SharePoint intranet
	Planning your SharePoint hub sites

Training

Administrators are often called upon to teach others in the organization how to use new technologies. Use these resources to help your users be successful with SharePoint and OneDrive.

[] [Expand table](#)

If you're looking for this information:	Go to this resource:
Get a list of training resources for your users	Training and change management for rolling out SharePoint and OneDrive
Set up a customizable training portal with Microsoft training content for your organization	Microsoft 365 learning pathways

If you're looking for this information:	Go to this resource:
Show your users the basics of SharePoint	SharePoint help & learning
Show your users the basics of OneDrive	OneDrive help & learning

Customization

SharePoint provides a wide range of options for customization. We recommend using the out-of-box features and functionality as much as possible to meet your organization's needs. If you do need to customize SharePoint, see these references.

[Expand table](#)

If you're looking for this information:	Go to this resource:
Understand how to customize SharePoint using modern tools and techniques	Customizing SharePoint
Build SharePoint Framework solutions, apps, add-ins, and solutions	SharePoint development

Related topics

[SharePoint Limits](#)

[Getting started with the SharePoint Online Management Shell](#)

[Microsoft Partner Center](#)

[Tips and tricks for navigating Microsoft 365 technical documentation](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Introduction to Microsoft Teams for admins

Article • 05/16/2024 • Applies to: Microsoft Teams

If you're the admin for Microsoft Teams in your organization, you're in the right place. When you're ready to get going with Teams, start with [How to roll out Teams](#) and [Set up secure collaboration with Microsoft 365 and Microsoft Teams](#).

Don't miss our Welcome to Teams for the Teams admin video (just over 3 minutes):
<https://www.microsoft.com/en-us/videoplayer/embed/RE47cdp?postJslIMsg=true>

If you're looking for end user Teams Help, click **Help** on the left side of the app, or go to the [Microsoft Teams help center](#). For training, go to [Microsoft Teams Training](#).

ⓘ Important

For details about Teams feature availability and licensing, see [Teams add-on licensing options](#).

Teams architecture

Teams is built on Microsoft 365 groups, Microsoft Graph, and the same enterprise-level security, compliance, and manageability as the rest of Microsoft 365. Teams leverages identities stored in Microsoft Entra ID.

When you create a team, here's what gets created:

- A new [Microsoft 365 group](#)
- A [SharePoint](#) site and document library to store team files
- An [Exchange Online](#) shared mailbox and calendar
- A OneNote notebook
- Ties into other Microsoft 365 apps such as Planner and Power BI

When you create a team from an existing group, that group's membership, site, mailbox, and notebook are surfaced in Teams.

To customize and extend Teams, add third-party apps using [app management tasks](#). With Teams, you can include people from outside your organization by adding them as a guest or an external user, depending on [what you need](#). Teams offers a robust

development platform so you can build the teamwork hub you need for your organization.

💡 Tip

For a deep dive into Teams architecture, watch the videos on the [Teams Platform Academy](#).

Managing Teams

As the admin, you'll manage Teams through the Teams admin center. For a quick orientation, watch the Manage Teams using the Teams admin center video (3:03 min): <https://www.microsoft.com/en-us/videoplayer/embed/RE476Yi?postJs||Msg=true>

To learn more:

- [Use Teams admin roles to manage Teams](#)
- [Manage Teams in the Teams admin center](#)
- [Manage Teams features in your Microsoft 365](#)

To stay on top of what's coming for Teams and all other Microsoft 365 products and services in your organization, be sure to check [Message center](#) and the [Teams roadmap](#). You'll get announcements about new and updated features, planned changes, and issues to help keep you informed and prepared.

Teamwork

Every team is different; there's no one-size-fits-all approach to collaboration. When deciding which apps and services to use, think about the work your organization does and the types of conversations your teams need to have:

- **Teams**, as the hub for teamwork, is where people--including people outside your organization--can actively connect and collaborate in real time to get things done. Have a conversation right where the work is happening, whether coauthoring a document, having a meeting, or working together in other apps and services. Teams is the place to have informal chats, iterate quickly on a project, work with team files, and collaborate on shared deliverables.
- **Outlook** for collaborating in the familiar environment of email and in a more formal, structured manner or when targeted and direct communication is required.

- **SharePoint** for sites, portals, intelligent content services, business process automation, and enterprise search. SharePoint keeps content at the center of teamwork, making all types of content easily shareable and accessible across teams. Tight integration with Outlook, Viva Engage, and Teams enables seamless content collaboration across conversation experiences.
- **OneDrive** for storing files and sharing them with people that a user invites. Content that a user saves to OneDrive is private until the user shares it with others, making it the best option for storing personal and draft documents that are not intended to be shared or not ready to be shared.
- **Viva Engage** to connect people across the organization. Drive company-wide initiatives, share best practices, and build communities around common topics of interest or areas of practice. Crowdsource ideas to foster open discussions with people across the company.
- **Office apps** are all the familiar tools that people know and use regularly, including Word, Excel, PowerPoint, and OneNote.

Related topics

[Teams Troubleshooting](#)

[What's new in Teams ↗](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Overview of meetings, webinars, and town halls

Article • 12/18/2023 • Applies to: Microsoft Teams

APPLIES TO: ✓ Meetings ✓ Webinars ✓ Town halls

There are multiple ways to meet in Microsoft Teams:

- Meetings
- Webinars
- Town halls

This article, intended for administrators and IT professionals, describes the differences between meetings, webinars, and town halls. You can use this information as a first step in planning for these types of virtual meetings and events.

The sections below include further information for planning and configuring these features, as well as links to information for your end users.

The following table shows the main features that are different between meetings, webinars, and town halls. You can use this information to help determine which is best for the use cases in your organization. For a detailed look at the features available in each, see [Meetings, webinars, and town halls feature comparison](#).

[] Expand table

Feature	Meetings	Webinars	Town halls
Lobby	✓	✓	✗
Attendee mic and camera	✓	✓	✗
End-to-end encryption	Premium	✗	✗
Watermarks	Premium	✗	✗
Theme	Premium	✓	✓
Registration	✗	✓	✗
Breakout rooms	✓	✗ ²	✗
Content sharing and interaction	✓	✓	Q&A only

Feature	Meetings	Webinars	Town halls
Interactive participants	1,000 (Enterprise plans) 300 (Business plans)	1,000	Town halls: 10,000 Premium town halls: 20,000
View-only participants	10,000 ¹ (Enterprise plans only)	✖	✖
Maximum total participants	11,000 ¹ (Enterprise plans only)	1,000	Town halls: 10,000 Premium town halls: 20,000

¹The usual 10,000 is increased to 20,000 through June 30, 2024. The maximum total participants for meetings is the sum of the interactive participants plus streaming participants.

² Breakout rooms can be used if a webinar has fewer than 300 participants. However, if the number of participants increases to above 300, breakout rooms aren't supported.

For more information on limits and specifications for Teams webinars, meetings, and town halls, see [Limits and specifications for Microsoft Teams](#).

Manage who can create meetings, webinars, and town halls

You can manage which of your users can create meetings, webinars, and town halls by using meeting and event policies. For example, you might want to allow all your users to create meetings, but only people in marketing to create webinars, and only executives to create town halls. Anyone invited can attend these types of meetings, but only those you specify can create them.

For details, see:

- [Manage who can start instant meetings and schedule meetings](#)
- [Manage who can schedule webinars](#)
- [Manage who can schedule town halls](#)

Meetings

Meetings in Teams include audio, video, and screen sharing for up to 1,000 people and a view-only streaming experience for participants over 1,000. Participants don't need to be a member of an organization (or have a Teams account) to join a Teams meeting. They

can join directly from the calendar invitation via the Join meeting link or call in via audio if available.

In addition to regularly scheduled meetings, your users can create channel meetings. With channel meetings, everybody in a team can see there's a meeting, join the meeting, and use the meeting chat.

Meetings are generally best for situations where participants need to interact with each other via voice or chat and where multiple people may be presenting.

For detailed information on how to plan for Teams meetings in your organization, see [Plan for Teams meetings](#).

Key training for end users

The following table lists meetings training available to the end users in your organization:

[] [Expand table](#)

Training	Description
Join a Teams meeting	A quick training video for users who are new to Teams meetings.
Schedule a meeting in Microsoft Teams	Article that describes how to schedule different types of meetings.
Participant settings in Microsoft Teams meetings	Article about managing meeting options.

Webinars

Webinars are structured meetings where presenters and participants have clear roles. A key difference between webinars and Teams meetings is that webinars support robust registration management, a customizable event and registration site, and event-oriented default meeting options.

Teams Premium offers additional webinar functionality through the Teams Premium subscription. The breakdown of features is highlighted in the following table:

[] [Expand table](#)

Feature name	Webinar features	Premium webinar features
Allow registered users to bypass the lobby	✓	✓
Assign a co-organizer	✓	✓
Limit the number of people who can register	✓	✓
Require attendees to register	✓	✓
Set up a green room for webinar presenters	✓	✓
Turn on Q&A for webinars with up to 1,000 attendees	✓	✓
View attendance reports	✓	✓
External presenters	✓	✓
Create a webinar wait list		✓
Limit the day and time when people can register		✓
Manage attendees' view		✓
Manually approve registrants		✓
Send reminder emails to registrants		✓
Use RTMP-In for webinars		✓

To learn more about advanced webinar features, see [Microsoft Teams Premium licensing](#).

For detailed information on how to plan for Teams webinars in your organization, see [Plan for Teams webinars](#).

Key training for end users

The following table lists webinars training available to the end users in your organization:

[Expand table](#)

Training	Description
Get started with Teams webinars	A quick training video for users who are new to Teams webinars.

Training	Description
Visual quick start guide ↗	A downloadable visual guide that describes how to start scheduling webinars.

Town halls

Town halls are generally best for situations where a limited number of presenters are presenting to a large group of attendees and direct interaction via chat or voice conversation isn't needed. For these event formats, attendees don't use their cameras and mics, but instead use Q&A to engage with presenters and organizers.

For detailed information on how to plan for Teams town halls, see [Plan for Teams town halls](#).

Teams Premium offers additional town hall functionality through the Teams Premium subscription. The breakdown of features is highlighted in the following table:

[\[+\] Expand table](#)

Capability	Town halls	Premium town halls
Broadcast capacity	10k	20k
Attendee reporting	✓	✓
eCDN	3rd and 1st party	1st party
Duration	30 hours	30 hours
RTMP-in	✓	✓
Producer UX	Manage what attendees see	Manage what attendees see
Default audio and video off	✓	✓
Layouts	Focused curated view	Focused curated view
Green room	✓	✓
External presenters	✓	✓
External presenters capacity	20	20
Presenter capacity (including external presenters)	100	100

Capability	Town halls	Premium town halls
Co-organizer capacity	10	10
Manage what attendees see	✓	✓
AI generated captions	✓	✓
Q&A capacity	10k	20k
VOD	✓	✓
Organizer level real time monitoring	✗	✓
Essential emails	✓	✓
Email editing	✗	✓

Best practices for large meetings and events

This section provides guidance for admins, along with tips that admins can share with their presenters and organizers.

To run a successful event, follow the practices outlined below:

- For the best experience in large meetings, webinars, and town halls, Microsoft recommends using the latest version of the Teams desktop client or Teams mobile clients.
- Ensure that all Microsoft [Network Connectivity Principles](#) have been followed both on-premises and for remote users. The network connectivity principles apply to meetings, webinars, and town halls.
- Use [real-time data telemetry](#) to monitor the event and identify any possible issues and its source.
 - Designate meeting monitors to [analyze](#) telemetry for users facing poor experience caused by metrics exceeding thresholds.
 - Set meeting monitors as presenters to disable rogue video streams, mute accidental live mics, and remove attendees if needed.

Related topics

[Meetings and conferencing in Teams](#)

[Use NDI® technology in Microsoft Teams](#)

Feedback

Was this page helpful?

 Yes

 No

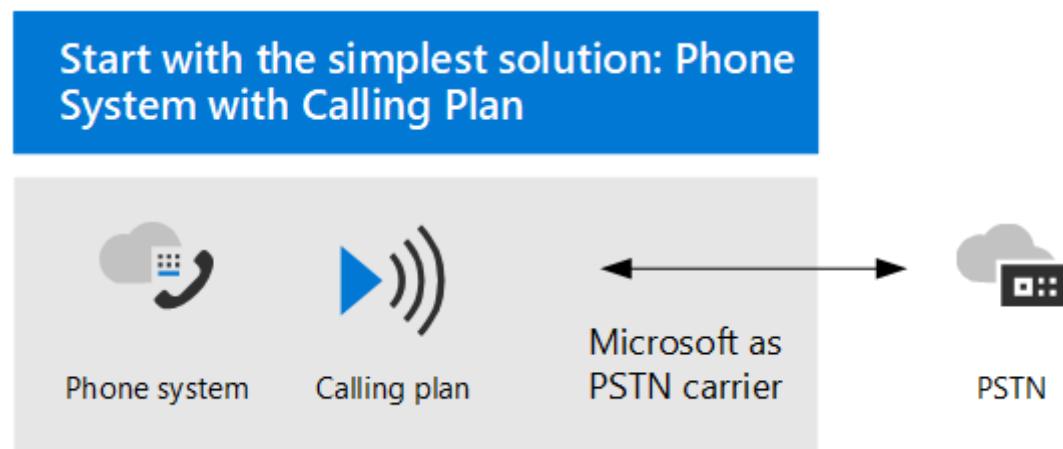
[Provide product feedback ↗](#)

Plan your Teams voice solution

Article • 08/03/2023 • Applies to: Microsoft Teams

This article helps you decide which Microsoft voice solution is right for your organization. After you've decided, the article provides a roadmap to content that will enable you to implement your chosen solution.

You might want the simplest solution—Microsoft Teams Phone with Calling Plan. This option is Microsoft's all-in-the-cloud solution that provides Private Branch Exchange (PBX) functionality and calls to the Public Switched Telephone Network (PSTN), as shown in the following diagram. With this solution, Microsoft is your PSTN carrier.



If you answer yes to the following, then Teams Phone with Calling Plan is the right solution for you:

- Calling Plan is available in your region.
- You don't need to retain your current PSTN carrier.
- You want to use Microsoft-managed access to the PSTN.

If you're a small to medium business (300 or fewer people), Microsoft now bundles Teams Phone with a Domestic Calling Plan.

However, your situation might be more complex. For example, you might have offices in locations where Calling Plan isn't available. Or you might need a combination solution that supports a complex, multi-national deployment, with different requirements for different geographic locations. Microsoft supports a combination of solutions:

- Teams Phone with Calling Plan
- Teams Phone with your own PSTN carrier with Operator Connect
- Teams Phone with your own PSTN mobile carrier with Teams Phone Mobile
- Teams Phone with your own PSTN carrier with Direct Routing

- A combination solution that uses Teams Phone with Calling Plan, Teams Phone with Operator Connect, and/or Teams Phone with Direct Routing

For a visual summary of all the voice solution options, see the voice solutions poster.



[PDF](#)

[Visio](#)

If you're interested in PSTN conferencing for meetings, you'll want to read about Microsoft's Audio Conferencing service and licensing requirements. Note that Audio Conferencing does not require a Teams Phone license. For more information, see [Audio Conferencing](#).

What do you need to read?

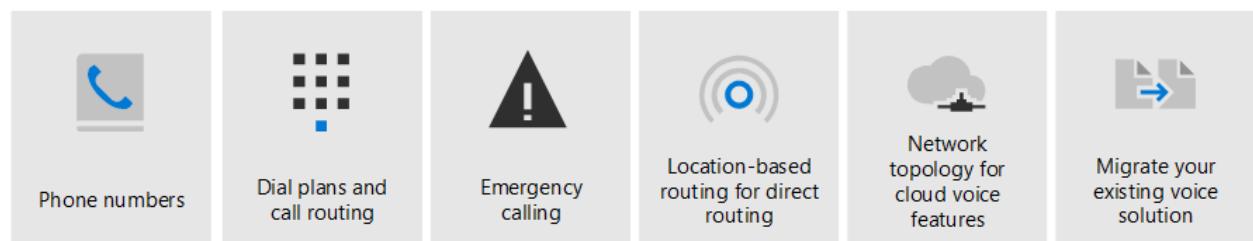
Required for all. Some of the sections in this article pertain to all organizations. For example, everyone should read about Teams Phone and understand the options for connecting to the Public Switched Telephone Network (PSTN).

Required for all	Description
Teams Phone	Microsoft's technology for enabling call control and Private Branch Exchange (PBX) capabilities in the Microsoft 365 cloud with Microsoft Teams.
Public Switched Telephone Network (PSTN) connectivity options	Choose Microsoft as your telephony carrier or connect your own telephony carrier to Microsoft Teams by using Operator Connect or Direct Routing. Combined with Teams Phone, PSTN connectivity options enable your users to make phone calls all over the world.

Depending on your requirements. Some of the sections in this and related articles are pertinent depending on your existing deployment and requirements. For example, Location-Based Routing is only required for Direct Routing customers in geographic locations that do not allow toll bypass.

Consider which of these other configurations you might need:

Consider whether you also need:



Depending on your requirements	Description
Phone number management	How to get and manage phone numbers differs depending on your PSTN connectivity option. Read this section if you need to obtain phone numbers, transfer existing numbers, obtain service numbers, and so on.
Call routing and dial plans	How to configure and manage dial plans that translate dialed phone numbers into an alternate format (typically E.164 format) for call authorization and call routing. Read this section if you need to understand what dial plans are and whether you need to specify dial plans for your organization.
Emergency calling	How to manage and configure emergency calling differs depending on your PSTN connectivity option. Read this section if you need to understand how to manage emergency calling for your organization.
Location-Based Routing for Direct Routing	How to use Location-Based Routing (LBR) to restrict toll bypass for Microsoft Teams users based on their geographic location. Read this section if your organization is using Direct Routing at a location that doesn't allow toll bypass.
Network topology for cloud voice features	If your organization is deploying Location-Based Routing (LBR) for Direct Routing or dynamic emergency calling, you must configure network settings for these features in Microsoft Teams. Read this section if you're implementing LBR for Direct Routing, or if you're implementing dynamic emergency calling with Calling Plan or Direct Routing.
Migrate your existing voice solution	What you need to think about when migrating your voice solution to Teams. Read this section if you're migrating from an existing voice solution to Teams.

Teams Phone

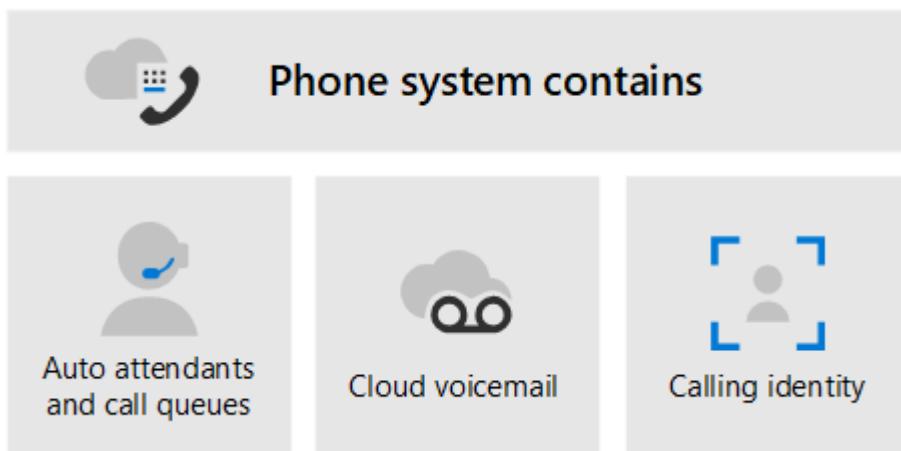
Teams Phone is Microsoft's technology for enabling call control and Private Branch Exchange (PBX) capabilities in the Microsoft 365 cloud with Microsoft Teams.

Teams Phone works with Teams clients and certified devices. Teams Phone allows you to replace your existing PBX system with a set of features directly delivered from Microsoft 365.

Calls between users in your organization--regardless of geographical area--are handled internally within Teams Phone. These internal calls never go to the Public Switched Telephone Network (PSTN), so your company avoids long-distance charges.

This article introduces the following Teams Phone key features and functionality, and the deployment decisions you'll need to consider:

- [Auto attendants and Call queues](#)
- [Cloud Voicemail](#)
- [Calling identity](#)



For information about all Teams Phone features, and how to set up Teams Phone, see the following articles:

- [Teams Phone features](#)
- [Set up Teams Phone in your organization](#)

Describes how to buy and assign Teams Phone licenses, manage phone numbers, and set up communication credits for toll-free numbers.

For information about managing supported devices, see [Manage your devices in Microsoft Teams](#) and [Teams Marketplace](#).

Auto attendants and Call queues

Auto attendants allow you to set up menu options to route calls based on caller input. Call queues are waiting areas for callers. Used together, Auto attendants and Call queues can easily route callers to the appropriate person or department in your organization.

For information about Auto attendants and Call queues, see the following articles:

- [Plan for Teams Auto attendants and Call queues](#)
- [Set up an Auto attendant](#)
- [Create a Call queue](#)
- [Contoso case study: Auto attendants and Call queues](#)

Describes how a fictional multi-national corporation, Contoso, implemented Auto attendants and Call queues for their voice solution.

Cloud Voicemail

Cloud Voicemail, powered by Azure Voicemail services, supports voicemail deposits to Exchange mailboxes only. It doesn't support third-party email systems.

Cloud Voicemail includes voicemail transcription, which is enabled for all users in your organization by default. Your business needs might require that you disable voicemail transcription for specific users or everyone throughout the organization.

Cloud Voicemail is automatically set up and provisioned for Teams users.

For more information about Cloud Voicemail and its configuration, see the following articles:

- [Set up Cloud Voicemail](#)
- [Manage voicemail policies](#)

Calling identity

By default, all outbound calls use the assigned phone number as calling identity (caller ID). The recipient of the call can quickly identify the caller and decide whether to accept or reject the call. For information about configuring caller ID or to change or block the caller ID, see [Manage caller ID policies for users](#).

Public Switched Telephone Network connectivity options

Teams Phone provides complete PBX capabilities for your organization. However, to enable users to make calls outside your organization, you need to connect Teams Phone to the Public Switched Telephone Network (PSTN). To connect Teams Phone to the PSTN, you can choose one of the following options:

- **Teams Phone with Calling Plan.** An all-in-the-cloud solution with Microsoft as your PSTN carrier.
- **Teams Phone with your own PSTN carrier by using Operator Connect.** With Operator Connect, if your existing operator participates in the Microsoft Operator Connect program, they can manage the service for bringing PSTN calling to Teams.
- **Teams Phone with your own PSTN mobile carrier by using Teams Phone Mobile.** With Teams Phone Mobile, if your existing operator participates in the Microsoft Teams Phone Mobile program, they can manage the service for using SIM-enabled mobile phone numbers with Teams.
- **Teams Phone with your own PSTN carrier by using Direct Routing** to connect your on-premises environment to Teams.

You can choose a combination of options, which enables you to design a solution for a complex environment, or manage a multi-step migration. You'll read more about migration later.

Most Teams Phone features are the same regardless of the PSTN connectivity option you choose. There are some differences in functionality, however, that affect how you configure certain Teams Phone features, such as call routing and emergency calling. For more information about PSTN connectivity options and configuration considerations, see [PSTN connectivity options](#).

Migrate your existing voice solution to Teams

For an organization that is upgrading to Teams, the ultimate goal is to move all users to TeamsOnly mode. Using Teams Phone is only supported when the user is in TeamsOnly mode. If you need basic information about upgrading to Teams, start here:

- [Getting started with your Microsoft Teams upgrade](#)
- [About the upgrade framework](#)
- [Upgrade strategies for IT administrators](#)

For guidance on planning a Teams voice solution as part as your overall plan to upgrade to Teams, see [PSTN considerations for upgrading to Teams from Skype for Business on-premises](#).

For more information about how to implement your voice migration, see the [Contoso voice migration case study](#). The case study describes how a fictional multi-national corporation, Contoso, implemented a Teams voice solution for their organization.

Activate rights management in the admin center

Article • 09/29/2022

You must activate the Rights Management service (RMS) before you can use the Information Rights Management (IRM) features of Microsoft 365 applications and services. After you activate RMS, your organization can start to protect important documents and emails by using Azure RMS. This information protection solution can protect all file types and integrates with client applications like Excel, Microsoft Word, and others, Exchange Online and SharePoint Online, and servers such as Microsoft Exchange and Microsoft SharePoint.

Tip

If you're not sure whether you need Rights Management, check whether your organization has one or more of **these business problems or requirements**.

Use these links for more information about RMS:

- To learn more about RMS, see [What is Azure Rights Management](#).
- If you're new to RMS, see [Overview of Azure Rights Management](#).
- For an overview of the deployment steps see the [Azure Rights Management deployment road map](#).
- For instructions about activating RMS for Microsoft 365, see [Activating the protection service from Azure Information Protection](#).

Microsoft 365 Business Premium

Article • 10/06/2023

Check out [Microsoft 365 small business help](#) on YouTube.

Watch: What is Microsoft 365 Business Premium?

Check out this video and others on our [YouTube channel](#).

<https://www.microsoft.com/en-us/videoplayer/embed/RE2mhaA?autoplay=false&postJsIMsg=true>

Microsoft 365 Business Premium is a subscription service that lets you run your organization in the cloud while Microsoft takes care of the IT for you, managing devices, protecting against real-world threats, and providing your organization with the latest in business software.

When you sign up for Microsoft 365 Business Premium, you get all the same productivity tools you get with Microsoft 365 Business Standard, and the following security features:

Safeguard your data

Feature	Description
Protect against threats	<p>Microsoft 365 Business Premium helps protect you against threats with advanced threat protection capabilities. These capabilities include safe attachments and safe links protection.</p> <p>Check out Overview of Microsoft Defender for Business (preview!) for additional security and threat protection capabilities.</p>
Secure business data	Your personal data is protected on personal devices with PIN access, and restricted copy and saving. You can also add information protection to make sure that only authorized people can access sensitive information.
Secure your devices	You can protect your work files on devices by restricting mobile access, such as copy and paste. You can also selectively wipe business data from enrolled mobile devices if they are lost or stolen.
Additional security features	Advanced features in Microsoft 365 Business Premium are available to help you protect your business against cyber-threats and safeguard sensitive information. The capabilities include Microsoft Defender for Office 365 Plan 1, Microsoft

Feature	Description
	Purview Data Loss Prevention policies (DLP), Exchange Online archiving, Azure Information Protection, and Intune.

If you have Microsoft Business Premium, the quickest way to setup security and begin collaborating safely is to follow the guidance in this library: [Microsoft 365 Business Premium – productivity and cybersecurity for small business](#). This guidance was developed in partnership with the Microsoft Defending Democracy team to protect all small business customers against cyber threats launched by sophisticated hackers.

For full details, see [Microsoft 365 Business content](#).

How to check Microsoft 365 service health

Article • 06/27/2024



The Admin Center is changing. If your experience doesn't match the details in this article, check out <https://aka.ms/aboutM365preview>.

You can view the health of your Microsoft services, including Office on the web, Microsoft Teams, Exchange Online, and Microsoft Dynamics 365 on the **Service health** page in the [Microsoft 365 admin center](#). If you're experiencing problems with a cloud service, you can check the service health to determine whether this is a known issue with a resolution in progress before you call support or spend time troubleshooting.

If you're unable to sign in to the admin center, you can use the [service status page](#) to check for known issues preventing you from logging into your tenant. Also, sign up to follow us at [@MSFT365status](#) on X (Twitter) to see information on certain events.

How to check service health

1. Go to the Microsoft 365 admin center at <https://admin.microsoft.com>, and sign in with an admin account.

Note

People who are assigned the Service Support admin and Helpdesk admin role can view service health. For more information about roles that can view service health, see [About admin roles](#).

2. To view service health, in the left-hand navigation of the admin center, go to **Health > Service health**, or select the **Service health** card on the **Home dashboard**. The dashboard card indicates whether there's an active service issue and links to the detailed **Service health** page.
3. On the **Service health** page, the health state of each cloud service is shown in a table format.

The screenshot shows the Microsoft 365 admin center Service health page. The Overview tab is selected. In the 'Issues for your organization to act on' section, there is one item: 'Reminder to authenticate outbound email with SPF, DKIM, and DMARC'. In the 'Active issues Microsoft is working on' section, there are four entries related to Microsoft Teams:

Issue title	Issue type	Affected service	Updated	ID
Guest users are unable to post messages in Microsoft Teams channels via all connection methods	Advisory	Microsoft Teams	September 25, 2023 at 2:19 PM...	TM676394
Anonymous users can't view or edit Microsoft Whiteboards in Microsoft Teams meetings via all connection methods	Advisory	Microsoft Teams	September 21, 2023 at 5:25 PM...	TM675793
Users may be unable to download multiple files at once when downloading from the Files tab of Microsoft Teams channels	Advisory	Microsoft Teams	September 22, 2023 at 12:52 P...	TM675794
Users may be unable to access Call Group Forwarding settings in Microsoft Teams (Preview)	Advisory	Microsoft Teams	September 14, 2023 at 4:19 PM...	TM671750

The **Overview** tab (the default view) shows all services, their current health state, and any active incidents or advisories. An icon and status in the **Health** column indicate the state of each service.

The **Issues for your organization to act on** section lists any issues detected in your environment that require your action. If there are no issues in your environment that need action, this section won't be visible.

The **Active issues Microsoft is working on** section lists active incidents and advisories that Microsoft is working to resolve.

The **Issue history** tab shows all incidents and advisories that have been resolved within the last 7 or 30 days.

If you're experiencing an issue with a Microsoft 365 service and you don't see it listed on the Service health page, tell us about it by selecting **Report an issue**, and completing the short form. We'll look at related data and reports from other organizations to see how widespread the issue is, and if it originated with our service. If it did, we'll add it as a new incident or advisory on the **Service health** page, where you can track its resolution. The **Reported issues** tab will show all issues your tenant has reported from this form and the status.

To customize your view of which services show up on the dashboard, select **Customize > Custom view**, and clear the checkboxes for the services you want to filter out of your Service health dashboard view. Make sure that the checkbox is selected for each service that you want to monitor.

To sign up for email notifications of new incidents that affect your tenant and status changes for an active incident, select **Customize > Email**, select **Send me email notifications about service health**, and then specify:

- Up to two email addresses.
- Whether you want notifications for incidents or advisories
- The services for which you want notification

You can also subscribe to email notifications for individual events instead of every event for a service. To do so, select the active issue you want to receive email notification updates for, select **Manage notifications for this issue**, and then specify:

- Up to two email addresses.

Note

Each admin can have their Preferences set and the above limit of two email address is per admin account.

Tip

You can also use the [Microsoft 365 Admin app](#)  on your mobile device to view Service health, which is a great way to stay current with push notifications.

View details of posted service health issue

In the **Active issues Microsoft is working on** section, select the issue title to see the issue detail page. This page shows more information about the issue, including a feed of all the messages posted while we work on a solution.

Active issues Microsoft is working on					
Issue title	Issue type	Affected service	Updated	ID	
Guest users are unable to post messages in Microsoft Teams channels via all connection methods	Advisory	Microsoft Teams	September 25, 2023 at 2:19 PM...	TM676394	
Anonymous users can't view or edit Microsoft Whiteboards in Microsoft Teams meetings via all connection methods	Advisory	Microsoft Teams	September 21, 2023 at 5:23 PM...	TM675793	
Users may be unable to download multiple files at once when downloading from the Files tab of Microsoft Teams channels	Advisory	Microsoft Teams	September 22, 2023 at 12:52 P...	TM674593	
Users may be unable to access Call Group Forwarding settings in Microsoft Teams (Preview)	Advisory	Microsoft Teams	September 14, 2023 at 4:19 PM...	TM671750	
Users may be unable to use Microsoft Teams accounts on any Microsoft Teams certified Android devices	Advisory	Microsoft Teams	September 25, 2023 at 3:52 PM...	TM670039	
Users may see delays syncing any change from Microsoft Entra ID to multiple Microsoft 365 services	Advisory	Microsoft 365 suite, Microsoft T...	September 26, 2023 at 8:41 AM...	MO677321	
Admins may experience delays when attempting to access Group Activity and Microsoft Teams Team reports	Advisory	Microsoft 365 suite	September 24, 2023 at 10:28 P...	TM677022	
Admins' Microsoft 365 Defender portal Advanced Hunting may not show some updated values in two columns for EmailEvents	Advisory	Microsoft 365 Defender	September 25, 2023 at 9:23 AM...	DZ670339	

The advisory or incident summary provides the following information:

- **Title** - A summary of the problem.
- **ID** - A numeric identifier for the problem.
- **Last updated** - The last time that the service health message was updated.
- **Estimated start time** - The estimated time when the issue started.
- **Affected services** - The names of the affected services.
- **Issue type** - The severity of the issue (incident or advisory).
- **Issue origin** - An indication of whether the issue was found at Microsoft or in your environment.
- **Status** - The current state of the issue.
- **User Impact** - A brief description of the impact this issue has on the end user.
- **All Updates** - We post frequent messages to let you know the progress that we're making in applying a solution.

The screenshot shows the Microsoft 365 admin center interface. The left sidebar is collapsed, and the main content area is titled "Service health". Below the title, there are three navigation links: "Overview", "Issue history", and "Reported issues". A sub-header states: "View the issues and health status of all services that are available with your current subscriptions. Learn more about Service Health". There are two buttons at the bottom of this section: "Report an issue" and "Customize".

Active issues Microsoft is working on:

Issue title	Issue type	Affected service
Guest users are unable to post messages in Microsoft Teams channels via all connection methods	Advisory	Microsoft Teams
Anonymous users can't view or edit Microsoft Whiteboards in Microsoft Teams meetings via all connection methods	Advisory	Microsoft Teams
Users may be unable to download multiple files at once when downloading from the Files tab of Microsoft Teams channels	Advisory	Microsoft Teams
Users may be unable to access Call Group Forwarding settings in Microsoft Teams (Preview)	Advisory	Microsoft Teams
Users may be unable to use Microsoft Teams accounts on any Microsoft Teams certified Android devices	Advisory	Microsoft Teams
Users may see delays syncing any change from Microsoft Entra ID to multiple Microsoft 365 services	Advisory	Microsoft 365
Admins may experience delays when attempting to access Group Activity and Microsoft Teams Team reports	Advisory	Microsoft 365
Admins' Microsoft 365 Defender portal Advanced Hunting may not show some updated values in two columns for EmailEvents	Advisory	Microsoft 365

Service status:

Service	Status
Service	Status

Guest users are unable to post messages in Microsoft Teams channels via all connection methods

TM676394. Last updated: September 25, 2023 at 2:19 PM MDT
Estimated start time: September 22, 2023 at 2:47 AM MDT

Affected services: Microsoft Teams

Issue type: Advisory
Issue origin: Microsoft

Status: Service degradation
Manage notifications for this issue

User Impact: Guest users are unable to post messages in Microsoft Teams channels via all connection methods.

Are you experiencing this issue?
Is this post helpful?

All updates:

September 25, 2023 at 2:19 PM MDT

Title: Guest users are unable to post messages in Microsoft Teams channels via all connection methods

User impact: Guest users are unable to post messages in Microsoft Teams channels via all connection methods.

Current status: We're continuing to develop a code fix to resolve the underlying issue, and anticipate we'll be able to confirm a timeline for its deployment by our next scheduled communications update.

Scope of impact: Your organization is affected by this event, and the problem

Translate service health details

We use machine translation to automatically display messages in your preferred language. Read [Language translation for the Service health page](#) for more information on how to set your language.

Definitions

Most of the time, services will appear as healthy with no further information. When a service is having a problem, the issue is identified as either an advisory or an incident and shows a current status.

Tip

Planned maintenance events aren't shown in service health. You can track planned maintenance events by staying up to date with the **Message center**. Filter to messages categorized as Plan for change to find out when the change is going to happen, its effect, and how to prepare for it. See [Message center in Microsoft 365](#) for more details.

Incidents and advisories

[\[+\] Expand table](#)

Icon	Description
	If a service has an advisory shown, we're aware of a problem that is affecting some users, but the service is still available. In an advisory, there's often a workaround to the problem and the problem might be intermittent or is limited in scope and user impact.
	If a service has an active incident shown, it's a critical issue and the service or a major function of the service is unavailable. For example, users might be unable to send and receive email or unable to sign-in. Incidents will have noticeable impact to users. When there's an incident in progress, we'll provide updates regarding the investigation, mitigation efforts, and confirmation of resolution in the Service health dashboard.

Status definitions

[\[+\] Expand table](#)

Status	Definition
Investigating	We're aware of a potential issue and are gathering more information about what's going on and the scope of impact.
Service degradation	We've confirmed that there's an issue that might affect use of a service or feature. You might see this status if a service is performing more slowly than usual, there are intermittent interruptions, or if a feature isn't working, for example.
Service interruption	You'll see this status if we determine that an issue affects the ability for users to access the service. In this case, the issue is significant and can be reproduced consistently.
Restoring service	The cause of the issue has been identified, we know what corrective action to take, and are in the process of bringing the service back to a healthy state.
Extended recovery	This status indicates that corrective action is in progress to restore service to most users but will take some time to reach all the affected systems. You

Status	Definition
	might also see this status if we've made a temporary fix to reduce impact while we wait to apply a permanent fix.
Investigation suspended	If our detailed investigation of a potential issue results in a request for additional information from customers to allow us to investigate further, you'll see this status. If we need you to act, we'll let you know what data or logs we need.
Service restored	We've confirmed that corrective action has resolved the underlying problem and the service has been restored to a healthy state. To find out what went wrong, view the issue details.
False positive	After a detailed investigation, we've confirmed the service is healthy and operating as designed. No impact to the service was observed or the cause of the incident originated outside of the service. Incidents and advisories with this status appear in the history view until they expire (after the period of time stated in the final post for that event).
Post-incident report published	We've published a Post Incident Report for a specific issue that includes root cause information and next steps to ensure a similar issue doesn't reoccur.

Message Post Types

[] Expand table

Type	Definition
Quick Update	Short and frequent incremental updates for broadly impacting incidents, available to all customers.
Additional Details	These additional posts will provide richer technical and resolution details to offer deeper visibility into the handling of incidents. This is available for tenants that meet the same requirements outlined for Exchange Online monitoring ,

History

Service health lets you look at your current health status and view the history of any service advisories and incidents that have affected your tenant in the past 30 days. To view the past health of all services, select **History** view.

For more information about our commitment to uptime, see [Transparent operations from Microsoft 365](#).

Language translation for the Service health page

Service health posts are written in English due to the timeliness of the information we're posting but can be automatically displayed in the language specified by your personal language settings for Microsoft 365. If you set your preferred language to anything other than English, you'll see an option in the Service health page to automatically translate posts. The messages are machine translated to your preferred language, meaning that a computer did the translation. Before you can choose your language settings, you have to set your preferred language. No translation options are shown when your language is set to English. You can't specify a preferred language for others; each person has to change this setting for themselves.

Before you can choose your language settings, you have to set your preferred language. No translation options are shown when your language is set to English. You can't specify a preferred language for others; each person has to change this setting for themselves.

Set your preferred language

1. Go to the Microsoft 365 admin center <https://admin.microsoft.com>, or home page, select the settings icon in the upper-right corner of the page.
2. Under **Language and time zone**, select **View all** to show the available options. Select your desired language from the drop-down menu, and then select **Save**. Microsoft 365 will try to refresh and display the new language. If that doesn't happen immediately or if it seems that it's taking too long, you can either refresh your browser or sign out and then sign back in.

Machine translation in Service health dashboard

When your preferred language isn't set to English, the option to translate the post into your language is available.

To set Service health posts to automatically machine-translate and display in your preferred language, go to **Health > Service health** dashboard. You'll see a button to toggle automatic translation on or off. When this setting is off, posts are shown in English. When this setting is on, messages display in your preferred language. The setting you choose will persist for each visit.

You also can toggle between seeing details for a specific issue in English and your preferred language in the issue details page that appears after you click the title of an issue.

Related articles

- [Message center Preferences](#)
 - [How to check Windows release health on admin center](#)
-

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Get support for Microsoft 365 for business

Article • 01/11/2024

Check out all of our small business content on [Small business help & learning](#).

Check out [Microsoft 365 small business help](#) on YouTube.

Watch: Get help or support

Check out this video and others on our [YouTube channel](#).

<https://www.microsoft.com/en-us/videoplayer/embed/RE1FOgo?autoplay=false&postJsIMsg=true>

Need to speak to someone right away? Admins, have your account details ready when you call Support.

i Important

You must be an admin for a business subscription to use these support methods. [Find out more about admin roles for the Microsoft 365 admin center](#). If you're not a business admin, please use [this support page](#).

Start by [checking the current health of your services](#). You can view detailed information about current and past issues on the [Service health dashboard](#). If you're experiencing an issue that isn't listed, you can get support in one of the following ways:

Online support

Save time by starting your service request online. We can help you find a solution or connect you to technical support.

i Important

You must have bought at least one subscription through Microsoft to access Microsoft support. If you bought all your subscriptions through a partner, contact your partner for support.

1. Go to the admin center at <https://admin.cloud.microsoft.com>. If you get a message that says you don't have permission to access this page or perform this action, you aren't an admin. For more information, see [Who has admin permissions in my business?](#).
2. On the bottom right side of the page, select **Help & support**.
3. Type a question or keyword into the text box. If you get a drop-down list, select the one closest to your question, or continue typing your question, then press **Enter**.
4. If the results don't help, at the bottom, select **Contact Support**.
5. Enter a description of your issue, confirm your contact number and email address, select your preferred contact method, and then select **Contact me**. The expected wait time is indicated in the **Contact support** pane.

Phone support

In most countries/regions, billing support for Microsoft 365 for business products and services is provided in English from 9 AM-5 PM, Monday through Friday. Local language support varies by country/region.

Technical support is provided in English 24 hours a day, 7 days a week, and in some cases, in local languages as noted.

[Find support phone numbers by country or region](#)

Admins, have your account details ready when you call.

 **Note**

To better protect your organization, we added a PIN-based verification step to our existing phone-based verification process. If you contact us from a number that isn't registered with your organization profile, the Microsoft support representative sends a verification code to the registered email or phone number in your Microsoft 365 admin center profile. You must provide this code to the support representative to grant them access to your organization's account.

Small business support with Business Assist

Get the most out of your subscription with expert advice from small business specialists.

Business Assist for Microsoft 365 is designed for small businesses to give you and your employees around-the-clock access to small business specialists as you grow your business, from onboarding to everyday use. To learn more, see [Business Assist](#).

Related content

[Find docs and training](#) (link page)

[Employee quick setup](#) ↗ (article)

[Overview of Microsoft 365 Business Premium setup](#) (video)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

Exchange Online

Article • 05/08/2024

Microsoft Exchange Online is a cloud based messaging platform that delivers email, calendar, contacts, and tasks. Users connect to Exchange Online using apps like Outlook, Outlook on the web, or Outlook mobile app to access email and collaboration functionality, including shared mailboxes, shared calendars and global address lists.

Exchange is included when you sign up for Microsoft 365 Business or Microsoft 365 for enterprise subscriptions. You can also buy standalone Exchange Online plans for your organization. For a full list of subscription options for Exchange, see the [Exchange Online service descriptions](#).

Manage Exchange Online

As an administrator for your organization, you manage Exchange using both the Microsoft 365 admin center and the Exchange admin center (EAC). Use the Microsoft 365 admin center for user, group, and resource management tasks. Use the EAC for more specific tasks related to Exchange line mail flow, migration, and mobile devices. Learn more at [Exchange admin center](#).

To access EAC:

1. [Sign in](#) to Microsoft 365 using your work or school account that has administrator rights.
2. In the Microsoft 365 admin center navigation, choose ...[Show all*](#) to see the full list.
3. Under Admin centers*, choose **Exchange**.

You can also access EAC directly at <https://admin.exchange.microsoft.com>.

EAC access requires the [Exchange administrator role](#). For more information about assigning administrator roles, see [Assign admin roles in the Microsoft 365 admin center](#).

Tip

When you assign someone to the Exchange administrator role, we recommend also assigning them to the Service Support administrator role. This way they can see important information in the Microsoft 365 admin center, such as the health of the Exchange service, as well as change and release notifications.

Introduction to SharePoint and OneDrive in Microsoft 365 for administrators

Article • 03/28/2024

SharePoint and OneDrive in Microsoft 365 are cloud-based services that help organizations share and manage content, knowledge, and applications to:

- Empower teamwork
- Quickly find information
- Seamlessly collaborate across the organization

The resources on this page are designed to get you started. Depending on the needs of your organization, you may want to read about [migration](#) and [governance](#) options before you start rolling SharePoint and OneDrive out to your users.

If you're ready to get started with SharePoint and OneDrive, read [Plan for SharePoint and OneDrive in Microsoft 365](#) and follow the planning and rollout articles that are listed in that article.

If you're just starting out with SharePoint and OneDrive, learn about the [FastTrack onboarding and adoption services](#), [find a SharePoint certified partner](#), or [visit the SharePoint community](#).

Once you're using SharePoint and OneDrive, get the [OneDrive sync app](#) and the [mobile app](#).

Migration

If you have files that you need to move to SharePoint and OneDrive, the resources in this section can help you get started.

[+] Expand table

If you're looking for this information:	Go to this resource:
Learn how to include migration as part of your plan to roll out SharePoint and OneDrive	Migration planning for SharePoint and OneDrive rollout
How to migrate content from file shares or other cloud providers using Migration Manager	Migrate your content to Microsoft 365

If you're looking for this information:	Go to this resource:
How to migrate SharePoint Server sites and content	Overview of the SharePoint Migration Tool (SPMT)

Governance

If your organization has legal or other requirements that govern the handling of data, or if you have sensitive or confidential information that you want to protect, these references can help you configure SharePoint for your governance standards and policies.

[Expand table](#)

If you're looking for this information:	Go to this resource:
How to plan your compliance requirements for SharePoint and OneDrive	Plan compliance requirements for SharePoint and OneDrive
How to ensure that you retain files for a specified period of time, or delete them on a specified schedule	Overview of retention policies OneDrive retention and deletion
How to classify documents based on the sensitivity of the information	Overview of sensitivity labels Enable sensitivity labels for Office files in SharePoint and OneDrive
How to prevent the loss or exfiltration of important data in documents emails	Learn data loss prevention
Search for in-place items such as email, documents, and instant messaging conversations	Content Search in Microsoft 365

If you use OneDrive in your organization and you want to protect important files by saving them to the cloud, govern how much storage space users get, or govern how users sync file, these references will help you configure your policies.

[Expand table](#)

If you're looking for this information:	Go to this resource:
Protect important files on users' desktops or in their Documents folder	Redirect and move Windows known folders to OneDrive and Redirect and move macOS Desktop and Documents folders to OneDrive

If you're looking for this information:	Go to this resource:
Control how users sync files to their devices	Use Group Policy to control OneDrive sync settings and Deploy and configure the OneDrive sync app for Mac
Configure the amount of storage space users have in OneDrive	Set the default storage space for OneDrive users

Microsoft Teams

SharePoint is deeply integrated into Teams. Files that are stored in Teams are stored in SharePoint sites. When you administer SharePoint sites in the SharePoint admin center, you may find that many of them are connected to teams. Use these resources to understand how SharePoint and Teams are integrated.

[\[\] Expand table](#)

If you're looking for this information:	Go to this resource:
Learn about how Teams and SharePoint work together	Overview of Teams and SharePoint integration
Learn how to manage settings and permissions when Teams and SharePoint are integrated together	Manage settings and permissions when SharePoint and Teams are integrated

Collaboration

SharePoint and OneDrive provide a rich collaboration environment where people inside and outside your organization can work together, coauthoring documents. Microsoft 365 provides a variety of options to help you create a secure and productive file collaboration environment that meets the needs of your organization. Use these resources to get started.

[\[\] Expand table](#)

If you're looking for this information:	Go to this resource:
Learn about secure collaboration in Microsoft 365	Set up secure collaboration with Microsoft 365
Learn about file collaboration and how to plan your implementation	Intro to file collaboration in Microsoft 365

If you're looking for this information:	Go to this resource:
	File collaboration in SharePoint with Microsoft 365
Learn about collaborating with people outside your organization	External sharing overview Collaborate with guests
Use the security and compliance features in Microsoft 365 to help secure your guest sharing environment	Create a secure guest sharing environment

Modern intranet

SharePoint provides a rich set of tools to help you create and maintain your organization's intranet. Use these resources to get started.

[] [Expand table](#)

If you're looking for this information:	Go to this resource:
Learn about the different types of SharePoint sites	Plan your SharePoint site ↗
Select whether to allow users to create their own sites	Manage site creation
Learn how to plan an intelligent intranet for your organization	Plan an intelligent SharePoint intranet
	Planning your SharePoint hub sites

Training

Administrators are often called upon to teach others in the organization how to use new technologies. Use these resources to help your users be successful with SharePoint and OneDrive.

[] [Expand table](#)

If you're looking for this information:	Go to this resource:
Get a list of training resources for your users	Training and change management for rolling out SharePoint and OneDrive
Set up a customizable training portal with Microsoft training content for your organization	Microsoft 365 learning pathways

If you're looking for this information:	Go to this resource:
Show your users the basics of SharePoint	SharePoint help & learning
Show your users the basics of OneDrive	OneDrive help & learning

Customization

SharePoint provides a wide range of options for customization. We recommend using the out-of-box features and functionality as much as possible to meet your organization's needs. If you do need to customize SharePoint, see these references.

[Expand table](#)

If you're looking for this information:	Go to this resource:
Understand how to customize SharePoint using modern tools and techniques	Customizing SharePoint
Build SharePoint Framework solutions, apps, add-ins, and solutions	SharePoint development

Related topics

[SharePoint Limits](#)

[Getting started with the SharePoint Online Management Shell](#)

[Microsoft Partner Center](#)

[Tips and tricks for navigating Microsoft 365 technical documentation](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Manage and monitor Teams

Article • 10/06/2023 • Applies to: Microsoft Teams

Teams provides several tools for managing and monitoring the Teams service, and for managing the users in your organization.

This article provides a roadmap to the content you'll need to successfully manage and monitor your Teams deployment.

- [Administrator roles](#). Read this article to understand Teams administrator roles and capabilities, and how to assign roles to users.
- [The Teams admin center](#). Read this article to understand how to use the Teams admin center for managing Teams.
- [Communicate with users from other organizations](#). Read this article to understand the differences between guest and external access and what functionality is available with both. Additional articles in this section describe how to manage guest and external access.
- [Manage policies](#). Read this article to understand how to define and assign policies to manage users, permissions, and Teams functionality.
- [Monitor and manage call quality](#). Read this article to understand how to use the tools available for monitoring and improving call quality for your organization.
- [Reports in the Teams admin center](#) and [Reports in the Microsoft 365 admin center](#). Read these articles to understand what reports are available, and how to use these reports to monitor Teams usage and service health.

See the following references for overviews of the major features in Teams:

- [Chat, teams, channels](#)
- [Overview of meetings, webinars, and town halls](#)
- [Audio Conferencing in Microsoft Teams](#)
- [Voice](#)
- [Overview of Teams apps](#)

Feedback

Was this page helpful?



Provide product feedback ↗

Office 365 performance tuning using baselines and performance history

Article • 08/15/2023

There are some simple ways to check the connection performance between Office 365 and your business that will let you establish a rough baseline of your connectivity. Knowing the performance history of your client computer connections can help you detect emerging issues early, identify, and predict problems.

If you're not used to working on performance issues, this article is designed to help you consider some common questions. How do you know the problem you're seeing is a performance issue and not an Office 365 service incident? How can you plan for good performance, long term? How can you keep an eye on performance? If your team or clients are seeing slow performance while using Office 365, and you wonder about any of these questions, read on.

Important

Have a performance issue between your client and Office 365 right now? Follow the steps outlined in the [Performance troubleshooting plan for Office 365](#).

Something you should know about Office 365 performance

Office 365 lives inside a high-capacity, dedicated Microsoft network that is monitored by automation and real people. Part of maintaining the Office 365 cloud is performance tuning and streamlining where possible. Since clients of the Office 365 cloud have to connect across the Internet, there's ongoing effort to fine-tune the performance across Office 365 services too.

Performance improvements never really stop in the cloud, so neither does experience with keeping the cloud healthy and quick. Should you have a performance issue connecting from your location to Office 365, it's best not to start with or wait on a Support case. Instead, you should begin investigating the problem from 'the inside out.' That is, start inside of your network, and work your way out to Office 365. Before you open a case with Support, you can gather data and take actions that will explore, and might resolve, the problem.

Important

Be aware of capacity planning and limits in Office 365. That information will put you ahead of the curve when trying to resolve a performance issue. Here's a link to the [**Microsoft 365 and Office 365 service descriptions**](#). This is a central hub, and all the services offered by Office 365 have a link that goes to their own Service Descriptions from here. That means, should you need to see the standard limits for SharePoint, for example, you would click [**SharePoint Service Description**](#) and locate its [**SharePoint Limits section**](#).

Make sure you go into your troubleshooting with the understanding that performance is a sliding scale. It's not about achieving an idealized value and maintaining it permanently. Occasional high-bandwidth tasks like on-boarding a large number of users, or doing large data migrations will be stressful, so *plan* for performance impacts then. You should have a rough idea of your performance targets, but many variables play into performance, so performance varies.

Performance troubleshooting isn't about meeting specific goals and maintaining those numbers indefinitely, it's about improving existing activities, given all the variables.

Okay, what does a performance problem look like?

First, you need to make sure that what you are experiencing is indeed a performance issue and not a service incident. A performance problem is different from a service incident in Office 365. Here's how to tell them apart.

Service Incidents happen when the Office 365 service itself is having issues. You might see red or yellow icons under **Current health** in the Microsoft 365 admin center. You might notice performance on client computers connecting to Office 365 is slow. For example, if Current health reports a red icon and you see **Investigating** beside Exchange, you might then also get calls from people in your organization who complain that client mailboxes using Exchange Online are slow. In that case, it's reasonable to assume that your Exchange Online performance was a victim of Service issues.

Current health

Exchange	Service restored ▾
Identity Service	No issues
Lync	No issues
Office 365 Portal	No issues
Office Subscription	No issues
SharePoint	No issues

[View details and history](#)

At this point, you, the Office 365 admin, should check **Current health** and then **View details and history**, often, to keep up to date on maintenance on the system. The **Current health** dashboard was made to update you about changes to, and problems in, the service. The notes and explanations written to health history, admin to admin, are there to help you gauge, and to keep you posted about ongoing work.

The screenshot shows the Microsoft 365 Admin Center interface. At the top, there's a blue header bar with the 'Office 365' logo and navigation links for Outlook, Calendar, People, Newsfeed, OneDrive, Sites, Tasks, Admin, and user profile. Below the header, a green circular icon with a white arrow indicates a 'New' or 'Updated' status. The main content area is titled 'exchange online'. A table with four columns (Incident, Date and Time, Status, Details) shows one entry. The 'Details' column contains text about a fix for EAC access issues and mentions no end-user impact. It also notes a customer impact related to RBAC features and PowerShell usage.

INCIDENT	DATE AND TIME	STATUS	DETAILS
			Final Status: Engineers have completed deployment of the fix which restored service degradation caused by the EAC access issues. User Experience: There was no end-user impact. Customer Impact: Customer impact appears to have been limited. Affected administrators were unable to view and select some menu items within Exchange Admin Center (EAC). Affected features may have included Role Based Access Control (RBAC), organization sharing, and retention policy. As a workaround, administrators could have executed commands via Powershell.

A performance issue isn't a service incident, even though incidents can cause slow performance. A performance issue looks like this:

- A performance issue occurs no matter what the admin center **Current health** is reporting for the service.
- A behavior that used to flow takes a long time to complete or never completes.
- You can replicate the problem too, or know it happens if you do the right series of steps.
- If the problem is intermittent, there can still be a pattern. For example, you know that by 10:00 AM you'll have calls from users who can't always access Office 365. The calls will end around noon.

This list probably sounds familiar; maybe too familiar. Once you're aware it's a performance problem, the question becomes, "What do you do next?" The rest of this article helps you determine exactly that.

How to define and test the performance problem

Performance issues often emerge over time, so it can be challenging to define the actual problem. Create a good problem statement with a good idea of issue context, and then you need to repeatable testing steps. Here are some examples of problems statements that don't provide enough information:

- Switching from my Inbox to my Calendar used to be something I didn't notice, and now it's a coffee-break. Can you make it act like it used to?
- Uploading my files to SharePoint is taking forever. Why is it slow in the afternoon, but any other time, it's fast? Can't it just be fast?

There are several large challenges posed by the problem statements above. Specifically, too many ambiguities to deal with. For example:

- It's unclear how switching between Inbox and Calendar used to act on the laptop.
- When the user says, "Can't it just be fast", what's "fast"?
- How long is "forever"? Is that several seconds? Or many minutes? Or could the user take lunch and the action would finish up 10 minutes after they got back?

The admin and troubleshooter can't be aware of the *details* of the problem from general statements like these. For example, they don't know when the problem started happening. The troubleshooter might not know the user works from home and only ever sees slow switching while on their home network. Or that the user runs other RAM intensive applications on the local client. Admins might not know the user is running an older operating system or hasn't run recent updates.

When users report a performance problem, there's much information to collect. Getting and recording information is called scoping the issue. Here's a basic scoping list you can use to collect information about performance issues. This list isn't exhaustive, but it's a place to start:

- On what date did the issue happen, and around what time of day or night?

- What kind of client computer were you using, and how does it connect to the business network (VPN, Wired, Wireless)?
- Were you working remotely or were you in the office?
- Did you try the same actions on another computer and see the same behavior?
- Walk through the steps that are giving you the trouble so that you can write the actions you take down.
- How slow in seconds or minutes is the performance?
- Where in the world are you located?

Some of these questions are more obvious than others. Most everyone will understand a troubleshooter needs the exact steps to reproduce the issue. After all, how else can you record what's wrong, and how else can you test if the issue is fixed? Less obvious are things like "What date and time did you see the issue?", and "Where in the world are you located?", information that can be used in tandem. Depending on when the user was working, a few hours of time difference might mean maintenance is already underway on parts of your company's network. For instance, your company has a hybrid implementation, like a hybrid SharePoint Search, which can query search indexes in both SharePoint in Microsoft 365 and an On-premises SharePoint Server 2013 instance, updates might be underway in the on-premises farm. If your company is all in the cloud, system maintenance might include adding or removing network hardware, rolling out updates that are company-wide, or making changes to DNS, or other core infrastructure.

When you're troubleshooting a performance problem, it's a bit like a crime scene, you need to be precise and observant to draw any conclusions from the evidence. In order to do this, you must get a good problem statement by gathering evidence. It should include the computer's context, the user's context, when the problem began, and the exact steps that exposed the performance issue. This problem statement should be, and stay, the topmost page in your notes. By walking through the problem statement again after you work on the resolution, you're taking the steps to test and prove whether the actions you take have resolved the issue. This is critical to knowing when your work, there, is done.

Do you know how performance used to look when it was good?

If you're unlucky, nobody knows. Nobody had numbers. That means nobody can answer the simple question "About how many seconds did it used to take to bring up an Inbox

in Office 365?", or "How long did it used to take when the Executives had a Lync Online meeting?", which is a common scenario for many companies.

What's missing here is a performance baseline.

Baselines give you a context for your performance. You should take a baseline occasionally to frequently, depending on the needs of your company. If you're a larger company, your Operations team may take baselines for your on-premises environment already. For example, if you patch all the Exchange servers on the first Monday of the month, and all your SharePoint servers on the third Monday, your Operations team probably has a list of tasks and scenarios it runs post-patching, to prove that critical functions are operational. For example, opening the Inbox, clicking Send/Receive, and making sure the folders update, or, in SharePoint, browsing the main page of the site, going into the enterprise Search page, and doing a search that returns results.

If your applications are in Office 365, some of the most fundamental baselines you can take measure the time (in milliseconds) from a client computer inside your network, to an egress point, or the point where you leave your network and go out to Office 365. Here are some helpful baselines that you can investigate and record:

- Identify the devices between your client computer and your egress point, for example, your proxy server.
 - You have to know your devices so that you have context (IP addresses, type of device, et cetera) for performance problems that arise.
 - Proxy servers are common egress points, so you can check your web browser to see what proxy server it's set to use, if any.
 - There are third-party tools that can discover and map your network, but the safest way to know your devices is to ask a member of your network team.
- Identify your Internet service provider (ISP), write down their contact information, and ask how many circuits how much bandwidth you have.
- Inside your company, identify resources for the devices between your client and the egress point, or identify an emergency contact to talk to about networking issues.

Here are some baselines that simple testing with tools can calculate for you:

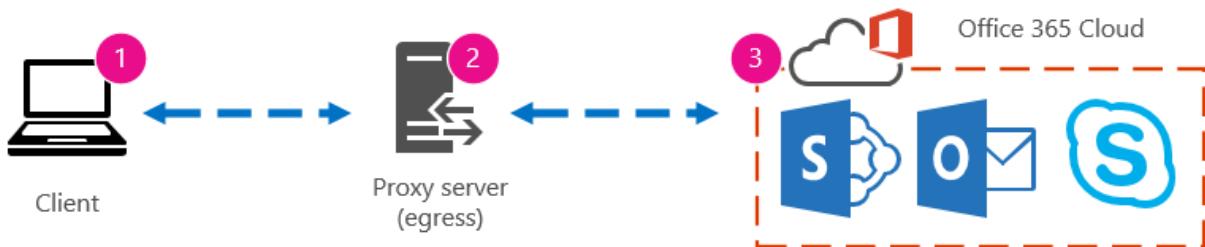
- Time from your client computer to your egress point in milliseconds
- Time from your egress point to Office 365 in milliseconds

- Location in the world of the server that resolves the URLs for Office 365 when you browse
- The speed of your ISP's DNS resolution in milliseconds, inconsistencies in packet arrival (network jitter), upload, and download times in milliseconds

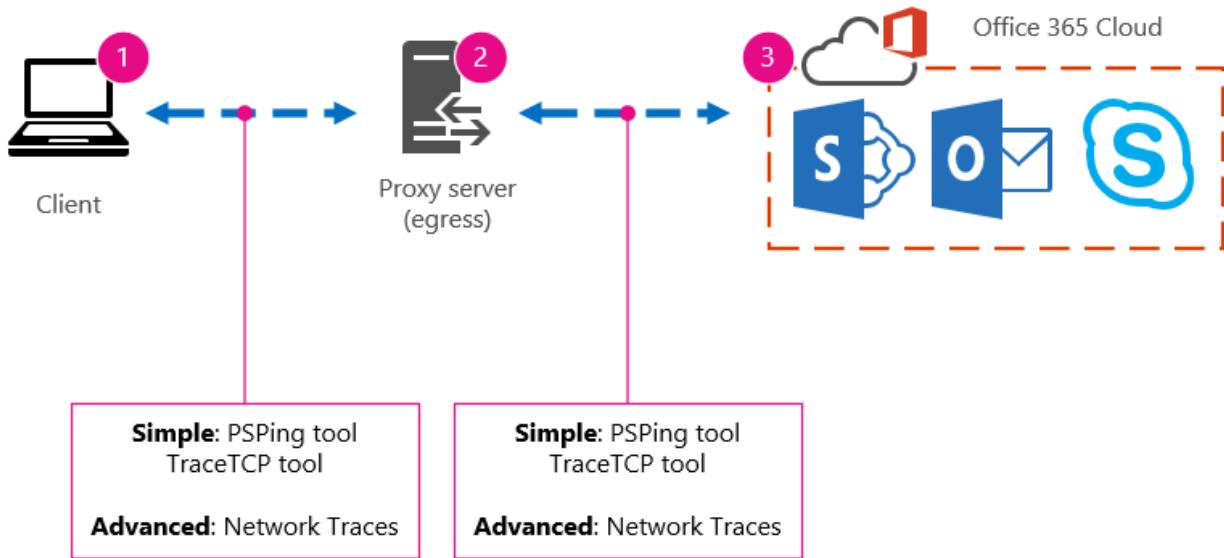
If you're unfamiliar with how to carry out these steps, we'll go into more detail in this article.

What is a baseline?

You'll know the impact when it goes bad, but if you don't know your historical performance data, it's not possible to have a context for how bad it may have become, and when. So without a baseline, you're missing the key clue to solve the puzzle: the picture on the puzzle box. In performance troubleshooting, you need a point of *comparison*. Simple performance baselines aren't difficult to take. Your Operations team can be tasked with carrying these out on a schedule. For example, let's say your connection looks like this:

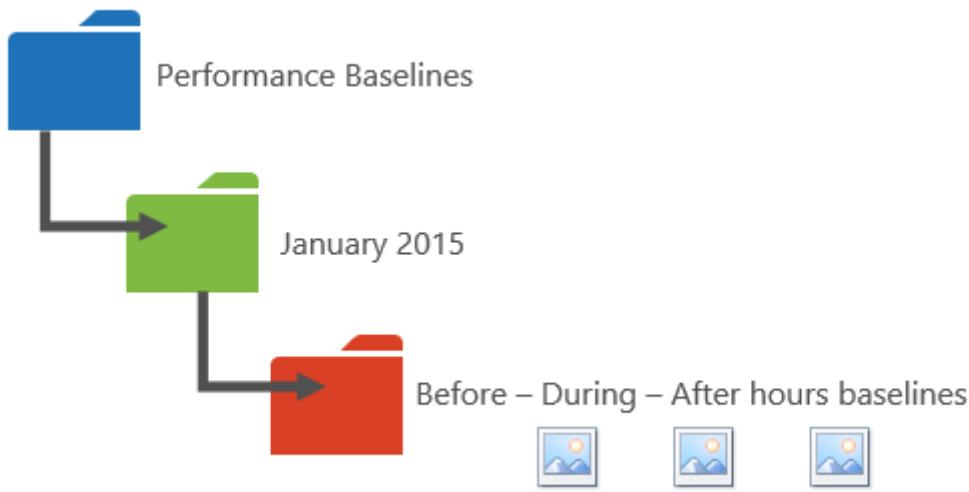


That means you've checked with your network team and found out that you leave your company for the Internet through a proxy server, and that proxy handles all the requests your client computer sends to the cloud. In this case, you should draw a simplified version of your connection that lists all the intervening devices. Now, insert tools that you can use to test the performance between the client, the egress point (where you leave your network for the Internet), and the Office 365 cloud.



The options are listed as **Simple** and **Advanced** because of the amount of expertise you need in order to find the performance data. A network trace will take much time, compared to running command-line tools like PsPing and TraceTCP. These two command-line tools were chosen because they don't use ICMP packets, which will be blocked by Office 365, and because they give the time in milliseconds that it takes to leave the client computer, or proxy server (if you have access) and arrive at Office 365. Each individual hop from one computer to another will end up with a time value, and that's great for baselines! Just as importantly, these command-line tools allow you to add a port number onto the command, this is useful because Office 365 communicates over port 443, which is the port used by Secure Sockets Layer and Transport Layer Security (SSL and TLS). However, other third-party tools might be better solutions for your situation. Microsoft doesn't support all of these tools, so if, for some reason, you can't get PsPing and TraceTCP working, move on to a network trace with a tool like Netmon.

You can take a baseline before business hours, again during heavy use, and then again after hours. This means you might have a folder structure that looks a bit like this in the end:



You should also pick a naming convention for your files. Here are some examples:

- Feb_09_2015_9amPST_PerfBaseline_Netmon_ClientToEgress_Normal
- Jan_10_2015_3pmCST_PerfBaseline_PsPing_ClientToO365_bypassProxy_SLOW
- Feb_08_2015_2pmEST_PerfBaseline_BADPerf
- Feb_08_2015_8-30amEST_PerfBaseline_GoodPerf

There are lots of different ways to do this, but using the format <**dateTime**><**what's happening in the test**> is a good place to start. Being diligent about this will help a lot when you're trying to troubleshoot issues later. Later, you'll be able to say "I took two traces on February 8, one showed good performance and one showed bad, so we can compare them". This is helpful for troubleshooting.

You need to have an organized way to keep your historical baselines. In this example, the simple methods produced three command-line outputs and the results were collected as screenshots, but you might have network capture files instead. Use the method that works best for you. Store your historical baselines and refer to them at points where you notice changes in the behavior of online services.

Why collect performance data during a pilot?

There is no better time to start making baselines than during a pilot of the Office 365 service. Your office might have thousands of users, hundreds of thousands, or it might have five, but even with a few users, you can perform tests to measure fluctuations in performance. In the case of a large company, a representative sample of several hundred users piloting Office 365 can be projected outward to several thousands so you know where issues might arise before they happen.

In the case of a small company, where on-boarding means that all users go to the service at the same time and there's no pilot, keep performance measures so that you have data to show to anyone who might have to troubleshoot a badly performing operation. For example, if you notice that all of a sudden you can walk around your building in the time it takes to upload a medium-sized graphic where it used to happen quickly.

How to collect baselines

For all troubleshooting plans you need to identify these things at a minimum:

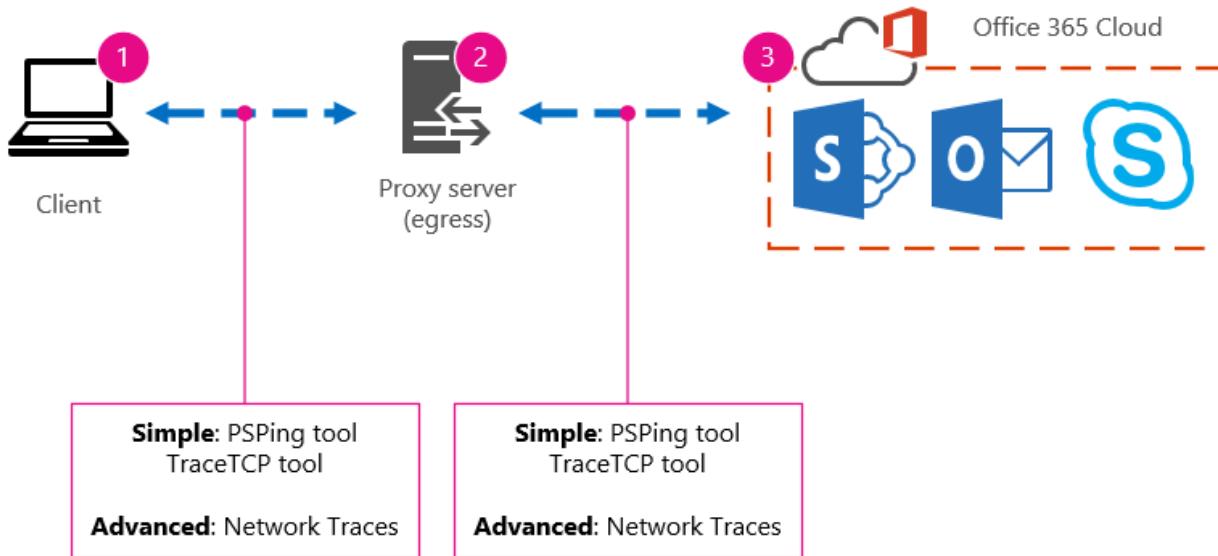
- The client computer you're using (the type of computer or device, an IP address, and the actions that caused the issue)
- Where the client computer is located in the world (for example, whether this user on a VPN to the network, working remotely, or on the company intranet)
- The egress point the client computer uses from your network (the point at which traffic leaves your business for an ISP or the Internet)

You can find out the layout of your network from the network administrator. If you're on a small network, take a look at the devices connecting you to the Internet, and call your ISP if you have questions about the layout. Create a graphic of the final layout for your reference.

This section is broken into simple command-line tools and methods, and more advanced tools options. We'll cover simple methods first. But if you've got a performance problem right now, you should jump to advanced methods and try out the sample performance-troubleshooting action plan.

Simple methods

The objective of these simple methods is to learn to take, understand, and properly store simple performance baselines over time so that you're informed about Office 365 performance. Here's the simple diagram for simple, as you've seen before:



① Note

TraceTCP is included in this screen shot because it's a useful tool for showing, in milliseconds, how long a request takes to process, and how many network hops, or connections from one computer to the next, that the request takes to reach a destination. TraceTCP can also give the names of servers used during hops, which can be useful to a Microsoft Office 365 troubleshooter in Support. > TraceTCP commands can be very simple, such as: > `tracetcp.exe outlook.office365.com:443` > Remember to include the port number in the command! > [TraceTCP](#) ↗ is a free download, but relies on Wincap. Wincap is a tool that is also used and installed by Netmon. We also use Netmon in the advanced methods section.

If you have multiple offices, you'll need to keep a set of data from a client in each of those locations as well. This test measures latency, which, in this case, is a number value that describes the amount of time between a client sending a request to Office 365, and Office 365 responding to the request. The testing originates inside your domain on a client computer, and looks to measure a round trip from inside your network, out through an egress point, across the Internet to Office 365, and back.

There are a few ways to deal with the egress point, in this case, the proxy server. You can either trace from 1 to 2 and then 2 to 3, and then add the numbers in milliseconds to get a final total to the edge of your network. Or, you can configure the connection to bypass the proxy for Office 365 addresses. In a larger network with a firewall, reverse proxy, or some combination of the two, you might need to make exceptions on the proxy server that will allow traffic to pass for a lot of URLs. For the list of endpoints used by Office 365, see [Office 365 URLs and IP address ranges](#) ↗. If you have an authenticating proxy, begin by testing exceptions for the following:

- Ports 80 and 443
- TCP and HTTPs
- Connections that are outbound to any of these URLs:
 - *.microsoftonline.com
 - *.microsoftonline-p.com
 - *.sharepoint.com
 - *.outlook.com
 - *.lync.com
 - osub.microsoft.com

All users need to be allowed to get to these addresses without any proxy interference or authentication. On a smaller network, you should add these to your proxy bypass list in your web browser.

To add these to your proxy bypass list in Internet Explorer, go to **Tools > Internet Options > Connections > LAN settings > Advanced**. The advanced tab is also where you'll find your proxy server and proxy server port. You might need to select the checkbox **Use a proxy server for your LAN**, to access the **Advanced** button. You'll want to make sure that **Bypass proxy server for local addresses** is checked. Once you select **Advanced**, you'll see a text box where you can enter exceptions. Separate the wildcard URLs listed above with semi-colons, for example:

`*.microsoftonline.com; *.sharepoint.com`

Once you bypass your proxy, you should be able to use ping or PsPing directly on an Office 365 URL. The next step will be to test ping **outlook.office365.com**. Or, if you're using PsPing or another tool that will let you supply a port number to the command, PsPing against **portal.microsoftonline.com:443** to see the average round-trip time in milliseconds.

The round-trip time, or RTT, is a number value that measures how long it takes to send an HTTP request to a server like outlook.office365.com and get a response back that acknowledges the server knows that you did it. You'll sometimes see this abbreviated as RTT. This should be a relatively short amount of time.

You have to use **PSPing** or another tool that doesn't use ICMP packets that are blocked by Office 365 in order to do this test.

How to use PsPing to get an overall round trip time in milliseconds directly from an Office 365 URL

1. Run an elevated command prompt by completing these steps:
2. Click Start.
3. In the Start Search box, type cmd, and then press CTRL+SHIFT+ENTER.
4. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue.
5. Navigate to the folder where the tool (in this case PsPing) is installed and test these Office 365 URLs:
 - psping admin.microsoft.com:443
 - psping microsoft-my.sharepoint.com:443
 - psping outlook.office365.com:443
 - psping [www.yammer.com:443 ↗](http://www.yammer.com:443)

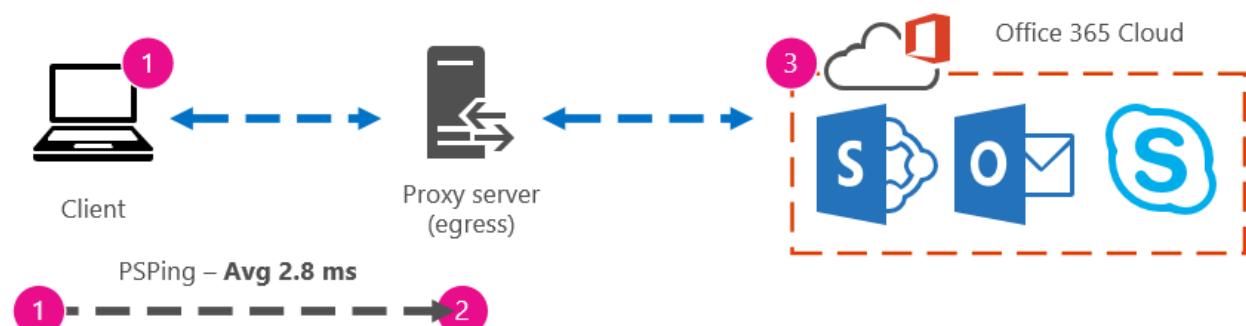
```
C:\>psping microsoft-my.sharepoint.com:443
PsPing v2.01 - PsPing - ping, latency, bandwidth measurement utility
Copyright <C> 2012-2014 Mark Russinovich
Sysinternals - www.sysinternals.com

TCP connect to 2a01:111:f402:340d::14:443:
5 iterations (warmup 1) connecting test:
Connecting to 2a01:111:f402:340d::14:443 (warmup): 51.42ms
Connecting to 2a01:111:f402:340d::14:443: 53.63ms
Connecting to 2a01:111:f402:340d::14:443: 51.41ms
Connecting to 2a01:111:f402:340d::14:443: 50.84ms
Connecting to 2a01:111:f402:340d::14:443: 51.48ms

TCP connect statistics for 2a01:111:f402:340d::14:443:
  Sent = 4, Received = 4, Lost = 0 (0% loss),
  Minimum = 50.84ms, Maximum = 53.63ms, Average = 51.84ms

C:\>
```

Be sure to include the port number of 443. Remember that Office 365 works on an encrypted channel. If you PsPing without the port number, your request will fail. Once you've pinged your short list, look for the Average time in milliseconds (ms). That is what you want to record!



If you're not familiar with proxy bypass, and prefer to take things step by step, you need to first find out the name of your proxy server. In Internet Explorer, go to **Tools > Internet Options > Connections > LAN settings > Advanced**. The **Advanced** tab is where you'll see your proxy server listed. Ping that proxy server at a command prompt by completing this task:

To ping the proxy server and get a round trip value in milliseconds for stage 1 to 2

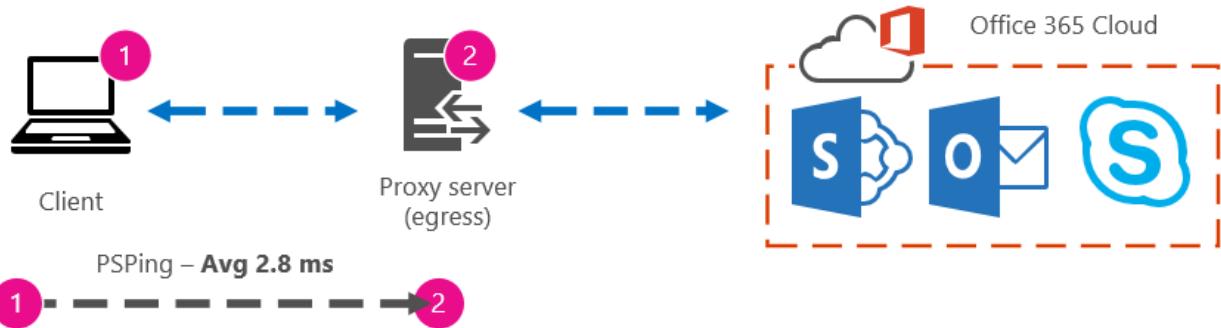
1. Run an elevated command prompt by completing these steps:
2. Click **Start**.
3. In the **Start Search** box, type cmd, and then press CTRL+SHIFT+ENTER.
4. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
5. Type ping <the name of the proxy server your browser uses, or the IP address of the proxy server> and then press ENTER. If you have PsPing, or some other tool, installed, you can choose to use that tool instead.

Your command might look like any of these examples:

- ping ourproxy.ourdomain.industry.business.com
- ping 155.55.121.55
- ping ourproxy
- psping ourproxy.ourdomain.industry.business.com:80
- psping 155.55.121.55:80
- psping ourproxy:80

3. When the trace stops sending test packets, you'll get a small summary that lists an average, in milliseconds, and that's the value you are after. Take a screenshot of the prompt and save it using your naming convention. At this point it might also help to fill in the diagram with the value.

Maybe you've taken a trace in the early morning, and your client can get to the proxy (or whatever egress server exits to the Internet) quickly. In this case, your numbers might look like this:



If your client computer is one of the select few with access to the proxy (or egress) server, you can run the next leg of the test by remotely connecting to that computer, running the command prompt to PsPing to an Office 365 URL from there. If you don't have access to that computer, you can contact your network resources for help with the next leg and get exact numbers that way. If that's not possible, take a PsPing against the Office 365 URL in question and compare it to the PsPing or Ping time against your proxy server.

For example, if you have 51.84 milliseconds from the client to the Office 365 URL, and you have 2.8 milliseconds from the client to the proxy (or egress point), then you have 49.04 milliseconds from the egress to Office 365. Likewise, if you have a PsPing of 12.25 milliseconds from the client to the proxy during the height of the day, and 62.01 milliseconds from the client to the Office 365 URL, then your average value for the proxy egress to the Office 365 URL is 49.76 milliseconds.



In terms of troubleshooting, you might find something interesting just from keeping these baselines. For example, if you find that you generally have about 40 milliseconds to 59 milliseconds of latency from the proxy or egress point to the Office 365 URL, and have a client to proxy or egress point latency of about 3 milliseconds to 7 milliseconds (depending on the amount network traffic you're seeing during that time of day) then you'll surely know something is problematic if your last three client to proxy or egress baselines show a latency of 45 milliseconds.

Advanced methods

If you really want to know what is happening with your Internet requests to Office 365, you need to become familiar with network traces. It doesn't matter which tools you prefer for these traces, HTTPWatch, Netmon, Message Analyzer, Wireshark, Fiddler, Developer Dashboard tool or any other will do as long as that tool can capture and filter

network traffic. You'll see in this section that it's beneficial to run more than one of these tools to get a more complete picture of the problem. When you're testing, some of these tools also act as proxies in their own right. Tools used in the companion article, [Performance troubleshooting plan for Office 365](#), include [Netmon 3.4](#), [HTTPWatch](#), or [WireShark](#).

Taking a performance baseline is the simple part of this method, and many of the steps are the same as when you troubleshoot a performance issue. The more advanced methods of creating baselines for performance require you to take and store network traces. Most of the examples in this article use SharePoint, but you should develop a list of common actions across the Office 365 services to which you subscribe to test and record. Here's a baseline example:

- Baseline list for SPO - **Step 1:** Browse the home page of the SPO website and do a network trace. Save the trace.
- Baseline list for SPO - **Step 2:** Search for a term (such as your company name) via Enterprise Search and do a network trace. Save the trace.
- Baseline list for SPO - **Step 3:** Upload a large file to a SharePoint document library and do a network trace. Save the trace.
- Baseline list for SPO - **Step 4:** Browse the home page of the OneDrive website and do a network trace. Save the trace.

This list should include the most important common actions that users take against SharePoint. Notice that the last step, to trace going to OneDrive, builds-in a comparison between the load of the SharePoint home page (which is often customized by companies) and OneDrive home page, which is seldom customized. This is a basic test when it comes to a slow-loading SharePoint site. You can build a record of this difference into your testing.

If you are in the middle of a performance problem, many of the steps are the same as when taking a baseline. Network traces become critical, so we'll handle *how* to take the important traces next.

To tackle a performance problem, *right now*, you need to be taking a trace at the time you're experiencing the performance issue. You need to have the proper tools available to gather logs, and you need an action plan, that is, a list of troubleshooting actions to take to gather the best information that you can. The first thing to do is record the date and time of the test so that the files can be saved in a folder that reflect the timing. Next, narrow down to the problem steps themselves. These are the exact steps you'll use for testing. Don't forget the basics: if the issue is only with Outlook, make sure to record

that the problem behavior happens in only one Office 365 service. Narrowing down the scope of this issue will help you to focus on something you can resolve.

See also

[Managing Office 365 endpoints](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Tune Exchange Online performance

Article • 09/29/2022

This article contains general tips and links to other resources that tell you how to improve performance of Exchange Online, particularly in front of a migration. This article is part of the [Network planning and performance tuning for Office 365](#) project.

Things to consider in order to improve Exchange Online performance

To improve the speed of migration and reduce your organization's bandwidth constraints for Exchange Online, consider the following:

- **Reduce mailbox sizes.** Smaller mailbox size improves migration speed.
- **Use the mailbox move capabilities with an Exchange hybrid deployment.** With an Exchange hybrid deployment, offline mail (in the form of .OST files) doesn't require redownload when migrating to Exchange Online. This significantly reduces your download bandwidth requirements.
- **Schedule mailbox moves to occur during periods of low Internet traffic and low on-premises Exchange use.** When scheduling moves, migration requests are submitted to the mailbox replication proxy and might not take place immediately.
- **Use lean popouts for Outlook on the web.** Lean popouts provide smaller, less memory-intensive versions of certain email messages in Microsoft Edge or Internet Explorer by rendering some components on the server. For more information, see [Use lean popouts to reduce memory used when reading mail messages](#).

General advice

- Make certain that DNS lookup for outlook.office.com enters the MS-datacenter at a logical entry location for your location.
- Research mailbox caching and choose the appropriate options (re. caching period, shared mailbox caching, et cetera).
- Keep your Outlook data from passing over VPN connections (to a central office) before it goes over the Internet.
- Be sure your mailbox data adheres to the limitations on folder, and item, amounts.

For more information about Exchange migration performance, see [Office 365 migration performance and best practices](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Tune SharePoint in Microsoft 365 performance

Article • 06/27/2024

This article contains links to other articles that tell you how to improve performance of page download times for SharePoint in Microsoft 365. This article is part of the [Network planning and performance tuning for Office 365](#) project.

Articles about fine tuning SharePoint in Microsoft 365 performance

Use these articles to fine tune SharePoint in Microsoft 365 performance.

- [Introduction to performance tuning for SharePoint](#)
- [Use the Page Diagnostics tool for SharePoint](#)
- [Navigation options for SharePoint](#)
- [Performance guidance for SharePoint portals](#)
- [Image optimization for SharePoint](#)
- [Delay loading images and JavaScript in SharePoint](#)
- [Minification and bundling in SharePoint](#)
- [Use the Office 365 Content Delivery Network \(CDN\) with SharePoint](#)
- [Using Content Search Web Part instead of Content Query Web Part to improve performance in SharePoint](#)
- [Capacity planning and load testing SharePoint](#)
- [Diagnosing performance issues with SharePoint](#)
- [Using the object cache with SharePoint](#)
- [How to: Avoid getting throttled or blocked in SharePoint](#)
- [Optimize iFrames in SharePoint modern portal pages](#)
- [Optimize web part performance in SharePoint modern portal pages](#)

- Optimize page calls in SharePoint modern portal pages
 - Optimize page weight in SharePoint modern portal pages
 - Optimize images in SharePoint modern portal pages
-

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Introduction to performance tuning for SharePoint

Article • 05/17/2024

This article explains what specific aspects you need to consider when designing pages for best performance in SharePoint.

SharePoint performance metrics

The following broad metrics for SharePoint provide real-world data about performance:

- The speed at which pages load
- The number of round-trips required per page
- Issues with the SharePoint service
- Other factors that cause performance degradation

Conclusions reached from the data

General benchmarking data tells us:

- Most of the pages perform well on SharePoint.
- Noncustomized pages load more quickly.
- OneDrive, team sites and system pages, such as _layouts, etc., are all quick to load.
- The slowest 1% of SharePoint pages take more than 5,000 milliseconds to load.

One simple benchmark test you can use would be to measure performance by comparing the load time of your own portal against the load time of the OneDrive home page as it uses few customized features. This step is often the first step Support asks you to complete when troubleshooting network performance issues.

Use a standard user account when checking performance

A site admin, Site Owner, Editor, or Contributor belong to another security groups, have more permissions, and therefore have extra elements that SharePoint loads on a page.

This scenario is applicable to SharePoint on-premises and SharePoint in Microsoft 365, but in an on-premises scenario the differences can't be as easily noticed as in SharePoint in Microsoft 365.

In order to correctly evaluate how a page performs for users, you should use a standard user account to avoid loading the authoring controls and extra traffic related to security groups.

Connection categories for performance tuning

You can categorize the connections between the server and the user into three main components. Consider these components when designing SharePoint pages for insight into load times.

- **Server** The servers that Microsoft hosts in datacenters.
- **Network** The Microsoft network, the Internet, and your on-premises network between the datacenter and your users.
- **Browser** Where the page is loaded.

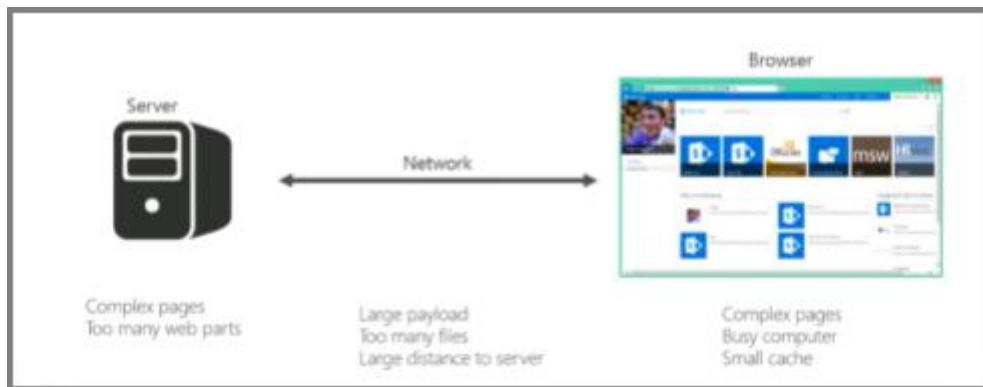
Within these three connections, there are typically five reasons that cause 95% of slow pages. Each of these reasons is discussed in this article:

- Navigation issues
- Content roll-up
- Large files
- Many requests to the server
- Web Part processing

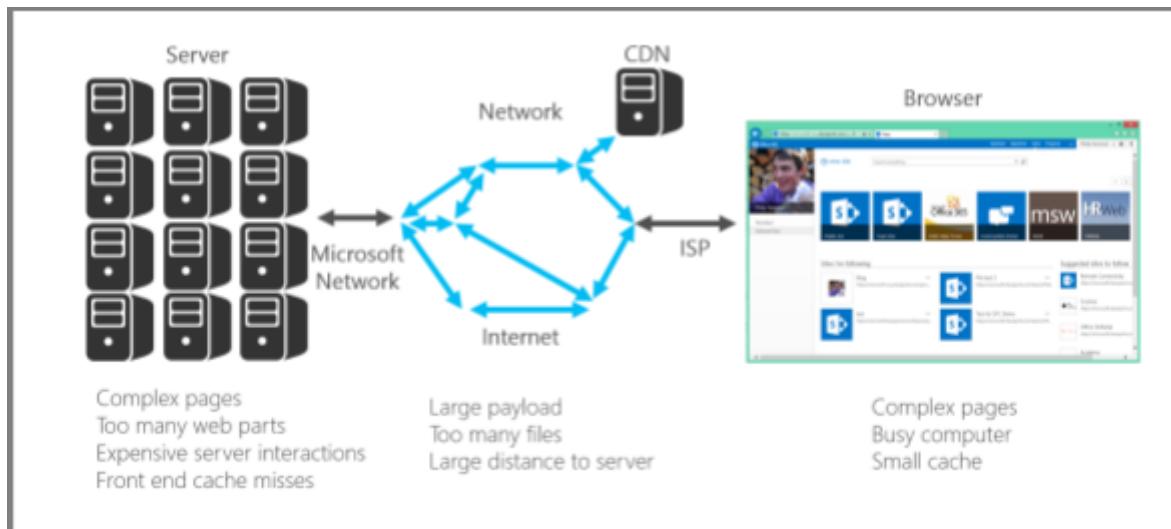
Server connection

Many of the issues that affect performance with SharePoint on-premises also apply to SharePoint in Microsoft 365.

As you would expect, you have far more control over how servers perform with on-premises SharePoint. With SharePoint in Microsoft 365, things are a little different. The more work you make a server do, the longer it takes to render a page. The biggest culprits in this respect are complex pages with multiple web parts.



SharePoint in Microsoft 365



With SharePoint on-premises, certain page requests might actually end up calling multiple servers. You could end up with a matrix of requests between servers for an individual request. These interactions are expensive from a page load perspective and make things slow.

Examples of these server-to-server interactions are:

- Web to SQL Servers
- Web to application servers

The other thing that can slow down server interactions is cache misses. Unlike on-premises SharePoint, there's a slim chance that you would hit the same server for a page that you visited previously; this makes object caching obsolete.

Network connection

With on-premises SharePoint that doesn't make use of a WAN, you can use a high-speed connection between datacenter and end users. Generally, things are easy to manage from a network perspective.

With SharePoint in Microsoft 365, there are a few more factors to consider; for example:

- The Microsoft network
- The Internet
- The Internet Service Provider (ISP)

Regardless of which version of SharePoint (and which network) you're using, things that typically cause the network to be busy include:

- Large payload
- Many files
- Large physical distance to the server

One feature that you can use in SharePoint in Microsoft 365 is the Microsoft 365 CDN (Content Delivery Network). A CDN is basically a distributed collection of servers deployed across multiple datacenters. With a CDN, content on pages can be hosted on a server close to the client even if the client is far away from the originating SharePoint server. Microsoft will be using this feature more in the future to store local instances of pages that can't be customized, for example the SharePoint admin home page. For more information about CDNs, see [Content delivery networks](#).

Something that you need to be aware of but have no control over is the connection speed of your ISP. A simple speed test tool tells you the connection speed.

Browser connection

There are a few factors to consider with web browsers from a performance perspective.

Visiting complex pages affects performance. Most browsers only have a small default cache size (around 90 MB), while the average web page is typically around 1.6 MB, which doesn't take long to get used up.

Bandwidth can also be an issue. For example, if a user is watching videos in another session, it can affect the performance of your SharePoint page. While you can't prevent users from streaming media, you can control the way a page loads for users.

Check out the following articles for different SharePoint page customization techniques and other best practices to help you achieve optimal performance.

- [Navigation options for SharePoint](#)
- [Use the Page Diagnostics tool for SharePoint](#)

- Image optimization for SharePoint
 - Delay loading images and JavaScript in SharePoint
 - Minification and bundling in SharePoint
 - Use the Office 365 Content Delivery Network (CDN) with SharePoint
 - Using Content Search Web Part instead of Content Query Web Part to improve performance in SharePoint
 - Capacity planning and load testing SharePoint
 - Diagnosing performance issues with SharePoint
 - Using the object cache with SharePoint
 - How to: Avoid getting throttled or blocked in SharePoint
-

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Diagnosing performance issues with SharePoint

Article • 02/21/2024

This article shows you how you can diagnose common issues with your SharePoint site using Internet Explorer developer tools.

There are four different ways that you can identify that a page on a SharePoint site has a performance problem with the customizations.

- The Page Diagnostics for SharePoint tool
- The F12 tool bar network monitor
- Comparison to a noncustomized baseline
- SharePoint response header metrics

This article describes how to use each of these methods to diagnose performance issues. Once you've figured out the cause of the problem, you can work toward a solution using the articles about improving SharePoint performance that you can find on <https://aka.ms/tune>.

Use the Page Diagnostics for SharePoint tool

The Page Diagnostics for SharePoint tool is a browser extension for Microsoft Edge (<https://www.microsoft.com/edge>) and Chrome browsers that analyzes both SharePoint modern portal and classic publishing site pages.

Important

This tool only works for SharePoint in Microsoft 365, and can't be used on a SharePoint system page or on a SharePoint App page. The App page type is designed to be used for specific business applications within SharePoint and not for portals. The tool is designed to optimize portal pages and Teams site pages.

The tool generates a report for each analyzed page showing how the page performs against a predefined set of rules and displays detailed information when results for a test fall outside the baseline value. SharePoint administrators and designers can use the tool to troubleshoot performance issues and to ensure that new pages are optimized prior to publishing.

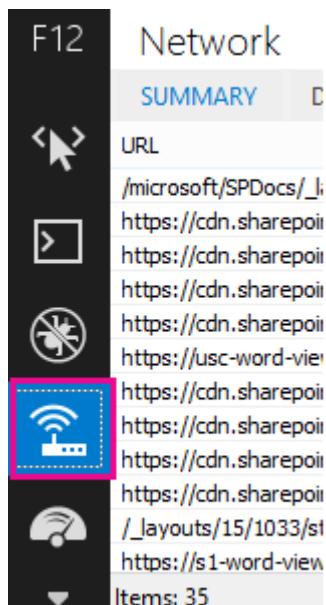
For more information about how to install and use the tool, see [Page Diagnostics for SharePoint tool](#).

Using the F12 tool bar to diagnose performance in SharePoint

In this article, we use Internet Explorer 11. Versions of the F12 developer tools on other browsers have similar features though they might look slightly different. For information on the F12 developer tools, see:

- [What's new in F12 Tools](#)
- [Using the F12 developer tools](#)

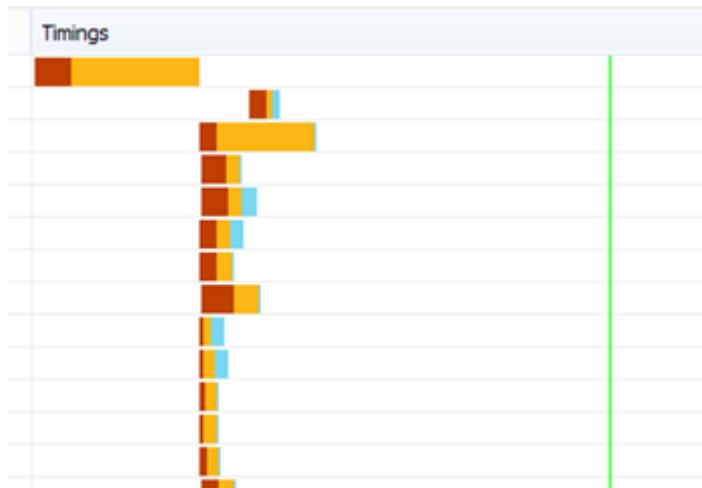
To bring up the developer tools press **F12** and then click the Wi-Fi icon:



On the **Network** tab, press the green play button to load a page. The tool returns all of the files that the browser requests in order to get the page you asked for. The following screenshot shows one such list.

URL
https://www.outlook.com/owa/?exch=1
https://spperformance.sharepoint.com/sites/NavigationBySearch/SitePages/Home.aspx
https://spperformance.sharepoint.com/sites/NavigationBySearch/SitePages/Home.aspx
https://secure.aadcdn.microsoftonline-p.com/aad/20.200.19625/js/jquery.easing.1.3.js
https://secure.aadcdn.microsoftonline-p.com/aad/20.200.19625/js/jquery.1.5.1.min.js
https://secure.aadcdn.microsoftonline-p.com/aad/20.200.19625/js/aad.login.js
https://secure.aadcdn.microsoftonline-p.com/aad/20.200.19625/css/login.ltr.css
https://prod.msocdn.com/16.00.0458.005/en-US/JSC/O365ShellPlus.js
https://prod.msocdn.com/16.00.0458.005/en-US/JSC/CoreShellBundle.js
https://prod.msocdn.com/16.00.0458.005/en-US/JSC/CoreShellBundle.js
https://prod.msocdn.com/16.00.0458.005/en-US/css/shellg1pluscss_7ae920ff.css
https://prod.msocdn.com/16.00.0458.005/en-US/css/shellg1corecss_55f6794d.css
https://prod.msocdn.com/16.00.0458.005/en-US/css/shelleoticons_f48736e7.eot?#iefix
https://portal.office.com/SuiteServiceProxy.aspx?exsvurl=1&realm=office365.com&Silent=1
https://portal.office.com/SuiteServiceProxy.aspx?exsvurl=1&realm=office365.com

You can also see the download times of the files on the right side as shown in this screenshot.



This gives you a visual representation of how long the file took to load. The green line represents when the page is ready to be rendered by the browser. This can give you a quick view of the different files that might be causing slow page loads on your site.

Setting up a noncustomized baseline for SharePoint

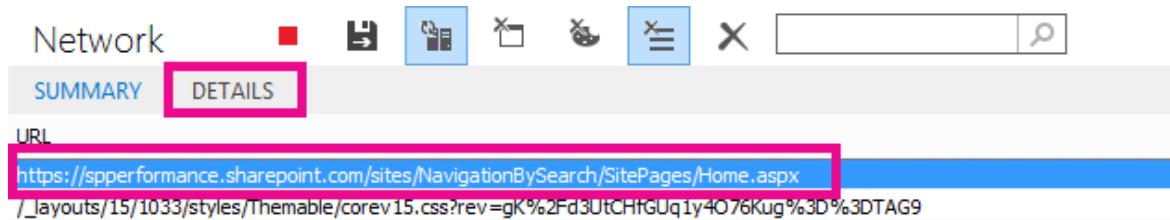
The best way to determine your site's performance weak points is to set up a completely out-of-the-box site collection in SharePoint. This way you can compare all the various aspects of your site with what you would get with no customization on the page. The OneDrive for Business home page is a good example of a separate site collection that is unlikely to have any customizations.

Viewing SharePoint response header information

In SharePoint, you can access the information that is sent back to the browser in the response header for each file. The most useful value for diagnosing performance issues is **SPRequestDuration**, which displays the amount of time that the request took on the server to be processed. This can help determine if the request is heavy and resource intensive. This is the best insight you have into how much work the server is doing to serve the page.

To view SharePoint response header information

1. Ensure that you have the F12 tools installed. For more information on downloading and installing these tools, see [What's new in F12 tools](#).
2. In the F12 tools, on the **Network** tab, press the green play button to load a page.
3. Click one of the .aspx files returned by the tool and then click **DETAILS**.



4. Click **Response headers**.

Request headers	Request body	Response headers	Response body
Key		Value	
Response		HTTP/1.1 200 OK	
Cache-Control		private, max-age=86400	
Content-Type		text/html; charset=utf-8	
Expires		Tue, 21 Oct 2014 21:47:52 GMT	
Server		Microsoft-IIS/7.5	
Set-Cookie		rtFa=EOjag36aM1ndJa+huflEw	
Set-Cookie		FedAuth=77u/PD94bWwgdmVy	
X-AspNet-Version		4.0.30319	
SPRequestGuid		4b1bc49c-6003-1000-8be7-ff19	
request-id		4b1bc49c-6003-1000-8be7-ff19	
X-FRAME-OPTIONS		SAMEORIGIN	
SPRequestDuration	71		
SPIisLatency	0		
X-Powered-By	ASP.NET		
MicrosoftSharePointTeamServices	16.0.0.3312		
X-Content-Type-Options	nosniff		
X-MS-InvokeApp	1; RequireReadOnly		
P3P	CP="ALL IND DSP COR ADM CO		
Date	Mon, 20 Oct 2014 21:47:51 GM		
Content-Length	21059		

What's causing performance issues in SharePoint?

The article [Navigation options for SharePoint](#) shows an example of using the SPRequestDuration value to determine that the complicated structural navigation was causing the page to take a long time to process on the server. By taking a value for a baseline site (without customization), it's possible to determine if any given file is taking a long time to load. The example used in [Navigation options for SharePoint](#) is the main .aspx file. That file contains most of the ASP.NET code that runs for your page load. Depending on the site template you use, this could be start.aspx, home.aspx, default.aspx, or another name if you customize the home page. If this number is considerably higher than your baseline site, then it's a good indication that there's something complex going on in your page that is causing performance issues.

Once you've identified that an issue specific to your site, the recommended way to figure out what is causing poor performance is to eliminate all of the possible causes, like page customizations, and then add them back to the site one by one. Once you have removed enough customizations that the page is performing well, you can then add back specific customizations one by one.

For example, if you have a complex navigation try changing the navigation to not show subsites then check the developer tools to see if this makes a difference. Or if you have a large number of content roll-ups try removing them from your page and see if this

improves things. If you eliminate all of the possible causes and add them back in one at a time, you can easily identify which features are the biggest problem and then work towards a solution.

Feedback

Was this page helpful?



Yes



No

[Provide product feedback ↗](#)

Use the Page Diagnostics for SharePoint tool

Article • 01/08/2024

This article describes how to use the **Page Diagnostics for SharePoint tool** to analyze SharePoint in Microsoft 365 modern and classic site pages against a predefined set of performance criteria.

The Page Diagnostics for SharePoint tool can be installed for:

- [Microsoft Edge extension](#)
- [Chrome extension](#)

Tip

Version 2.0.0 and later includes support for modern pages in addition to classic site pages. If you are unsure which version of the tool you are using, you can select the **About** link or the ellipses (...) to verify your version. **Always update to the latest version** when using the tool.

The Page Diagnostics for SharePoint tool is a browser extension for the new Microsoft Edge (<https://www.microsoft.com/edge>) and Chrome browsers that analyzes both SharePoint in Microsoft 365 modern portal and classic publishing site pages.

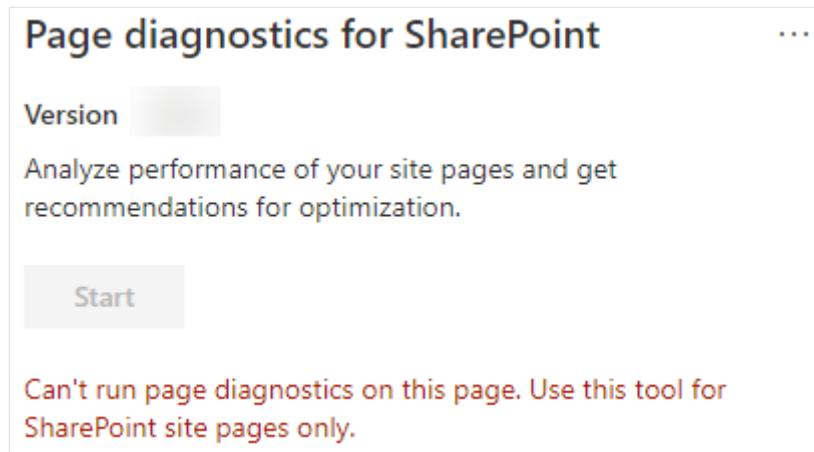
Important

This tool only works for SharePoint in Microsoft 365, and can't be used on a SharePoint system page or on a SharePoint App page. The App page type is designed to be used for specific business applications within SharePoint in Microsoft 365 and not for portals. The tool is designed to optimize portal pages and Teams site pages.

The tool generates a report for each analyzed page showing how the page performs against a predefined set of rules and displays detailed information when results for a test fall outside the baseline value. SharePoint administrators and designers can use the tool to troubleshoot performance issues and to ensure that new pages are optimized prior to publishing.

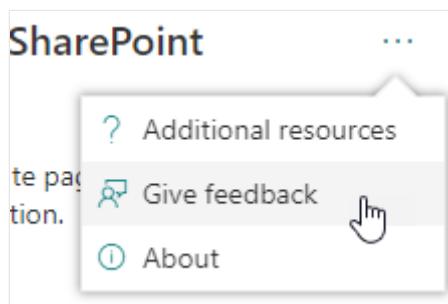
The Page Diagnostics tool is designed to analyze SharePoint site pages only, not system pages such as *allitems.aspx* or *sharepoint.aspx*. If you attempt to run the tool on a

system page or any other nonsite page, you'll receive an error message advising that the tool can't be run for that type of page.



This isn't an error in the tool as there's no value in assessing libraries or system pages. Navigate to a SharePoint site page to use the tool. If this error occurs on a SharePoint page, check the master page to ensure that the SharePoint metatags haven't been removed.

To provide feedback about the tool, select the ellipsis at the top right corner of the tool and then select **Give feedback**.



Install the Page Diagnostics for SharePoint tool

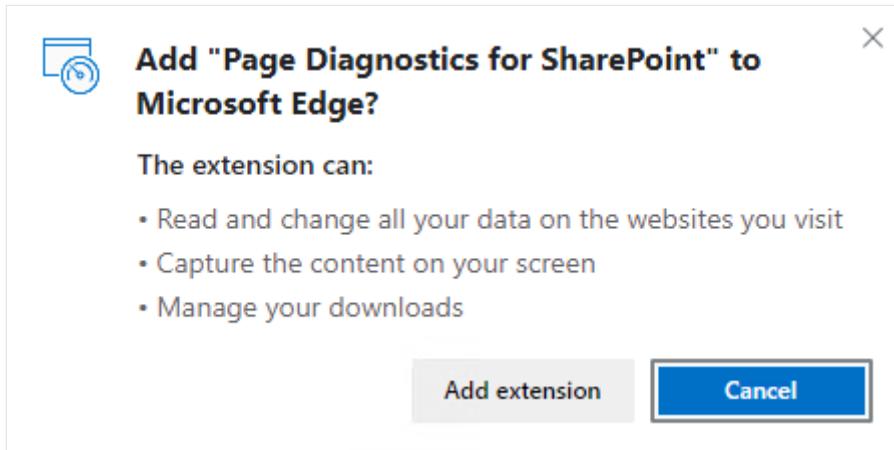
The installation procedure in this section works for both the Chrome and Microsoft Edge browsers.

ⓘ Important

Microsoft does not read data or page content that is analyzed by the Page Diagnostics for SharePoint tool, and we do not capture any personal information, website or download information. The only identifiable information logged to Microsoft by the tool is the tenant name, counts of rules that have failed and the date and time the tool was run. This information is used by Microsoft to better

understand modern portal and publishing site usage trends and common performance issues.

1. Install the Page Diagnostics for SharePoint tool for **Microsoft Edge** ([Edge extension](#)) or **Chrome** ([Chrome extension](#)). Review the User Privacy Policy provided on the description page in the store. When adding the tool to your browser, you'll see the following permissions notice.



This notice is in place because a page may contain content from locations outside of SharePoint depending on the web parts and customizations on the page. This means that the tool will read the requests and responses when the start button is clicked and only for the active SharePoint tab where the tool is running. This information is captured locally by the web browser and is available to you via the **Export to JSON** or **Export to HAR** button in the tool's *Network trace* tab. **The information is not sent to or captured by Microsoft.** (The tool respects the Microsoft privacy policy accessible [here](#).)

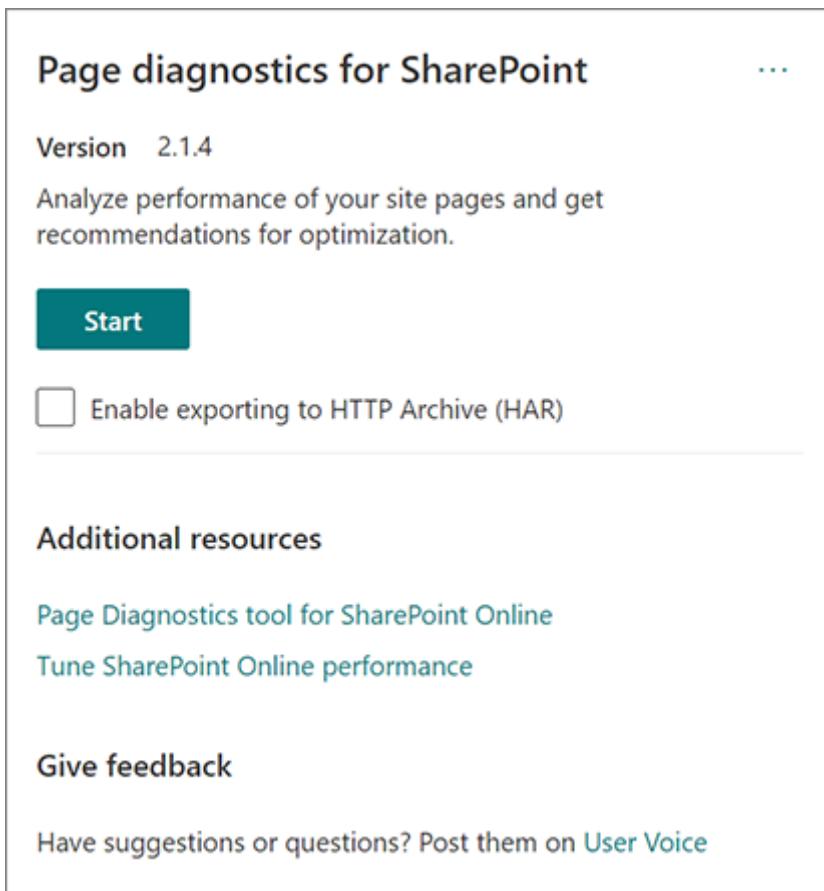
The *Manage your downloads* permission covers use of the tool's **Export to JSON** functionality. Follow your company's own privacy guidelines before sharing the JSON file outside of your organization, as the results contain URLs and that can be classified as PII (Personally Identifiable Information).

2. If you want to use the tool in Incognito or InPrivate mode, follow the procedure for your browser:
 - a. In Microsoft Edge, navigate to **Extensions** or type `edge://extensions` in the URL bar and select **Details** for the extension. In the extension settings, select the checkbox for **allow in InPrivate**.
 - b. In Chrome, navigate to **Extensions** or type `chrome://extensions` in the URL bar and select **Details** for the extension. In the extension settings, select the slider for **allow in Incognito**.

3. Navigate to the SharePoint site page on SharePoint that you would like to review.

We've allowed for "delay loading" of items on pages; therefore, the tool won't stop automatically (this is by design to accommodate all page load scenarios). To stop collection, select **Stop**. Make sure that the page load has completed before you stop data collection or you'll only capture a partial trace.

4. Click on the extension's toolbar button  to load the tool and you'll be presented with the following extension popup window:



Select **Start** to begin collecting data for analysis.

What you'll see in the Page Diagnostics for SharePoint tool

1. Click the ellipses (...) in the top right corner of the tool to find the following links:
 - a. The **Additional resources** link provides general guidance and details regarding the tool including a link back to this article.
 - b. The **Give feedback** link provides a link to the *SharePoint Sites and Collaboration User Voice* site.
 - c. The **About** link includes the currently installed version of the tool and a direct link to the tool's third party notice.

2. The Correlation ID, SPRequestDuration, SPIISLatency, Page load time, and URL details are informational and can be used for a few purposes.

Page diagnostics for SharePoint

CorrelationID 5183039f-b0aa-1000-a23e-e0095bed0b95
SPRequestDuration 453ms
SPIISLatency 1ms
Page load time 3333ms
Page URL [https://\[REDACTED\].sharepoint.com/](https://[REDACTED].sharepoint.com/)

- **CorrelationID** is an important element when working with Microsoft Support as it allows them to gather more diagnostic data for the specific page.
- **SPRequestDuration** is the time taken for SharePoint to process the page. Structural navigation, large images, lots of API calls could all contribute to longer durations.
- **SPIISLatency** is the time in milliseconds taken for SharePoint begin loading the page. This value doesn't include the time taken for the web application to respond.
- **Page load time** is the total time recorded by the page from the time of the request to the time the response was received and rendered in the browser. This value is affected by various factors including network latency, the performance of the computer and the time it takes for the browser to load the page.
- The **Page URL** (Uniform Resource Locator) is the web address of the current page.

3. The **Diagnostic tests** tab displays the analysis results in three categories; **No action required**, **Improvement opportunities** and **Attention required**. Each test result is represented by an item in one of these categories as described in the following table:

[] Expand table

Category	Color	Description
Attention required	Red	Test result falls outside the baseline value and is affecting page performance. Follow remediation guidance.
Improvement opportunities	Yellow	Test result falls outside the baseline value and could be contributing to performance issues. Test-specific criteria may apply.
No action required	Green	Test result falls within the test's baseline value.

The screenshot shows the 'Page diagnostics for SharePoint' interface. At the top, there's a header with the title and a '...' button. Below the header, there are two tabs: 'Diagnostic tests' (which is selected) and 'Network trace'. The main content area is divided into three sections: 'Attention required', 'Improvement opportunities', and 'No action required'. Each section contains a list of items with icons and dropdown arrows.

Section	Item	Status
Attention required	Large images detected	Attention Required (Red)
	Content Delivery Network (CDN) check	Attention Required (Red)
	Requests to SharePoint	Attention Required (Red)
Improvement opportunities	Web parts using Iframes detected	Improvement Opportunity (Yellow)
No action required	Page weight under 500 KB	No Action Required (Green)
	No web parts impacting page load time	No Action Required (Green)

4. A **Network trace** tab provides details about page build requests and responses.

How to use the Diagnostic tests tab

When you analyze a SharePoint modern portal page or classic publishing site page with the Page Diagnostics for SharePoint tool, results are analyzed using predefined rules that compare results against baseline values and displayed in the **Diagnostic tests** tab. Rules for certain tests may use different baseline values for modern portal and classic publishing sites depending on how specific performance characteristics differ between the two.

Test results that appear in the **Improvement opportunities** or **Attention required** categories indicate areas that should be reviewed against recommended practices, and can be selected to display additional information about the result. Details for each item include a *Learn more* link, which will take you directly to the appropriate guidance related to the test. Test results that appear in the **No action required** category indicate compliance with the relevant rule and don't display additional details when selected.

The information in the Diagnostics tests tab won't tell you how to design pages, but will highlight factors that may impact page performance. Some page functionality and customizations have an unavoidable impact on page performance, and should be reviewed for potential remediation or omission from the page if their impact is substantial.

Red or yellow results may also indicate web parts that refresh data too frequently. For example, corporate news isn't updated every second but custom web parts are often built to fetch the latest news every second instead of implementing caching elements that could improve the overall user experience. Keep in mind when including web parts on a page that there are often simple ways to reduce their performance impact by evaluating the value of each available parameter to ensure it's set appropriately for its intended purpose.

Note

Classic team sites that don't have the publishing feature enabled cannot make use of CDNs. When you run the tool on these sites, the CDN test is expected to fail and can be ignored, but all of the remaining tests are applicable. The additional functionality of the SharePoint publishing feature can increase page load times, so it should not be enabled just to allow CDN functionality.

Important

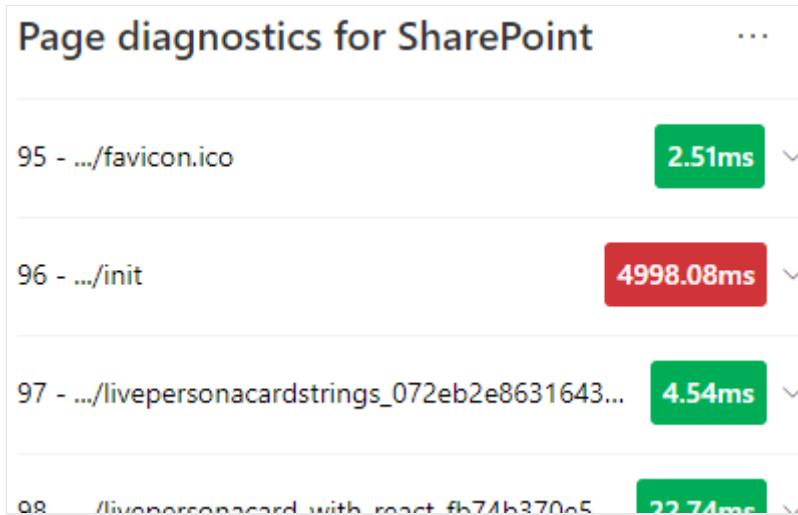
Test rules are added and updated regularly so please refer to the latest version of the tool for details about current rules and specific information included in test results. You can verify the version by managing your extensions and the extension will advise whether an update is available.

How to use the Network Trace tab and how to export a HAR file

The **Network Trace** tab provides detailed information about both requests to build the page and the responses received from SharePoint.

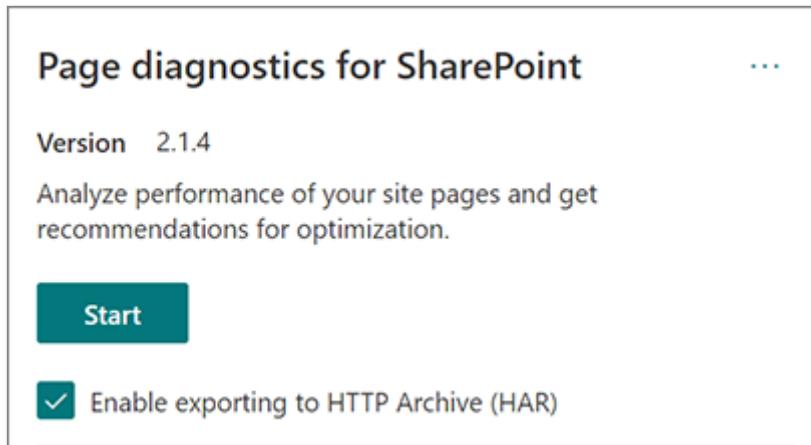
1. **Look for item load times flagged as red.** Each request and response is color coded to indicate its impact on overall page performance using the following latency metrics:
 - Green: < 500 ms

- Yellow: 500-1000 ms
- Red: > 1000 ms



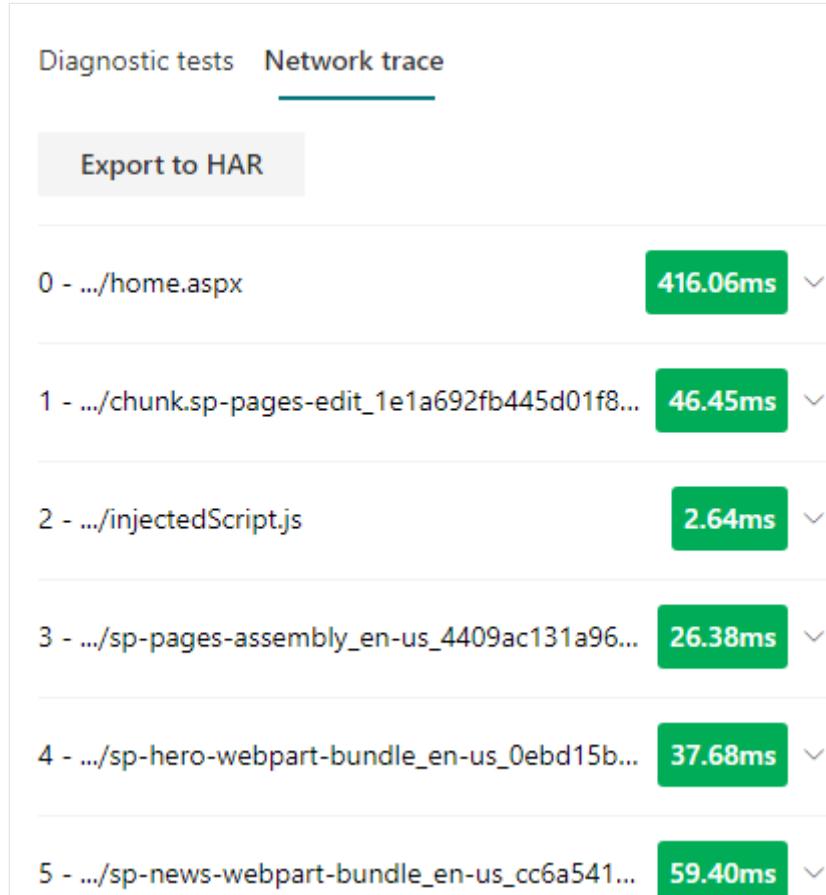
In the image shown above, the red item pertains to the default page. It will always show red unless the page loads in < 1000 ms (less than 1 second).

- Test item load times.** In some cases there will be no time or color indicator because the items have already been cached by the browser. To test this correctly, open the page, clear browser cache, and then click **Start** as that will force a "cold" page load and be a true reflection of the initial page load. This should then be compared to the "warm" page load as that will also help determine what items are being cached on the page.
- Share relevant details with others who can help investigate issues.** To share the details or information provided in the tool with your developers or a technical support person, using the **Enable exporting to HTTP Archive (HAR)** is the recommended approach.



Exporting should be enabled prior to clicking Start, which will then enable debug mode in your browser. This generates an HTTP Archive file (HAR) which can then be accessed through the "Network Trace" tab. Click the "Export to HAR" button to download the file

to your computer and you can then share it accordingly. The file can be opened in various debug tools, like F12 Developer Tools and Fiddler.



ⓘ Important

These results contain URLs and that can be classified as PII (Personally Identifiable Information). Make sure to follow your organization's guidelines before distributing that information.

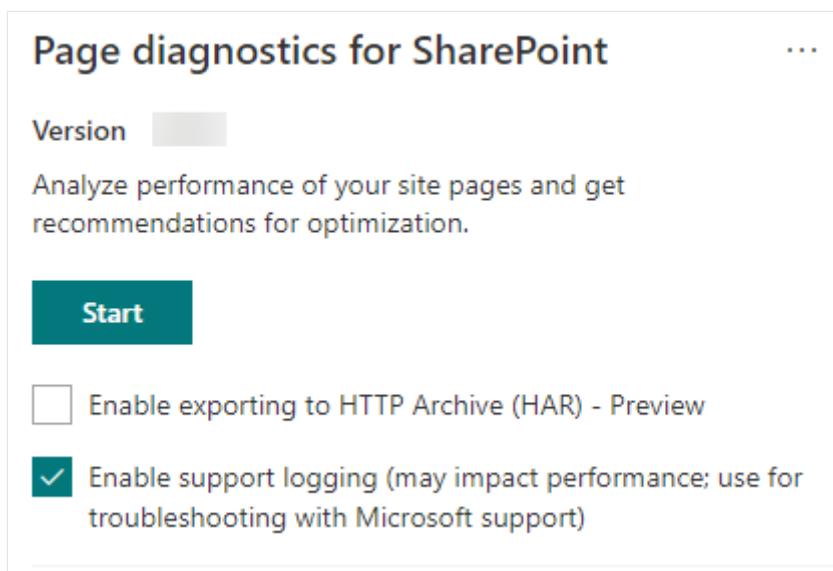
Engaging with Microsoft Support

We've included a **Microsoft Support level feature** that should only be utilized when working directly on a support case. Utilizing this feature will provide no benefit to you when used without support team engagement, and can make the page perform significantly slower. There's no additional information when using this feature in the tool as the additional information is added to the logging in the service.

No change is visible except that you'll be notified that you have enabled it and your page performance will be degraded by 2-3 times slower performance whilst enabled. It will only be relevant for the particular page and that active session. For this reason, this should be used sparingly and only when actively engaged with support.

To enable the Microsoft Support level feature

1. Open the Page Diagnostics for SharePoint tool.
2. On your keyboard, press **ALT-Shift-L**. This will display the **Enable support logging** check box.
3. Select the check box, and then click **Start** to reload the page and generate verbose logging.



You should note the CorrelationID (displayed at the top of the tool) and provide it to your support representative to enable them to gather additional information about the diagnostic session.

Related articles

[Tune SharePoint performance](#)

[Performance in the modern SharePoint experience](#)

[Content delivery networks](#)

[Use the Office 365 Content Delivery Network \(CDN\) with SharePoint](#)

Feedback

Was this page helpful?

Yes

No

[Provide product feedback ↗](#)

Tune Project Online performance

Article • 04/27/2023

With the launch of Project Online a few years ago, organizations of all sizes have been able to use Microsoft's rich set of Project Portfolio Management (PPM) capabilities within the convenience of our Office 365 cloud infrastructure.

Although one of the obvious benefits of using a cloud-based service is avoiding having to deal with deployment, setup, and hardware and software tuning, there are still some steps you can take to ensure your organization gets the best performance out of Project Online.

Project Online offers many configuration and customization settings, but customizations can have a performance impact. This article highlights the performance impact and tradeoffs of some of the most common Project Online settings, so you can make informed decisions when it comes to customizing and configuring Project Online.

This article is part of the [Network planning and performance tuning for Office 365](#) project.

Office 365 and SharePoint Online best practices

There is a wealth of information around network planning and performance tuning for [SharePoint Online](#) and [Office 365](#). All this information is relevant to Project Online customers and should be consulted in addition to the following best practices specific to Project Online.

Project Online configuration and customization

Many elements of a Project Web App site can be configured and customized, from administrative settings to permissions, and from collaboration settings to look-and-feel. Let's look at the settings that can potentially have an impact on the overall performance of your Project Web App site.

We will cover:

- Security permissions modes
- Enterprise Project Types
 - Project site configuration

- Synchronization mechanisms between Project Online and SharePoint Online
- Active Directory Resource Pool sync
- UI customization and look-and-feel
- Project Detail Pages (PDP) and workflows
- Event Handling
- OData and reporting
- Project Online quota

(Some of this information applies to Project Server 2013 and Project Server 2016 as well.)

Permission modes: SharePoint or Project

With Project Online and Project Server 2013, we introduced a new and simplified permission model called SharePoint permission mode, as opposed to the legacy Project permission mode. The comparison between both modes can be found on [Technet](#).

New Project Online instances are provisioned in SharePoint permission mode by default, and we are confident this mode will address the needs of the vast majority of customers. By using this mode, you can manage user authorization via regular SharePoint groups and permissions.

Project permission mode offers a high degree of customizability, but it can come at a price in terms of performance. If you create hundreds of categories and rely heavily on dynamic permissions via your Resource Breakdown Structure (RBS), it might slow down the end-user experience for users who have access to a lot of content, such as admins and portfolio managers.

Note

Switching between SharePoint permission mode and Project Server permission mode deletes all security-related settings. If you switch from SharePoint permission mode to classic Project Server permission mode, you have to manually configure your security permissions structure in Project Server 2013 and Project Server 2016. Switching from Project Server permission mode back to SharePoint permission mode deletes your security permissions information from Project Server 2013 and Project Server 2016.

Recommendation:

When possible, keep the default SharePoint permission mode for better overall performance. If you need to [use Project permission mode](#), limit your customizations as much as possible.

Enterprise Project Types

An [Enterprise Project Types ↗](#) (EPT) represents a wrapper that encapsulates phases, stages, a single workflow, and Project Detail Pages (PDPs).

EPTs also allow you to define:

- Project site configuration
- Synchronization mechanisms between Project Online and SharePoint Online

Project site configuration

Project sites are built on core SharePoint functionality. Creating project sites is not a lightweight process, and deciding if and when your organization might need project sites can go a long way in improving the overall end-user experience.

A lot of organizations use Project Online to collect and rate project proposals before deciding which projects to fund. If project sites are set to be automatically created the first time a project is published, then all project proposals, even the ones that don't make the cut, get a project site. These unnecessary sites would have to be manually cleaned up afterwards.

A better approach, if you decide to use project sites, is either letting the user choose when to create their collaboration site, or, even better, having it created by a workflow as soon as the project proposal reaches a certain stage gate.

SharePoint Online currently [SharePoint Online limits ↗](#) the number of subsites that can be created for each site collection. An EPT allows you to define which site collection to create new project sites in. This will allow you to create a project site for each project as you can span them across multiple site collections.

Project Online				
Projects up to 30,000	PWA	Marketing	Finance	Operations
Project sites one per project	Site 1	Site 1	Site 1	Site 1
	Site 2	Site 2	Site 2	Site 2
	Site 3	Site 3	Site 3	Site 3

For example, if you have a site collection dedicated to your IT department, you can configure your *IT Projects* EPT to create Project sites off of <https://contoso.sharepoint.com/sites/IT>.

Site Creation Location

We will create Project sites as subsites of this location

Location URL:

Recommendation:

If your organization uses project sites, select the option to create them on demand rather than automatically. This speeds up the first publishing experience and avoids creating unnecessary sites and content.

For each EPT, you can configure this option by:

1. In Project Web App Settings, click **Enterprise Project Types**.
2. Select the EPT to which you need to change the setting.
3. In the EPT settings page, in the **Project Site** section, select **Allow users to choose**.

Site Creation

Choose when a Project Site should be created.

If you select 'Allow users to choose', users will get the option to create a Project Site when they publish a project.

Automatically create a site on first publish

Allow users to choose

Do not create a site

Create project sites in their own site collection by the EPT. Keep the number of project sites in a site collection below the SharePoint Online [SharePoint Online limits](#).

What do you sync?

Project Online runs on top of SharePoint Online the same way Project Server runs on top of SharePoint Server. As a result, we have to keep in sync a certain number of components between two systems. These synchronizations can be time consuming and, depending on your business needs, can sometimes be unnecessary. This article

explores all these various synchronization systems to help you decide which ones you need and which ones you can safely turn off. Some of these settings are already off by default.

In the following sections, we discuss:

- Sync user permissions for your project site
- Sync SharePoint Tasks Lists for Enterprise projects

Sync User Permissions

Project Sites are workspaces where project teams can collaborate, upload documents, and raise issues. When sync user permissions is turned on, whenever a person is granted permission to a project, the corresponding Project site permissions are updated.

This synchronization happens every time the project is published. The tradeoff for the sync convenience is performance, e.g., the more users and sites that need to be synced, the slower the operation, especially if you're bulk publishing, importing or creating multiple projects (with Projects sites), or updating group memberships that will require a resync of project site permissions.

For each EPT, you can define if sync user permissions is turned on.

ⓘ Note

If project sites are created in a different site collection than where the Project Web App site is located (for example, <https://contoso.sharepoint.com/sites/pwa> is where Project Web App is located and the EPT is creating project sites in <https://contoso.sharepoint.com/sites/IT>), syncing user permissions is not supported.

Recommendation:

We strongly recommend that you disable the Project site permission sync option if the following is true of your deployment:

- You have a large number of resources (>1000)
- You have a large number of projects which require a Project site (>1000)
- You have a large number of resources that need to be granted access to the majority of Project sites

- Project sites are created outside of the default site collection (sync is disabled)

Here are some options to consider for managing your Project site permissions:

- If your project teams have low turnover, consider turning off Project site permission sync to improve Project Publish and Project Detail Pages performance. You would then have to manually grant or remove permission to your Project sites whenever someone joins or leaves a project team.
- If access needs to be granted for all users in PWA and it maps to your existing group permissions, consider configuring your Project sites to [inherit](#) from the parent PWA site.
- If site access aligns with specific roles, create one or more groups that map to those roles (possibly if you have Group sync enabled, you can use the same groups) and grant those groups access to the Project site.

For each EPT, you can turn on Sync User Permissions by:

1. In Project Web App Settings, click **Enterprise Project Types**.
2. Select the EPT to which you need to change the setting.
3. In the EPT settings page, in the **Synchronize** section, select **User Permission Sync**.

Synchronization

Turning on User Permissions Sync will grant project work resources permissions to the Project Site.

Note: Only Project Sites created inside of the Project Web App site will synchronize user permissions.

Synchronizing SharePoint Tasks Lists will copy tasks to the SharePoint Tasks List when the Enterprise Project Feature is activated. Only Project Sites created inside of the Project Web App site will synchronize tasks.

Note: SharePoint Tasks list will be read-only.

Sync User Permissions
 Sync SharePoint Tasks Lists

Sync SharePoint Tasks Lists for Enterprise projects

Sync SharePoint Tasks Lists is turned off by default to improve the speed of project publishing. This also helps speed the transition between Project Detail Pages. If your users rely on the task list and its timeline visualization in the Project site, you can turn this feature on and check if its impact on the performance of project publishing is reasonable.

 **Note**

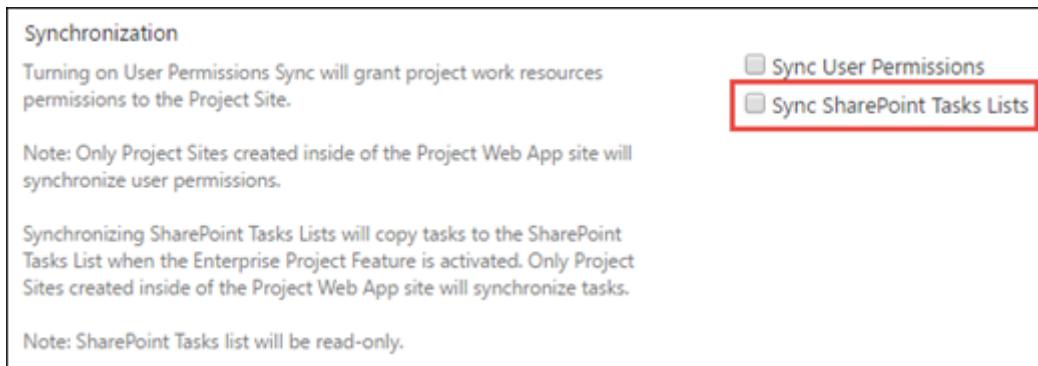
If project sites are created in a different site collection than where the Project Web App site is located (for example, <https://contoso.sharepoint.com/sites/pwa> is where Project Web App is located and the EPT is creating project sites in <https://contoso.sharepoint.com/sites/IT>), syncing SharePoint Tasks Lists is not supported.

Recommendation

The Sync SharePoint Task Lists option was intended for use with small project plans. If the project has a large number of tasks, syncing them on publish will take some time as each task needs to be updated one at a time. For example, it takes several minutes to sync a 500 task project plan to the SharePoint task list. Even though the queue job is on a separate correlation and does not block saving and editing of the project plan, we recommend not enabling the Sync SharePoint Task Lists option. We recommend only syncing projects with less than 250 tasks.

This option is turned off by default. Only turn SharePoint Tasks Lists sync on if your users need the feature for each EPT. To configure this option:

1. In Project Web App Settings, click **Enterprise Project Types**.
2. Select the EPT to which you need to change the setting.
3. In the EPT settings page, in the **Synchronize** section, select **Sync SharePoint Tasks Lists**.



Active Directory Resource Pool sync

Active Directory Resource Pool sync by itself does not have particular performance issues and can import thousands of resources into your Project Web App instance in minutes. However, its downstream effect on other parts of the system can impact performance. The primary process to keep an eye on is the resource permission sync previously mentioned. If there is large turnover in your Active Directory groups

membership, and that requires you to sync your Resource Pool often, monitor any potential downstream effects on related permission sync jobs.

Recommendation:

Limit Active Directory sync to groups of resources that actually need to use the system, and monitor any potential permission issues after the synchronization of large groups. (To configure Active Directory Enterprise Resource Pool Synchronization, in Project Web App Settings, click [Active Directory Resource Pool Synchronization](#).

PWA pages and views customizations

Page customizations

The SharePoint platform offers great customization capabilities with its modular webpart infrastructure and support for custom pages. When you add logos, custom webparts, and new themes, it might not have a significant impact on performance on an on-premises infrastructure due to the benefits of server proximity, low latency, and high bandwidth networks. However, on an online service, the story is different.

When you upload a logo or graphic with a large file size, it might slow down pages a bit on an on-premises deployment, but online, the performance hit on page loads is substantial.

The same principle applies when you add multiple webparts to a page. It might be tempting to have a custom page with multiple webparts, but unless users actually need to see the data side by side, it is better to have separate specialized pages than having it all in one place. If users only need the content of one webpart on the page, they still have to wait longer for the page to load and display the data for all the other webparts.

Recommendation:

When you customize pages, treat your Project Online site as any regular Internet website, and create lightweight pages as much as possible.

Views customizations

Here again, simplicity goes a long way to improving page load performance. Organizations can create custom views by using multiple Project Web App pages, including Project Center, Resource Center, Tasks, and Timesheets.

The more content is displayed, the slower page rendering will be. You can reduce each page load time by a few seconds if you provide users with a greater number of simple and targeted views rather than a few "all-in-one" views.

In the examples below, the second view takes an average of 2 to 3 seconds less to load than the first one.

This screenshot shows a complex view of the Project Center in Office 365. On the left, a navigation bar includes 'Office 365' and 'Projects' tabs, along with links for 'BROWSE', 'PROJECTS', 'SHARE', 'FOLLOW', and a search bar. The main area is titled 'Project Center' and displays a detailed grid of project data. The grid columns include 'Project Name', 'Project Department', 'Project Health', 'Risk Rating', 'ROI', 'Total Cost', and 'Total Benefits'. The data is categorized into four groups: 'Type: Infrastructure & Dev', 'Type: Marketing Campaign', 'Type: Merger & Acquisition', and 'Type: New Product Develop'. Each group contains several specific projects like 'Apparel ERP Upgrade', 'Hub Upgrade', etc. To the right of the grid is a Gantt chart showing tasks from January to October 2015. The chart has a blue background with green vertical bars representing task progress.

This screenshot shows a simplified view of the Project Center in Office 365. The layout is similar to the previous one, with the 'Office 365' and 'Projects' tabs at the top. The main area is titled 'Project Center' and displays a grid of project names. The grid columns include 'Projektname' and three ellipsis columns. To the right of the grid is a Gantt chart showing tasks from March 9, 2015, to April 5, 2015. The chart has a blue background with green vertical bars representing task progress.

Recommendation:

When you configure views, offer users simple specialized views for faster navigation rather than a complex all-in-one view that would load unnecessary data most of the time.

User View Settings

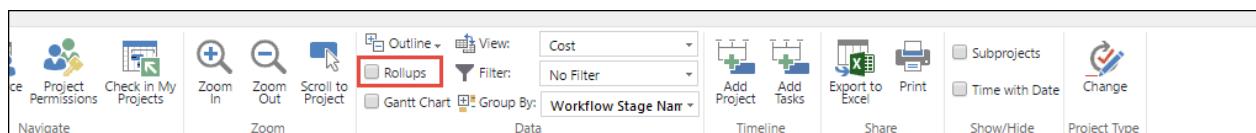
Project Center: Group by with Rollups

Users can configure different ways to have the view rendered to them including having data grouped by different fields. When using **group by**, data can be rolled up for supported aggregation fields (for example, summing costs or a custom field). Computing these aggregate values requests the service to load up all the values in order to display the total.

	Project Name	Health	Schedul	Cost	Start ↑	Finish	Cost	Baseline Cost	Business Unit
	- Workflow Phase Name:				9/19/2016	6/28/2017	\$582,420.00	\$582,420.00	
	CFO Campaign	...			9/19/2016	5/12/2017	\$176,800.00	\$176,800.00	1 - Upstream
	Tax Checker	...			1/31/2017	6/28/2017	\$405,620.00	\$405,620.00	7 - Finance
	- Workflow Phase Name: 1. Create				2/2/2017	2/2/2018	\$9,345,072.40	\$9,235,472.40	
	IT HR Rebuild	...			2/2/2017	8/4/2017	\$384,580.00	\$384,580.00	5 - IT
	Helmet with integrated sunvisor	...			2/13/2017	2/2/2018	\$3,914,542.40	\$3,893,102.40	3 - Functions
	Apparel ERP Upgrade	...			3/1/2017	8/30/2017	\$3,085,350.00	\$3,085,350.00	3 - Functions
	Print Advertising Campaign	...			3/27/2017	10/25/2017	\$630,800.00	\$542,640.00	5 - IT
	Hub Upgrade	...			4/3/2017	11/22/2017	\$613,400.00	\$613,400.00	2 - Downstream
	Catalog Publishing	...			4/6/2017	1/10/2018	\$716,400.00	\$716,400.00	5 - IT

Recommendation:

Unless the user needs to see the rolled up values, disable the **Rollup** option in the ribbon.



The screenshot shows the Project Center ribbon with several tabs: Home, Insert, Project, Permissions, Check in My Projects, Navigate, Zoom, Data, Timeline, Share, Show/Hide, and Project Type. The 'Data' tab is selected. Within the 'Data' tab, there is a 'Group By' dropdown set to 'Workflow Stage Name'. A red box highlights the 'Rollups' button in the ribbon bar above the 'Data' tab.

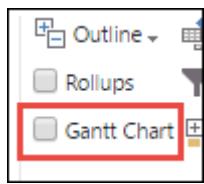
	Project Name ↑	Start	Finish	% Complete	Work	Duration	Other
	- Workflow Stage Name:						
	CFO Campaign	...	9/19/2016	5/12/2017	0%	4,140h	170d
	Tax Checker	...	1/31/2017	6/28/2017	0%	1,532h	107d

Project Center: Gantt Chart

The chart portion of the Gantt Chart view displays each project as a summary Gantt bar.

Recommendation:

Unless the user needs to see the Gantt, disable the **Gantt Chart** option in the ribbon.



Custom Project Detail Pages and Workflows

In addition to the recommendation provided above for page design, Project Detail Pages (PDPs) are particular in that they can trigger a recalculation of the entire project and kick off workflow actions, both of which can be expensive operations in terms of performance, depending on your customizations.

Project Online and Project Server have two main update processes for project information:

- Updates requiring a scheduling recalculation (see list below)
- Nonschedule-related fields, such as project name, description, and owner.

We recommend that you avoid updating both types of data on the same PDP to avoid triggering both update processes at the same time.

Here is a list of the most common actions that require a schedule recalculation.

- Project calendar changes
- Changes to the following date fields:
 - Start date
 - Finish date
 - Status date
 - Current date
- Changes in project custom fields
- If the project has any dependencies on deliverables

A second way to improve PDP performance is to reduce the number of webparts and custom fields displayed on each PDP. If your business processes require frequent updates to the same set of fields, create a dedicated PDP with only these fields to

improve load and save time. Displaying all custom fields at all times results in a lot of unnecessary overhead.

Recommendation:

Create lightweight specialized PDPs, and avoid mixing schedule-related and nonschedule-related updates.

Bulk custom fields updates in workflows with new REST API

Updating project custom fields values in a workflow one at a time requires a separate server request using the Set Project Field action. This results in reduced performance when updating a lot of custom fields at the same time on a high-latency, low-bandwidth network.

To solve this issue, there is a [CSOM method to update custom fields in bulk](#). This method requires you to pass in a dictionary containing the name and values of all the custom fields you want to update.

API for provisioning project sites on-demand

Each project can have its own dedicated SharePoint site where team members can collaborate, share documents, and raise issues. These sites can be automatically created on first publish or manually created by the project manager via Project Pro or the administrator via Project Web App settings, or they can simply be disabled.

You can use the [CreateProjectSite\(""\) method](#) to decide when to create their project sites. This is particularly useful for organizations who want to create their sites only after a project proposal reaches a specific stage in a predefined workflow, rather than on first publish. This significantly improves the performance of project creation by postponing the creation of Project sites.

Event Handling

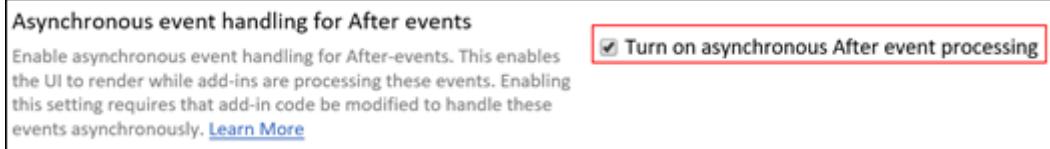
Add-ins can respond to events being raised in Project Online. For example, an add-in can perform some additional activity after a project has been created. Users may have to wait for these add-ins to complete handling the events before they can continue working with Project Online.

Recommendation:

Project Online should be configured to handle certain events asynchronously to minimize the amount of time users will need to wait. To do this, ask the developer of any add-ins you use to make sure their code is able to handle After events asynchronously. They can go to [this article](#) to learn more about practices they can follow for handling these events.

If the developer confirms the add-in is ready for the change, you then need to enable the **Turn on asynchronous After event processing** setting on your **PWA Settings** page.

1. On your **PWA Settings** page, in the **Operational Policies** section, select **Additional Server Settings**.
2. In the **Asynchronous event handling for After events** section, make sure that **Turn on asynchronous After event processing** is selected.



3. Select **Save**.

You'll then need to test your instances to verify that everything works correctly.

 **Note**

This setting can only be seen and changed by the Site Collection Administrator.

OData and Reporting

ProjectData OData Service

Project Online has an OData reporting service that provides a way to build reporting/visualization on the data stored in the service. The ProjectData OData reporting service API is defined [here](#).

Calls to the ProjectData OData reporting service are governed by SharePoint Online. Please review the article [Avoid getting throttled or blocked in SharePoint Online](#) to ensure that the calls are less likely to be throttled and to correctly implement retry and exponential back off recommendations.

In addition, following the recommendations outlined in this document will reduce the number, length and frequency of calls needed to retrieve data. If throttling is occurring often, check across the organization as multiple departments could be querying the same data or not following the best practices outlined in this article and affecting everyone.

Timephased Reporting

In Project Online you can choose the level of granularity you need for timephased reporting data. The options and impact of the levels are fully documented in [Configure rollup of timephased reporting data in Project Online](#). Choosing a level that generates the least amount of data for your scenarios will allow the data to be visible in OData Reporting service endpoint faster and will reduce the amount of time it will take to download.

The list of options in order of performance (from most to least performant correlating to the amount of data generated):

- Never
- Fiscal Periods
- Monthly
- Weekly
- Daily

Fiscal Periods has the big advantage over *Monthly* in that reporting data is only held for defined Fiscal Periods, whereas *Monthly* will hold data for the full duration across all of your projects.

By using the Project OData service, you can extract information from your Project Online instance for reporting.

Recommendation:

Store the least amount of timephased data that is consistent with your business needs. Do not use Daily if you have workflows that wait on publish to complete. Daily can take significant time to generate the required data causing workflows to wait.

Querying the service

There are [limits](#) to the number of entities that can be returned in one query of the ProjectData OData service. As a result, querying a large amount of data requires multiple web requests to be sent to the service, adding network overhead and latency for each request.

Recommendation:

Avoid performing full “refresh everything” data loads. These refreshes can impact performance of the PWA site especially during peak use times leading to overall performance degradation of user operations in PWA or throttling.

Perform Odata refresh actions after hours. Decisions to maintain real time or close to real reports should also take into consideration the performance tradeoffs to the user experience in the PWA site. If “refresh everything” requirements exist, please review the “SQL Server Integration Services (SSIS) – Recommended for large datasets” section.

For a Project Web App instance that contains a large number of entities, such as projects, assignments, or tasks, you should limit the data returned in at least one of the following ways. If you don't limit the data returned, the query can exceed the default limits and affect server performance.

- **Always use a \$filter URL option and \$select to limit the data.** For example, the following query filters by project start date and returns only four fields, in order of the project name:

HTTP

```
http://ServerName/ProjectServerName/_api/ProjectData/Projects?  
$filter=ProjectStartDate gt datetime'2012-01-  
01T00:00:00'& $orderby=ProjectName& $select=ProjectName,ProjectSt  
artDate,ProjectFinishDate,ProjectCost
```

- **Avoid Custom Fields that are multi-value lookups.** Extra computation is required to process custom field values which are multi-value lookups. These fields are not able to take advantage of several optimizations that have been implemented for more common customer scenarios. If multi value custom fields have already been configured, improve the lookup speed and reliability by ensuring that none of those fields are specified in your filtered Odata query.

- **Querying entities by key or association.** When querying entities, refer to the metadata document at

```
https://yourdomain.sharepoint.com/sites/PWA/_api/ProjectData/$metadata.
```

Whenever possible query the entity in one of the following ways:

- Keys

(!) Note

If there is more than one key, using the first key will perform better than only using the second key.

- Associations

For example, you can query the [Assignment](#) entity via AssignmentId and ProjectId:

HTTP

```
https://ServerName/ProjectServerName/_api/ProjectData/Assignments?  
$filter=AssignmentId eq guid'719d849a-79b4-e911-b073-00155d9c3d12' and  
ProjectId eq guid'b5b02399-79b4-e911-b073-00155d9c3d12'
```

or

```
https://ServerName/ProjectServerName/_api/ProjectData/Assignments(Assig  
nmentId=guid'719d849a-79b4-e911-b073-  
00155d9c3d12',ProjectId=guid'b5b02399-79b4-e911-b073-00155d9c3d12')
```

via AssignmentId:

HTTP

```
https://ServerName/ProjectServerName/_api/ProjectData/Assignments?  
$filter=AssignmentId eq guid'719d849a-79b4-e911-b073-00155d9c3d12'
```

via ProjectId:

HTTP

```
https://ServerName/ProjectServerName/_api/ProjectData/Assignments?  
$filter= ProjectId eq guid'b5b02399-79b4-e911-b073-00155d9c3d12'
```

via association via Project:

HTTP

```
https://ServerName/ProjectServerName/_api/ProjectData/Projects(guid'263  
fc8d7-427c-e111-92fc-00155d3ba208')/Assignments
```

- Do multiple queries to return data one page at a time, by using the \$top operator and the \$skip operator in a loop. For example, the following query gets Issues 11 through 20 for all projects, in order of the resource who is assigned to the issue:

```
HTTP
```

```
https://ServerName/ProjectServerName/\_api/ProjectData/Issues?  
\$skip=10& \$top=10& \$orderby=AssignedToResource
```

- Avoid retrieving the Project/Task/Resource name when querying the Assignment Entity. The service performs additional processing to retrieve the respective names. If the data has already been retrieved from other queries, do not include it in the \$select filter when querying Assignment.

Recommendation:

- Limit the amount of data you query at runtime by using server-side filtering to retrieve only the columns that you need. The impact of this is most noticeable with custom fields. Add in the custom fields only if you need them.
- Ensure that you are filtering on the entity key. The entity key is indexed and will offer a much more performant data retrieval experience. You can find the key(s) for each entity by reviewing the Service Metadata Document in your PWA instance:
[https://Contoso.sharepoint.com/sites/PWA/_api/ProjectData/\\$metadata ↗](https://Contoso.sharepoint.com/sites/PWA/_api/ProjectData/$metadata)

Retrieving Data and Building Reports

PowerBI

If the amount of data is small, then Power BI can regularly read data from the Project OData service and help provide a variety of dynamics reports. A sample content pack can be found [here ↗](#).

If the amount of data in Project Online is large, you can still bring in a subset of the data as long as it meets the PowerBI data size limits outlined [here ↗](#). Another option is to create your reports in a moving window, i.e., filtering projects who were active in the last 30 days or viewing resource capacity for the next 6 months. Review the \$filter/\$select section for best practices as PowerBI may not take advantage of the service-side filtering optimizations.

Excel OData

Excel can be used to download data and build custom visualizations/reports. If the amount of data in Project Online is large, a subset of the data can be using a moving window, i.e., filtering projects who were active in the last 30 days or viewing resource capacity for the next 6 months. Review the \$filter/\$select section for best practices as Excel may not take advantage of the service-side filtering optimizations.

SQL Server Integration Services (SSIS)

Using SSIS, Project Online reporting data can be downloaded from the Project OData service into a local SQL server database or into Microsoft Azure. Once downloaded, any reports/visualizations can be authored. A further process is needed to keep the local data in sync with Project Online.

When using SSIS, use the following pattern that Project Online has been optimized for. The pattern will reduce the amount of time it takes to retrieve and keep the local data in sync. Further only download the fields that are needed to perform the business requirements. The fewer the fields being queried, the quicker the data can be retrieved.

Full Sync

Retrieve the current snapshot of the reporting data you are interested in. Use the following method to efficiently retrieve [Project](#) and related entities.

For example, using the [Project](#) entity.

1. Query the ProjectId from the Project entity including any additional filters. For example, filter on projects that have specific start or finish dates.
2. Query the Project entity specifying the fields that need to be downloaded, filtering on a single ProjectId that was previously retrieved. Include the ProjectModifiedDate as it is used in the delta sync pattern below.
3. Repeat step 2 for each ProjectId. In addition, for each ProjectId, download the data for related entities.

For example, using [Task](#) entity:

1. Query on the TaskId from Task entity filtering on any additional fields as well as the project ProjectId from the previous step.
2. Query the Task entity specifying the fields that need to be downloaded and filtering on a single TaskId that was previously retrieved. Include the TaskModifiedDate as it is used in the delta sync pattern below.
3. Repeat for each TaskId.

Similarly, use the same approach for each related entity, e.g., [Assignment](#), [TaskTimephasedData](#)

The preceding steps apply to other groups of entities, for example, when retrieving timesheet information:

- [Timesheet](#): Retrieve the TimesheetId and ModifiedDate based on filter criteria , then Timesheet records, then [TimeSheetLines](#) filtering on the TimeSheetId and continue on to other related entities, ensuring that you're filering by primary key Ids (TimesheetUID) and modification date fields.

When retrieving Resource entity information:

- Retrieve the ResourceId and ResourceModifiedDate, then [Resource](#) records, then [ResourceTimephasedData](#) etc. Include the respective primary key Ids and modification dates fields.

Delta Sync

Check periodically to keep the local copy of the reporting data up to date. Repeat the steps below as needed for the respective group of entitles, e.g., Timesheet, Resource...

1. Query all the ProjectId's and modification date from the Project endpoint using \$filter criteria.
2. Delete local project and related records (Tasks, Assignments, etc.) where the ProjectId no longer exists.
3. Where the service modification date and the local modification date are different for the project record, query the Project endpoint for all the required fields filtering on a single ProjectId at a time. In addition, for each ProjectId, download the data for related entities.

For example, using [Task](#) entity:

1. Query on the TaskId and TaskModifiedDate from Task entity filtering on any additional fields as well as the project ProjectId from the previous step where the data has changed, i.e., Project service modification date didn't match the local modification date.
2. Delete local and related records for TaskId that no longer exists.
3. Where the service modification date and the local modification date are different, query the respective entity endpoint passing in TaskId and entity primary key and update the local version.

Repeat for each related entity, e.g., Assignment, TaskTimephasedData.

Project Web App Quota

By default, the Project Web App Site comes with a 25GB limit and is separate from the [limit on all data stored in the SharePoint site collection](#) where Project Web App is enabled. Using the reporting granularity options to reduce your data volume can help in staying within the quota.

ⓘ Note

PWA quota can be increased (in increments) to a maximum of 100 GB. A new PWA site will be required once the quota limit has been reached. Increases beyond 50GB require that the PWA site no longer use the [daily timephased reporting granularity](#) option. To discuss increasing the PWA site quota, please contact Microsoft.

Conclusion

Project Online, like any cloud service running on the Internet, requires specific tuning to deliver the best performance compared with an on-premises deployment.

Although we are constantly improving the system to speed up performance, there are some steps you can take in the meantime to provide a good experience to your end users.

Summary recommendation:

- Use SharePoint permission mode when possible.
- Only turn on the features you will actually use.
- Keep pages and customization as simple and lightweight as possible for faster page load times.
- Use server-side filtering or export Odata feeds data to a SQL Server database for more reporting flexibility.
- Choose a reporting granularity option that uses the least amount of data that satisfies your reporting needs.

Related Topics

[Project Online: software boundaries and limits](#)

Performance troubleshooting plan for Office 365

Article • 04/12/2024

Do you need to know the steps to take to identify and fix lags, hangs, and slow performance between SharePoint, OneDrive, Exchange Online, or Skype for Business Online, and your client computer? Before you call support, this article can help you troubleshoot Office 365 performance issues and even fix some of the most common issues.

This article is actually a sample action plan that you can use to capture valuable data about your performance issue as it's happening. Some top issues are also included in this article.

If you're new to network performance and want to make a long term plan to monitor performance between your client machines and Office 365, take a look at [Office 365 performance tuning and troubleshooting - Admin and IT Pro](#).

Sample performance troubleshooting action plan

This action plan contains two parts; a preparation phase, and a logging phase. If you have a performance problem right now, and you need to do data collection, you can start using this plan right away.

Prepare the client computer

- Find a client computer that can reproduce the performance problem. This computer will be used during troubleshooting.
- Write down the steps that cause the performance problem to happen so you're ready when it comes time to test.
- Install tools for gathering and recording information:
 - Install [Netmon 3.4](#) (or use an equivalent network tracing tool).
 - Install the free Basic Edition of [HTTPWatch](#) (or use an equivalent network Tracing tool).
 - Use a screen recorder or run the Steps Recorder (PSR.exe) that comes with Windows Vista and later, in order to keep a record of the steps you take during testing.

Log the performance issue

- Close all extraneous Internet browsers.
- Start the Steps Recorder, or another screen recorder.
- Start your Netmon capture (or network tracing tool).
- Clear your DNS cache on the client computer from the command line by typing ipconfig /flushdns.
- Start a new browser session and turn on HTTPWatch.
- Optional: If you're testing Exchange Online, run the Exchange Client Performance Analyzer tool from the Office 365 admin console.
- Reproduce the exact steps that cause the performance issue.
- Stop your Netmon or other tool's trace.
- At the command line, run a trace route to your Office 365 subscription by typing the following command and then pressing ENTER:

```
Windows Command Prompt
```

```
tracert <subscriptionname>.onmicrosoft.com
```

- Stop the Steps Recorder and save the video. Be sure to include the date and time of the capture and whether it demonstrates good or bad performance.
- Save the trace files. Again, be sure to include the date and time of the capture and whether it demonstrates good or bad performance.

If you're not familiar with running the tools mentioned in this article, don't worry because we provide those steps next. If you're accustomed to doing this kind of network capturing, you can skip to [How to collect baselines](#), which describes filtering and reading the logs.

Flush the DNS Cache first

Why? By flushing out the DNS cache, you're starting your tests with a clean slate. By clearing the cache, you're resetting the DNS resolver contents to the most up-to-date entries. Remember that a flush doesn't remove HOST file entries. If you use HOST file entries extensively, you should copy those entries out to a file in another directory and then empty the HOST file.

Flush your DNS resolver cache

1. Open the command prompt, (either **Start > Run > cmd** or **Windows key > cmd**).
2. Type the following command and press ENTER:

```
Windows Command Prompt
```

```
ipconfig /flushdns
```

Netmon

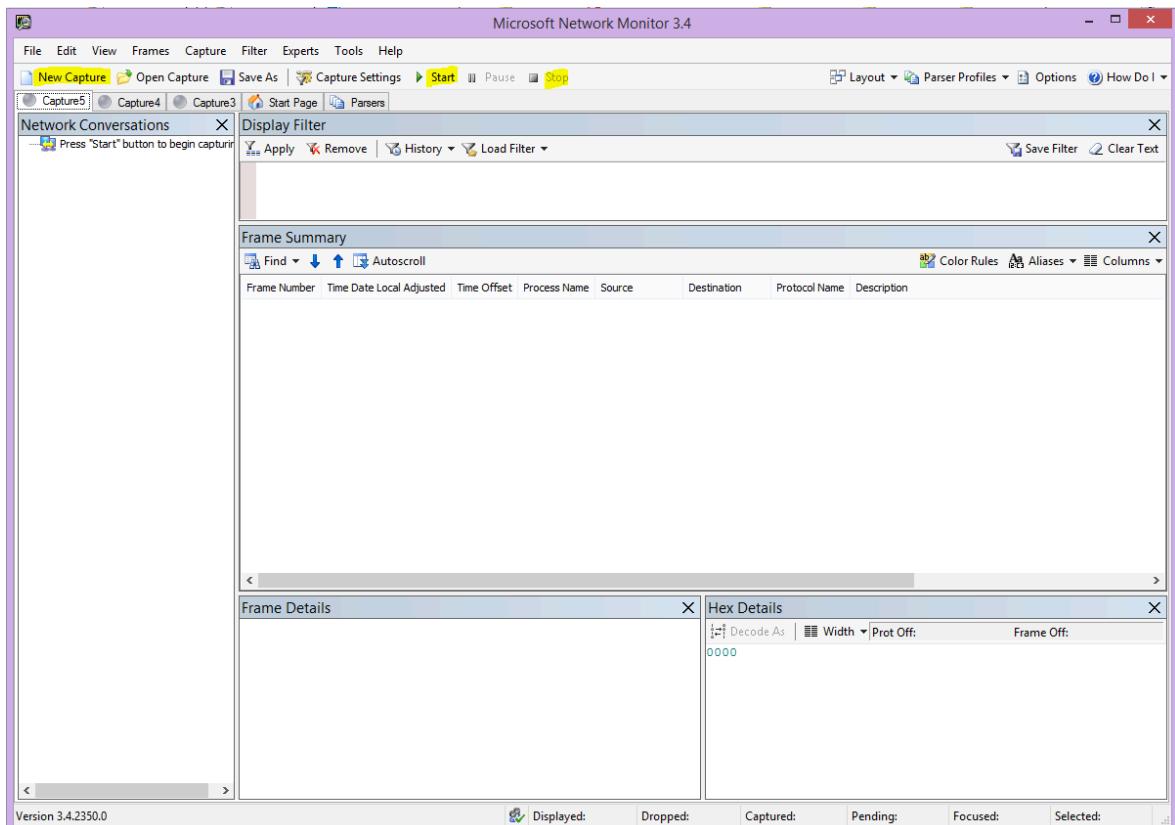
Microsoft's Network Monitoring tool ([Netmon](#)) analyzes packets (network traffic) that passes between computers on networks. By using Netmon to trace traffic with Office 365 you can capture, view, and read packet headers, identify intervening devices, check important settings on network hardware, look for dropped packets, and follow the flow of traffic between computers on your corporate network and Office 365. Because the actual body of the traffic is encrypted, that is, it travels on port 443 via SSL/TLS, you can't read the files being sent. Instead, you get an unfiltered trace of the path that the packet takes which can help you track down the problem behavior.

Be sure you don't apply a filter at this time. Instead, run through the steps and demonstrate the problem before stopping the trace and saving.

After you install Netmon 3.4, open the tool and take these steps:

Take a Netmon trace and reproduce the issue

1. Launch Netmon 3.4. There are three panes on the **Start** page: **Recent Captures**, **Select Networks**, and the **Getting Started with Microsoft Network Monitor 3.4**. **Notice**. The Select Networks panel will also give you a list of the default networks from which you can capture. Be sure that network cards are selected here.
2. Click **New Capture** at the top of the **Start** page. This adds a new tab beside the **Start** page tab called **Capture 1**.



3. To take a simple capture, click **Start** on the toolbar.
4. Reproduce the steps that present a performance issue.
5. Click **Stop** > **File** > **Save As**. Remember to give the date and time with the time zone and to mention if it demonstrates bad or good performance.

HTTPWatch

[HTTPWatch](#) comes in charged, and a free edition. The free Basic Edition covers everything you need for this test. HTTPWatch monitors network traffic and page load time right from your browser window. HTTPWatch is a plug-in to Microsoft Edge that graphically describes performance. The analysis can be saved and viewed in HTTPWatch Studio.

Note

If you use another browser, such as Firefox, Google Chrome, or if you can't install HTTPWatch in Edge, open a new browser window and press F12 on your keyboard. You should see the Developer Tool pop-up at the bottom of your browser. If you use Opera, press CTRL+SHIFT+I for Web Inspector, then click the **Network** tab and complete the testing outlined below. The information will be slightly different, but

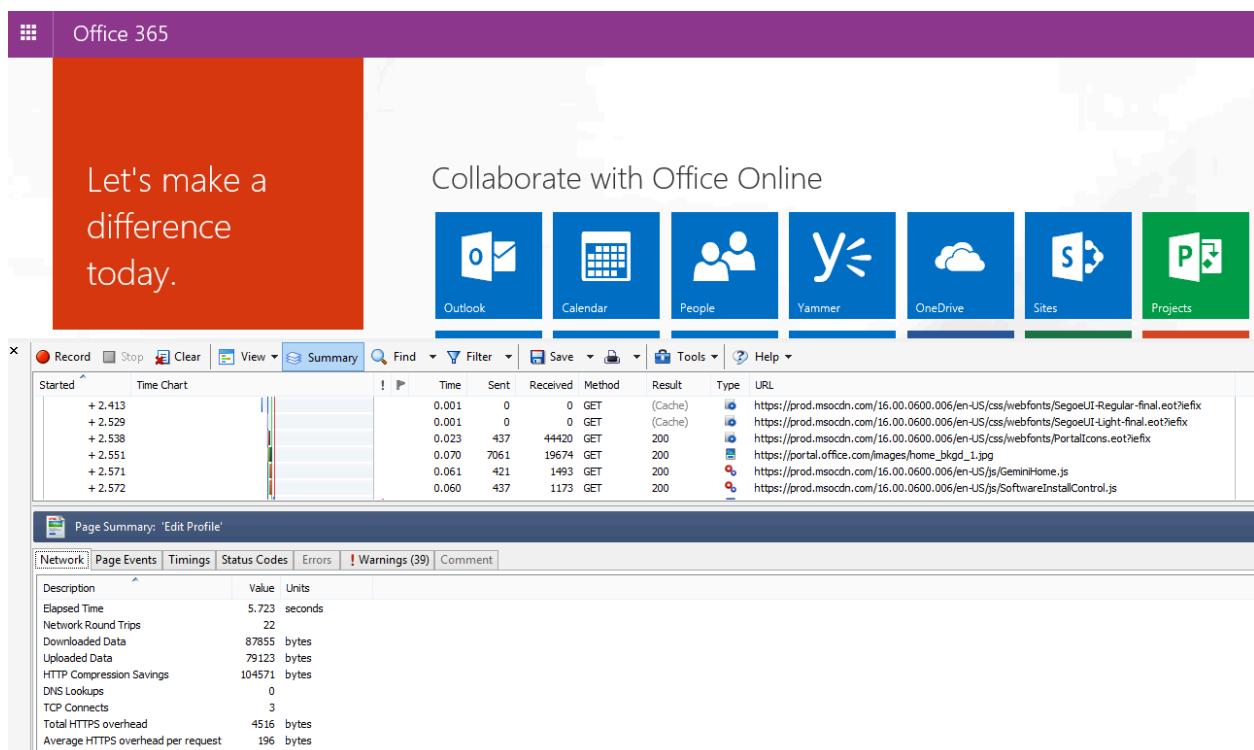
load times will still be displayed in milliseconds. > HTTPWatch is also very useful for issues with SharePoint page load times.

Run HTTPWatch and reproduce the issue

HTTPWatch is a browser plug-in, so exposing the tool in the browser is slightly different for each version of Microsoft Edge. Typically, you can find HTTPWatch under the Commands bar in the Microsoft Edge browser. If you don't see the HTTPWatch plug-in in your browser window, check the version of your browser by clicking **Help > About**, or in later versions of Microsoft Edge, click the gear symbol and **About Edge**. To launch the **Commands bar**, right-click the menu bar in Microsoft Edge and click **Commands bar**.

In the past, HTTPWatch has been associated with both the Commands and the Explorer bars, so once you install, if you don't immediately see the icon (even after reboot) check **Tools**, and your toolbars for the icon. Remember that toolbars can be customized and options can be added to them.

1. Launch HTTPWatch in an Microsoft Edge browser window. It appears docked to the browser at the bottom of that window. Click **Record**.
2. Reproduce the exact steps involved in the performance issue. Click the **Stop** button in HTTPWatch.
3. **Save the HTTPWatch or Send by Email**. Remember to name the file so that it includes date and time information and an indication of whether your Watch contains a demonstration of good or bad performance.



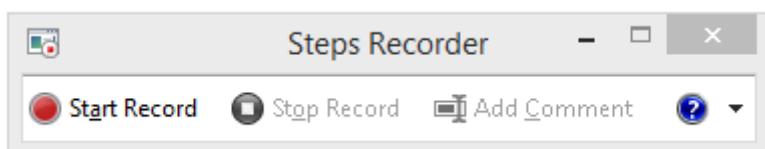
This screenshot is from the Professional version of HTTPWatch. You can open traces taken in the Basic Version on a computer with a Professional version and read it there. Extra information might be available from the trace through that method.

Problem Steps Recorder

Steps Recorder, or PSR.exe, allows you to record issues as they're occurring. It's a very useful tool and simple to run.

Run Problem Steps Recorder (PSR.exe) to record your work

1. Either use **Start > Run > type PSR.exe > OK**, or, click the **Windows Key > type PSR.exe >** and then press **ENTER**.
2. When the small PSR.exe window appears, click **Start Record** and reproduce the steps that reproduce the performance issue. You can add comments as needed, by clicking **Add Comments**.
3. Click **Stop Record** when you've completed the steps. If the performance issue is a page render, wait for the page to render before you stop the recording.
4. Click **Save**.



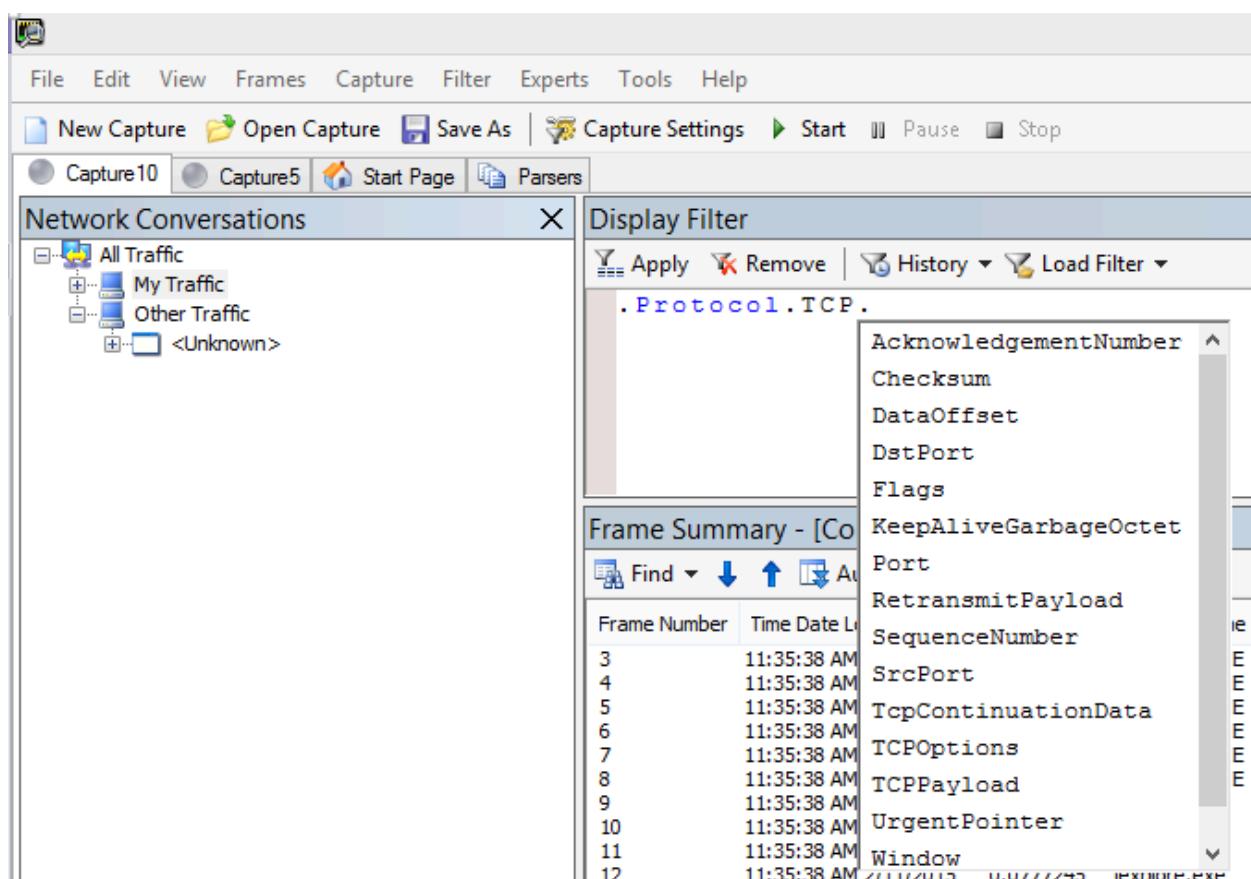
The date and time is recorded for you. This links your PSR to your Netmon trace and HTTPWatch in time, and helps with precision troubleshooting. The date and time in the PSR record can show that a minute passed between the sign in and browsing of the URL and the partial render of the admin site, for example.

Read your traces

It isn't possible to teach everything about network and performance troubleshooting that someone would need to know via an article. Getting good at performance takes experience, and knowledge of how your network works and usually performs. But it's possible to round up a list of top issues and show how tools can make it easier for you to eliminate the most common problems.

If you want to pick up skills reading network traces for your Office 365 sites, there's no better teacher than creating traces of page loads regularly and gaining experience reading them. For example, when you have a chance, load an Office 365 service and trace the process. Filter the trace for DNS traffic, or search the FrameData for the name of the service you browsed. Scan the trace to get an idea of the steps that occur when the service loads. This helps you learn what normal page load should look like, and in the case of troubleshooting, particularly around performance, comparing good to bad traces can teach you a lot.

Netmon uses Microsoft Intellisense in the Display filter field. Intellisense, or intelligent code completion, is that trick where you type in a period and all available options are displayed in a drop-down selection box. For example, you're worried about TCP window scaling, you can find your way to a filter (such as `.protocol.tcp.window < 100`) by this means.



Netmon traces can have a lot of traffic in them. If you aren't experienced with reading them, it's likely you'll be overwhelmed opening the trace the first time. The first thing to do is separate the signal from the background noise in the trace. You tested against Office 365, and that's the traffic you want to see. If you're used to navigating through traces, you might not need this list.

Traffic between your client and Office 365 travels via TLS, which means that the body of the traffic will be encrypted and not readable in a generic Netmon trace. Your performance analysis doesn't need to know the specifics of the information in the

packet. It is, however, very interested in packet headers and the information that they contain.

Tips to get a good trace

- Know the value of the IPv4 or IPv6 address of your client computer. You can get this from the command prompt by typing **IPConfig** and then pressing ENTER. Knowing this address lets you tell at a glance whether the traffic in the trace directly involves your client computer. If there's a known proxy, ping it and get its IP address as well.
- Flush your DNS resolver cache and, if possible, close all browsers except the one in which you're running your tests. If you aren't able to do this, for instance, if support is using some browser-based tool to see your client computer's desktop, be prepared to filter your trace.
- In a busy trace, locate the Office 365 service that you're using. If you have never or seldom seen your traffic before, this is a helpful step in separating the performance issue from other network noise. There are a few ways to do this. Directly before your test, you can use *ping* or *PsPing* against the URL of the specific service (`ping outlook.office365.com` or `psping -4 microsoft-my.sharepoint.com:443`, for example). You can also easily find that *ping* or *PsPing* in a Netmon trace (by its process name). That will give you a place to start looking.

If you're only using Netmon tracing at the time of the problem, that's okay too. To orient yourself, use a filter like `ContainsBin(FrameData, ASCII, "office")` or `ContainsBin(FrameData, ASCII, "outlook")`. You can record your frame number from the trace file. You might also want to scroll the *Frame Summary* pane all the way to the right and look for the Conversation ID column. There's a number indicated there for the ID of this specific conversation that you can also record and look at in isolation later. Remember to remove this filter before applying any other filtering.

💡 Tip

Netmon has a lot of helpful built-in filters. Try the **Load Filter** button at the top of the *Display* filter pane.

```

C:\Perf>psping outlook.office365.com:443
PsPing v2.01 - PsPing - ping, latency, bandwidth measurement utility
Copyright <C> 2012-2014 Mark Russinovich
Sysinternals - www.sysinternals.com

TCP connect to 2a01:111:f400:1428::2:443:
5 iterations <warmup 1> connecting test:
Connecting to 2a01:111:f400:1428::2:443 <warmup>: 5.80ms
Connecting to 2a01:111:f400:1428::2:443: 5.98ms
Connecting to 2a01:111:f400:1428::2:443: 6.24ms
Connecting to 2a01:111:f400:1428::2:443: 6.20ms
Connecting to 2a01:111:f400:1428::2:443: 6.43ms

TCP connect statistics for 2a01:111:f400:1428::2:443:
  Sent = 4, Received = 4, Lost = 0 <0% loss>,
    Minimum = 5.98ms, Maximum = 6.43ms, Average = 6.21ms

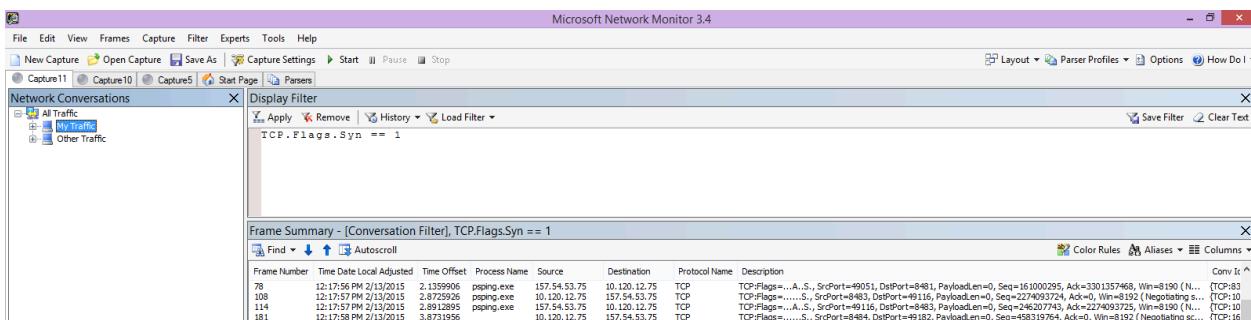
C:\Perf>psping -4 outlook.office365.com:443
PsPing v2.01 - PsPing - ping, latency, bandwidth measurement utility
Copyright <C> 2012-2014 Mark Russinovich
Sysinternals - www.sysinternals.com

TCP connect to 132.245.92.34:443:
5 iterations <warmup 1> connecting test:
Connecting to 132.245.92.34:443 <warmup>: 251.65ms
Connecting to 132.245.92.34:443: 9.12ms
Connecting to 132.245.92.34:443: 9.33ms
Connecting to 132.245.92.34:443: 9.15ms
Connecting to 132.245.92.34:443: 8.44ms

TCP connect statistics for 132.245.92.34:443:
  Sent = 4, Received = 4, Lost = 0 <0% loss>,
    Minimum = 8.44ms, Maximum = 9.33ms, Average = 9.01ms

C:\Perf>

```



Get familiar with your traffic, and learn to locate the information you need. For example, learn to determine which packet in the trace has the first reference to the Office 365 service you're using (like "Outlook").

Taking Office 365 Outlook Online as an example, the traffic begins something like this:

- DNS Standard Query and DNS Response for outlook.office365.com with matching QueryIDs. It's important to note the time offset for this turn-around, and where in the world the Office 365 Global DNS sends the request for name resolution. Ideally, as locally as possible, rather than halfway across the world.
- An HTTP GET Request whose status report Moved Permanently (301)
- RWS Traffic including RWS Connect requests and Connect replies. (This is Remote Winsock making a connection for you.)

- A TCP SYN and TCP SYN/ACK conversation. Many settings in this conversation impact your performance.
- Then a series of TLS:TLS traffic, which is where the TLS handshake and TLS certificate conversations take place. (Remember the data is encrypted via SSL/TLS.)

All parts of the traffic are important and connected, but small portions of the trace contain information important in terms of performance troubleshooting, so we'll focus on those areas. Also, since we've done enough Office 365 performance troubleshooting at Microsoft to compile a Top 10 list of common problems, we'll focus on those issues and how to use the tools we have to root them out next.

If you haven't installed them already, the matrix below makes use of several tools where ever possible. Links are provided to the installation points. The list includes common network tracing tools like [Netmon](#) and [Wireshark](#), but use any tracing tool you're comfortable with, and in which you're accustomed to filtering network traffic. When you're testing, remember:

- *Close your browsers, and test with only one browser running* - This will reduce the overall traffic you capture. It makes for a less busy trace.
- *Flush your DNS resolver cache on the client computer* - This will give you a clean slate when you start to take your capture, for a cleaner trace.

Common issues

Some common issues you might face and how to find them in your Network trace.

TCP Windows Scaling

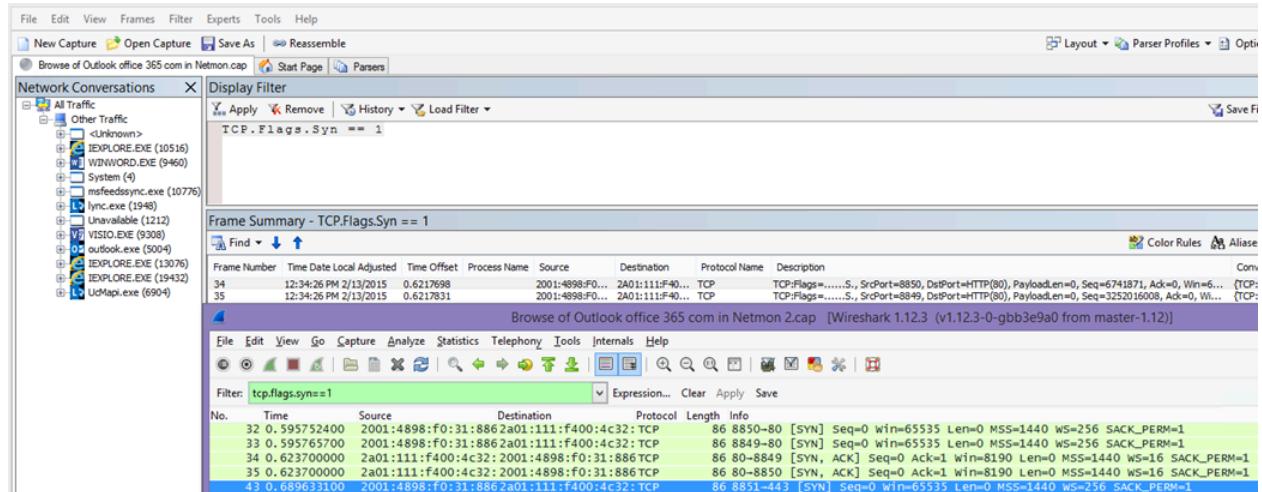
Found in the SYN - SYN/ACK. Legacy or aging hardware might not take advantage of TCP windows scaling. Without proper TCP windows scaling settings, the default 16-bit buffer in TCP headers fills in milliseconds. Traffic can't continue to send until the client receives an acknowledgment that the original data has been received, causing delays.

Tools

- Netmon
- Wireshark

What to look for

Look for the SYN - SYN/ACK traffic in your network trace. In Netmon, use a filter like `tcp.flags.syn == 1`. This filter is the same in Wireshark.



Notice that for every SYN there's a source port (SrcPort) number that is matched in the destination port (DstPort) of the related Acknowledgment (SYN/ACK).

To see the Windows Scaling value that is used by your network connection, expand first the SYN, and then the related SYN/ACK.

Frame Details	
Frame: Number = 34, Captured Frame Length = 86, MediaType = ETHERNET	
Ethernet: Etype = IPv6, DestinationAddress:[00-00-5E-00-02-0D], SourceAddress:[78-2B-CB-8A-82-65]	SYN
IPv6: Next Protocol = TCP, Payload Length = 32	
Tcp: Flags=....S., SrcPort=8850, DstPort=HTTP(80), PayloadLen=0, Seq=6741871, Ack=0, Win=65535 (Negotiating scale factor 0x8) = 65535	
Frame Details	
Frame: Number = 37, Captured Frame Length = 86, MediaType = ETHERNET	
Ethernet: Etype = IPv6, DestinationAddress:[78-2B-CB-8A-82-65], SourceAddress:[10-F3-11-63-00-47]	ACK
IPv6: Next Protocol = TCP, Payload Length = 32	
Tcp: Flags=...A..S., SrcPort=HTTP(80), DstPort=8850, PayloadLen=0, Seq=2792161571, Ack=6741872, Win=8190 (Negotiated scale factor 0x4) = 131040	

TCP Idle Time Settings

Historically, most perimeter networks are configured for transient connections, meaning idle connections are generally terminated. Idle TCP sessions can be terminated by proxies and firewalls at greater than 100 to 300 seconds. This is problematic for Outlook Online because it creates and uses long-term connections, whether they're idle or not.

When connections are terminated by proxy or firewall devices, the client isn't informed, and an attempt to use Outlook Online will mean a client computer will try, repeatedly, to revive the connection before making a new one. You might see hangs in the product, prompts, or slow performance on page load.

Tools

- Netmon
- Wireshark

What to look for

In Netmon, look at the Time Offset field for a round-trip. A round-trip is the time between client sending a request to the server and receiving a response back. Check between the Client and the egress point (ex. Client --> Proxy), or the Client to Office 365 (Client --> Office 365). You can see this in many types of packets.

As an example, the filter in Netmon may look like `.Protocol.I Pv4.Address == 10.102.14.112 AND .Protocol.I Pv4.Address == 10.201.114.12`, or, in Wireshark, `ip.addr == 10.102.14.112 && ip.addr == 10.201.114.12`.

Tip

Don't know if the IP address in your trace belongs to your DNS server? Try looking it up at the command line. Click **Start > Run >** and type **cmd**, or press **Windows Key >** and type **cmd**. At the prompt, type `nslookup <the IP address from the network trace>`. To test, use nslookup against your own computer's IP address. To see a list of Microsoft's IP ranges, see [Office 365 URLs and IP address ranges](#).

If there's a problem, expect long Time Offsets to appear, in this case (Outlook Online), particularly in TLS:TLS packets that show the passage of Application Data (for example, in Netmon you can find application data packets via `.Protocol.TLS AND Description == "TLS:TLS Rec Layer-1 SSL Application Data"`). You should see a smooth progression in the time across the session. If you see long delays when refreshing your Outlook Online, this could be caused by a high degree of resets being sent.

Latency/Round Trip Time

Latency is a measure that can change a lot depending on many variables, such as upgrading aging devices, adding a large number of users to a network, and the percentage of overall bandwidth consumed by other tasks on a network connection.

There are bandwidth calculators for Office 365 available from this [Network planning and performance tuning for Office 365](#) page.

Need to measure the speed of your connection, or your ISP connection's bandwidth? Try this site (or sites like it): [Speedtest Official Site](#), or query your favorite search engine for the phrase **speed test**.

Tools

- Ping
- PsPing
- Netmon
- Wireshark

What to look for

To track latency in a trace, you'll benefit from having recorded the client computer IP address and the IP address of the DNS server in Office 365. This is for easier trace filtering. If you connect through a proxy, you'll need your client computer IP address, the proxy/egress IP address, and the Office 365 DNS IP address, to make the work easier.

A ping request sent to outlook.office365.com will tell you the name of the datacenter receiving the request, even if ping *might* not be able to connect to send the trademark consecutive ICMP packets. If you use PsPing (a free tool for download), and specific the port (443) and perhaps to use IPv4 (-4) you'll get an average round-trip-time for packets sent. This will work this for other URLs in the Office 365 services, like `psping -4 yourSite.sharepoint.com:443`. In fact, you can specify a number of pings to get a larger sample for your average, try something like `psping -4 -n 20 yourSite-my.sharepoint.com:443`.

Note

PsPing doesn't send ICMP packets. It pings with TCP packets over a specific port, so you can use any one you know to be open. In Office 365, which uses SSL/TLS, try attaching port :443 to your PsPing.

```

C:\Perf>
C:\Perf>ping outlook.office365.com
Pinging outlook-namnorthandwest.office365.com [2a01:111:f400:2c40::2] with 32 bytes
of data:
Request timed out.

Ping statistics for 2a01:111:f400:2c40::2:
  Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
Control-C
^C
C:\Perf>psping -4 outlook.office365.com:443
PsPing v2.01 - PsPing - ping, latency, bandwidth measurement utility
Copyright (C) 2012-2014 Mark Russinovich
Sysinternals - www.sysinternals.com

TCP connect to 132.245.92.194:443:
5 iterations (warmup 1) connecting test:
Connecting to 132.245.92.194:443 (warmup): 6.48ms
Connecting to 132.245.92.194:443: 6.66ms
Connecting to 132.245.92.194:443: 6.34ms
Connecting to 132.245.92.194:443: 6.47ms
Connecting to 132.245.92.194:443: 6.61ms

TCP connect statistics for 132.245.92.194:443:
  Sent = 4, Received = 4, Lost = 0 (0% loss),
  Minimum = 6.34ms, Maximum = 6.66ms, Average = 6.52ms

C:\Perf>

```

If you loaded the slow performing Office 365 page while doing a network trace, you should filter a Netmon or Wireshark trace for `DNS`. This is one of the IPs we're looking for.

Here are the steps to take to filter your Netmon to get the IP address (and take a look at DNS Latency). This example uses `outlook.office365.com`, but may also use the URL of a SharePoint tenant (`hithere.sharepoint.com` for example).

1. Ping the URL `ping outlook.office365.com` and, in the results, record the name and IP address of the DNS server the ping request was sent to.
2. Network trace opening the page, or doing the action that gives you the performance problem, or, if you see a high latency on the ping, itself, network trace it.
3. Open the trace in Netmon and filter for DNS (this filter also works in Wireshark, but is sensitive to case `-- dns`). Since you know the name of the DNS server from your ping you may also filter more speedily in Netmon like this: `DNS AND ContainsBin(FrameData, ASCII, "namnorthandwest")`, which looks like this in Wireshark dns and frame contains "namnorthandwest".
Open the response packet and, in the Netmon **Frame Details** window, click **DNS** to expand for more information. In the DNS information, you'll find the IP address of the DNS server the request went to in Office 365. You'll need this IP address for the next step (the PsPing tool). Remove the filter, right-click on the DNS Response in Netmon (**Frame Summary > Find Conversations > DNS**) to see the DNS Query and Response side-by-side.
4. In Netmon, also note the Time Offset column between the DNS Request and Response. In the next step, the easy-to-install and use [PsPing](#) tool comes in very

handy, both because ICMP is often blocked on Firewalls, and because PsPing elegantly tracks latency in milliseconds. PsPing completes a TCP connection to an address and port (in our case open port 443).

5. Install PsPing.
6. Open a command prompt (Start > Run > type cmd, or Windows Key > type cmd) and change directory to the directory where you installed PsPing to run the PsPing command. In my examples you can see I made a 'Perf' folder on the root of C. You can do the same for quick access.
7. Type the command so that you're making your PsPing against the IP address of the Office 365 DNS server from your earlier Netmon trace, including the port number, like `psping -n 20 132.245.24.82:445`. This will give you a sampling of 20 pings and average the latency when PsPing stops.

If you're going to Office 365 through a proxy server, the steps are a little different. First, PsPing to your proxy server to get an average latency value in milliseconds to proxy/egress and back, and then either run PsPing on the proxy, or on a computer with a direct Internet connection to get the missing value (the one to Office 365 and back).

If you choose to run PsPing from the proxy, you'll have two millisecond values: Client computer to proxy server or egress point, and proxy server to Office 365. And you're done! Well, recording values, anyway.

If you run PsPing on another client computer that has a direct connection to the Internet, that is, without a proxy, you'll have two millisecond values: Client computer to proxy server or egress point, and client computer to Office 365. In this case, subtract the value of client computer to proxy server or egress point from the value of client computer to Office 365, and you'll have the RTT numbers from your client computer to the proxy server or egress point, and from proxy server or egress point to Office 365.

However, if you can find a client computer in the impacted location that is directly connected, or bypasses the proxy, you may choose to see if the issue reproduces there to begin with, and test using it thereafter.

Latency, as seen in a Netmon trace, those extra milliseconds can add up, if there are enough of them in any given session.

Frame Summary - [Conversation Filter]									
	Find ▾	▼	▲						
Frame Number	Time Date Local Adjusted	Time Offset	Time Delta	Process Name	Source	Destination	Protocol Name	Description	
2	12:16:32 PM 3/4/2015	0.0000000	0.0000000	IEXPLORE.EXE	10.164.114.89	10.190.224.84	TCP	TCP:Flags=CE...S., SrcPo	
3	12:16:32 PM 3/4/2015	0.2598509	0.2598509	IEXPLORE.EXE	10.190.224.84	10.164.114.89	TCP	TCP:Flags=..A..S., SrcPo	
4	12:16:32 PM 3/4/2015	0.2606875	0.0008366	IEXPLORE.EXE	10.164.114.89	10.190.224.84	TCP	TCP:Flags=...A..., SrcPo	
5	12:16:32 PM 3/4/2015	0.2612543	0.0005668	IEXPLORE.EXE	10.164.114.89	10.190.224.84	HTTP	HTTP:Request, GET http://	
6	12:16:32 PM 3/4/2015	0.5527667	0.2915124	IEXPLORE.EXE	10.190.224.84	10.164.114.89	HTTP	HTTP:Response, HTTP/1.	
7	12:16:32 PM 3/4/2015	0.5527667	0.0000000	IEXPLORE.EXE	10.190.224.84	10.164.114.89	TCP	TCP:[Continuation to #6]	
8	12:16:32 PM 3/4/2015	0.5528663	0.0000996	IEXPLORE.EXE	10.164.114.89	10.190.224.84	TCP	TCP:Flags=...A..., SrcPo	
9	12:16:32 PM 3/4/2015	0.8402279	0.2873616	IEXPLORE.EXE	10.190.224.84	10.164.114.89	TCP	TCP:[Continuation to #6]	
10	12:16:32 PM 3/4/2015	0.8402279	0.0000000	IEXPLORE.EXE	10.190.224.84	10.164.114.89	TCP	TCP:[Continuation to #6]	
11	12:16:32 PM 3/4/2015	0.8403318	0.0001039	IEXPLORE.EXE	10.164.114.89	10.190.224.84	TCP	TCP:Flags=...A..., SrcPo	
12	12:16:32 PM 3/4/2015	0.8406364	0.0003046	IEXPLORE.EXE	10.164.114.89	10.190.224.84	HTTP	HTTP:Request, GET http://	
13	12:16:32 PM 3/4/2015	0.8406364	0.0000000	IEXPLORE.EXE	10.164.114.89	10.190.224.84	TCP	TCP:[Continuation to #21]	
14	12:16:32 PM 3/4/2015	0.8406364	0.0000000	IEXPLORE.EXE	10.164.114.89	10.190.224.84	TCP	TCP:[Continuation to #12]	

ⓘ Note

Your IP address may be different than the IPs shown here, for example, your ping may return something more like 157.56.0.0/16 or a similar range. For a list of ranges used by Office 365, check out [Office 365 URLs and IP address ranges](#).

Remember to expand all the nodes (there's a button at the top for this) if you want to search for, for example, 132.245.

Proxy Authentication

This only applies to you if you're going through a proxy server. If not, you can skip these steps. When working properly, proxy authentication should take place in milliseconds, consistently. You shouldn't see intermittent bad performance during peak usage periods (for example).

If Proxy authentication is on, each time you make a new TCP connection to Office 365 to get information, you need to pass through an authentication process behind the scenes. So, for example, when switching from Calendar to Mail in Outlook Online, you'll authenticate. And in SharePoint, if a page displays media or data from multiple sites or locations, you'll authenticate for each different TCP connection that is needed in order to render the data.

In Outlook Online, you might experience slow load times whenever you switch between Calendar and your mailbox, or slow page loads in SharePoint. However, there are other symptoms not listed here.

Proxy authentication is a setting on your egress proxy server. If it's causing a performance issue with Office 365, you must consult your networking team.

Tools

- Netmon

- Wireshark

What to look for

Proxy authentication takes place whenever a new TCP session must be spun up, commonly to request files or info from the server, or to supply info. For example, you might see proxy authentication around HTTP GET or HTTP POST requests. If you want to see the frames where you're authenticating requests in your trace, add the 'NTLMSSP Summary' column to Netmon and filter for `.property.NTLMSSPSummary`. To see how long the authentication is taking, add the Time Delta column.

To add a column to Netmon:

1. Right-click on a column such as **Description**.
2. Click **Choose Columns**.
3. Locate *NTLMSSP Summary* and *Time Delta* in the list and click **Add**.
4. Move the new columns into place before or behind the *Description* column so you can read them side-by-side.
5. Click **OK**.

Even if you don't add the column, the Netmon filter will work. But your troubleshooting will be much easier if you can see what stage of authentication you're in.

When looking for instances of Proxy Authentication, be sure to study all frames where there's an NTLM Challenge, or an Authenticate Message is present. If necessary, right-click the specific piece of traffic and Find Conversations > TCP. Be aware of the Time Delta values in these Conversations.

Frame Summary - [Conversation Filter]						
	Frame Number	Time Date Local Adjusted	Time Offset	Time Delta	Process Name	NTLMSSP Summary
	2943	9:14:02 AM 2/27/2015	16.9582094	0.0000000	outlook.exe	{TCP:468, IPv4:467}
	2948	9:14:02 AM 2/27/2015	17.0323365	0.0741271	outlook.exe	{TCP:468, IPv4:467}
	2949	9:14:02 AM 2/27/2015	17.0330259	0.0006894	outlook.exe	{TCP:468, IPv4:467}
	2950	9:14:02 AM 2/27/2015	17.0337605	0.0007346	outlook.exe	NTLM NEGOTIATE MESSAGE, Workstation N...
	2955	9:14:02 AM 2/27/2015	17.1084402	0.0746797	outlook.exe	{HTTP:472, TCP:468, IPv4:467}
	2956	9:14:02 AM 2/27/2015	17.1167295	0.0082893	outlook.exe	NTLM CHALLENGE MESSAGE
	2957	9:14:02 AM 2/27/2015	17.1167809	0.0000514	outlook.exe	{HTTP:472, TCP:468, IPv4:467}
	2958	9:14:02 AM 2/27/2015	17.1192755	0.0024946	outlook.exe	NTLM AUTHENTICATE MESSAGEVersion:v2, ...

A four-second delay in proxy authentication as seen in Wireshark. The **Time delta from previous displayed frame** column was made via right-clicking the field of the same

name in the frame details and selecting Add as Column.

Time	Source	Time delta from previous displayed frame	Destination	Protocol	Info
9 0.127317300	10.190.224.120	0.000390100	10.164.114.89	TCP	[TCP segment of a reassembled PDU]
10 0.127317300	10.190.224.120	0.000000000	10.164.114.89	HTTP	HTTP/1.1 407 Proxy Authentication Required (Forefront TMG requires authorization
11 0.127354100	10.164.114.89	0.000036800	10.190.224.120	TCP	60299-8080 [ACK] Seq=565 Ack=4556 Win=262144 Len=0
12 0.251045900	10.164.114.89	0.123691800	10.190.224.120	TCP	[TCP segment of a reassembled PDU]
13 0.251045900	10.164.114.89	0.000000000	10.190.224.120	TCP	[TCP segment of a reassembled PDU]
14 0.251045900	10.164.114.89	0.000000000	10.190.224.120	TCP	[TCP segment of a reassembled PDU]
15 0.251045900	10.164.114.89	0.000000000	10.190.224.120	TCP	[TCP segment of a reassembled PDU]
16 0.251045900	10.190.224.120	0.000751500	10.164.114.89	TCP	8080-60299 [ACK] Seq=4556 Ack=6405 Win=131328 Len=0
17 0.251837200	10.164.114.89	0.000039800	10.190.224.120	TCP	[TCP segment of a reassembled PDU]
18 0.251837200	10.164.114.89	0.000000000	10.190.224.120	TCP	[TCP segment of a reassembled PDU]
19 0.251837200	10.164.114.89	0.000000000	10.190.224.120	TCP	[TCP segment of a reassembled PDU]
20 0.251837200	10.164.114.89	0.000000000	10.190.224.120	HTTP	GET http://www.bing.com/ HTTP/1.1
21 0.252528000	10.190.224.120	0.000690800	10.164.114.89	TCP	8080-60299 [ACK] Seq=4556 Ack=9325 Win=131328 Len=0
22 0.252528000	10.190.224.120	0.000000000	10.164.114.89	TCP	8080-60299 [ACK] Seq=4556 Ack=10842 Win=131328 Len=0
23 4.220500000	10.190.224.120	3.967972000	10.164.114.89	TCP	[TCP segment of a reassembled PDU]
24 4.220579100	10.164.114.89	0.000079100	10.190.224.120	TCP	60299-8080 [ACK] Seq=10842 Ack=5254 Win=261376 Len=0
25 4.361238800	10.190.224.120	0.140659700	10.164.114.89	TCP	[TCP segment of a reassembled PDU]
26 4.361317500	10.164.114.89	0.000078700	10.190.224.120	TCP	60299-8080 [ACK] Seq=10842 Ack=6714 Win=262144 Len=0
27 4.361383400	10.190.224.120	0.000065900	10.164.114.89	TCP	[TCP segment of a reassembled PDU]
28 4.361383400	10.190.224.120	0.000000000	10.164.114.89	TCP	[TCP segment of a reassembled PDU]

DNS Performance

Name resolution works best and most quickly when it takes place as close to the client's country/region as possible.

If DNS name resolution is taking place overseas, it can add seconds to page loads. Ideally, name resolution happens in under 100 ms. If not, you should do further investigation.

Tip

Not sure how Client Connectivity works in Office 365? Take a look at the Client Connectivity Reference document [here](#).

Tools

- Netmon
- Wireshark
- PsPing

What to look for

Analyzing DNS performance is typically another job for a network trace. However, PsPing is also helpful in ruling in, or out, a possible cause.

DNS traffic is based on TCP and UDP requests and responses are clearly marked with an ID that will help to match a specific request with its specific response. You'll see DNS traffic when, for example, SharePoint uses a network name or URL on a web page. As a rule of thumb, most of this traffic, except when transferring Zones, runs over UDP.

In both Netmon and Wireshark, the most basic filter that will let you look at DNS traffic is simply `dns`. Be sure to use lower case when specifying the filter. Remember to flush

your DNS resolver cache before you begin to reproduce the issue on your client computer. For example, if you have a slow SharePoint page load for the Home page, you should close all browsers, open a new browser, start tracing, flush your DNS resolver cache, and browse to your SharePoint site. Once the entire page resolves, you should stop and save the trace.

cal Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
/25/2015 14:7454102			10.222.120.24	10.120.12.114	DNS	DNS:QueryId = 0x6153, QUERY (Standard query), Response - Success,
/25/2015 15.0606288			10.120.12.114	10.222.120.24	DNS	DNS:QueryId = 0xC582, QUERY (Standard query), Query for prod.msocdn.com of type AAAA on class
/25/2015 15.0646496			10.222.120.24	10.120.12.114	DNS	DNS:QueryId = 0xC582, QUERY (Standard query), Response - Success, 2600:1409:A:388:0:0:0:1D8E
/25/2015 15.2505381			10.120.12.114	10.222.120.24	DNS	DNS:QueryId = 0x659, QUERY (Standard query), Query for outlook.office365.com of type Host Addr
/25/2015 15.2508051			10.120.12.114	10.222.120.24	DNS	DNS:QueryId = 0x5B08, QUERY (Standard query), Query for outlook.office365.com of type AAAA on class
/25/2015 15.2544294			10.222.120.24	10.120.12.114	DNS	DNS:QueryId = 0x659, QUERY (Standard query), Response - Success, 132.245.81.146, 157.56.239.1
/25/2015 15.2560364			10.222.120.24	10.120.12.114	DNS	DNS:QueryId = 0x5B08, QUERY (Standard query), Response - Success, 2A01:111:F400:2C2C:0:0:0:1

You want to look at the time offset here. And it might be helpful to add the **Time Delta** column to Netmon which you can do by completing these steps:

1. Right-click on a column such as **Description**.
2. Click **Choose Columns**.
3. Locate *Time Delta* in the list and click **Add**.
4. Move the new column into place before or behind the *Description* column so you can read them side-by-side.
5. Click **OK**.

If you find a query of interest, consider isolating it by right-clicking that query in the frame details panel, choosing **Find Conversations > DNS**. Notice that the Network Conversations panel jumps right to the specific conversation in its log of UDP traffic.

Fra...	Time Date Local Adjusted	Time Offset	Time Delta	P..	Source	Destination	Protocol...	Description
3260	11:04:21 AM 2/26/2015	14.2613303	0.0000000		10.120.12.114	10.222.120.24	DNS	DNS:QueryId = 0x4FC3, QUERY (Standard query), Query for outlook.office365.com
3263	11:04:21 AM 2/26/2015	14.2654494	0.0041191		10.222.120.24	10.120.12.114	DNS	DNS:QueryId = 0x4FC3, QUERY (Standard query), Response - Success, 132.245.64.

In Wireshark, you can make a column for DNS time. Take your trace (or open a trace) in Wireshark and filter by `dns`, or, more helpfully, `dns.time`. Click on any DNS query, and, in the panel showing details, expand the `Domain Name System (response)` details. You'll see a field for time (for example, `[Time: 0.001111100 seconds]`). Right-click this time and select **Apply as Column**. This will give you a **Time** column for quicker sorting of your

trace. Click on the new column to sort by descending values to see which DNS call took the longest to resolve.

A browse of SharePoint filtered in Wireshark by (lowercase) dns.time, with the time from the details made into a column and sorted ascending.

If you would like to do more investigation of the DNS resolution time, try a PsPing against the DNS port used by TCP (for example, `psping <IP address of DNS server>:53`). Do you still see a performance issue? If you do, then the problem is more likely to be a broader network issue than an issue of specific the DNS application you're hitting to do resolution. It's also worth mentioning, again, that a ping to outlook.office365.com will tell you where DNS name resolution for Outlook Online is taking place (for example, outlook-namnordwest.office365.com).

If the issue looks to be DNS specific, it may be necessary to contact your IT department to look at DNS configurations and DNS Forwarders to further investigate this issue.

Proxy Scalability

Services like Outlook Online in Office 365 grant clients multiple long-term connections. Therefore, each user might use more connections that require a longer life.

Tools

Math

What to look for

There's no network trace or troubleshooting tool specific to this. Instead, it's based upon bandwidth calculations given limitations and other variables.

TCP Max Segment Size

Found in the SYN - SYN/ACK. Do this check in any performance network trace you've taken to ensure that TCP packets are configured to carry the maximum amount of data possible.

The goal is to see an MSS of 1,460 bytes for transmission of data. If you're behind a proxy, or you're using a NAT, remember to run this test from client to proxy/egress/NAT, and from proxy/egress/NAT to Office 365 for best results! These are different TCP sessions.

Tools

Netmon

What to look for

TCP Max Segment Size (MSS) is another parameter of the three-way handshake in your network trace that means you'll find the data you need in the SYN - SYN/ACK packet. MSS is pretty simple to see.

Open any performance network trace you have and find the connection you're curious about, or that demonstrates the performance problem.

ⓘ Note

If you are looking at a trace and need to find the traffic relevant to your conversation, filter by the IP of the Client, or the IP of the proxy server or egress point, or both. Going directly, you will need to ping the URL that you're testing for the IP address of Office 365 in the trace, and filter by it.

Looking at the trace second-hand? Try using filters to orient yourself. In Netmon, run a search based on the URL, such as `containsbin(framedata, ascii, "sphybridExample")`, take note of the frame number.

In Wireshark, use something like `frame contains "sphybridExample"`. If you notice that you've found Remote Winsock (RWS) traffic (it might appear as a [PSH, ACK] in Wireshark), remember that RWS connects can be seen shortly before relevant SYN - SYN/ACKs, as discussed earlier.

At this point, you can record the frame number, drop the filter, and click **All Traffic** in the Network Conversations window in Netmon to look at the nearest SYN.

Importantly, if you didn't receive any of the IP address information at the time of the trace, finding your URL in the trace (part of `sphybridExample-my.sharepoint.com`, for example), will give you IP addresses to filter by.

Locate the connection in the trace that you're interested in seeing. You may do this by either scanning the trace, by filtering by IP addresses, or by selecting specific Conversation IDs using the Network Conversations window in Netmon. Once you've found the SYN packet, expand TCP (in Netmon), or Transmission Control Protocol (in Wireshark) in the Frame Details panel. Expand TCP Options and MaxSegmentSize. Locate the related SYN-ACK frame and Expand TCP Options and MaxSegmentSize. The smaller

of the two values will be your Maximum Segment Size. In this picture, I make use of the built-in Column in Netmon called TCP Troubleshoot.

Frame Summary

Frame Number	Time Delta	Source	Destination	TCP Short Sequence Range	TCP Short Ack Number	TCP Fl...	TCP Window Size	TCP Payload Length	TCP Description
1	0.0000000	10.164.114.89	10.190.224.84	0	0 (0x0)	CE...S.	65535	0	Flags=CE...S., SrcPort=51597, DstPort=HTTP Alternate(8080),
2	0.0000000	10.190.224.84	10.164.114.89	0	1	...A.S.	2097152	0	Flags=...A.S., SrcPort=HTTP Alternate(8080), DstPort=51597,
3	0.0008366	10.164.114.89	10.190.224.84	1	1	...A...	262144	0	Flags=...A..., SrcPort=51597, DstPort=HTTP Alternate(8080),
4	0.0005668	10.164.114.89	10.190.224.84	1 - 248	1	...AP...	262144	247	Flags=...AP..., SrcPort=51597, DstPort=HTTP Alternate(8080),

Frame Details

```

Frame: Number = 3, Captured Frame Length = 66, MediaType = ETHERNET
Ethernet: Etype = Internet IP (IPv4), DestinationAddress:[00-18-FE-62-EE-F2], SourceAddress:[00-1D-46-C8-DC-00]
IPv4: Src = 10.190.224.84, Dest = 10.164.114.89, Next Protocol = TCP, Packet ID = 1999, Total IP Length = 52
TCP: Flags=...A..S., SrcPort=HTTP Alternate(8080), DstPort=51597, PayloadLen=0, Seq=2729334249, Ack=2810613926, Win=8192 ( Negotiated scale factor )
    SrcPort: HTTP Alternate(8080)
    DstPort: 51597
    SequenceNumber: 2729334249 (0xA2AE55E9)
    AcknowledgementNumber: 2810613926 (0xA78690A6)
    DataOffset: 128 (0x80)
    Flags: ...A..S.
    Window: 8192 ( Negotiated scale factor 0x8 ) = 2097152
    Checksum: 0xCDD0, Good
    UrgentPointer: 0 (0x0)
    TCPOptions:
        MaxSegmentSize: 1
            type: Maximum Segment Size. 2(0x2)
            OptionLength: 4 (0x4)
            MaxSegmentSize: 1460 (0x5B4)

```

The built-in column is at the top of the **Frame Details** panel. (To switch back to your normal view, click **Columns** again, and then choose **Time Zone**.)

Layout ▾ Parser Profiles ▾ Options How Do I ▾

Save Filter Clear Text

Color Rules Aliases ▾ Columns ▾

Time Zone (NM 3.4)

- NM 3.3
- ETW (ETL)
- PCAP
- TCP Troubleshoot
- HTTP Troubleshoot
- Choose Columns...
- Automatically Save Column Layout
- Restore Default Column Layout

Here's a filtered trace in Wireshark. There's a filter specific to the MSS value (`tcp.options.mss`). The frames of a SYN, SYN/ACK, ACK handshake are linked at the

bottom of the Wireshark equivalent to Frame Details (so frame 47 ACK, links to 46 SYN/ACK, links to 43 SYN) to make this kind of work easier.

No.	Time	Source	Destination	Protocol	Time	Info
42	0.038290000	10.120.12.114	157.54.86.84	TCP		58099-40700 [PSH, ACK] Seq=771 Ack=484 Win=255 Len=281
43	0.039039500	10.120.12.114	157.54.86.84	TCP		58100-40700 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SA
44	0.039887500	157.54.86.84	10.120.12.114	TCP		1745-58097 [PSH, ACK] Seq=771 Ack=484 Win=255 Len=281
45	0.040505800	10.120.12.114	157.54.86.84	TCP		58099-40702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SA
46	0.080978100	157.54.86.84	10.120.12.114	TCP		40700-58100 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460
47	0.081497400	10.120.12.114	157.54.86.84	TCP		58100-40700 [ACK] Seq=1 Ack=1 Win=262144 Len=0
48	0.082292500	157.54.86.84	10.120.12.114	TCP		40702-58099 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460
49	0.082619100	10.120.12.114	157.54.86.84	TCP		58099-40702 [ACK] Seq=1 Ack=1 Win=262144 Len=0
50	0.082619100	2001:1::1	2001:1::1	UDP		Source port: 52055 Destination port: 2280

Destination Geolip: UNKNOWN

- Transmission Control Protocol, Src Port: 40700 (40700), Dst Port: 58100 (58100), Seq: 0, Ack: 1, Len: 0
 - Source Port: 40700 (40700)
 - Destination Port: 58100 (58100)
 - [Stream index: 1]
 - [TCP Segment Len: 0]
 - Sequence number: 0 (relative sequence number)
 - Acknowledgment number: 1 (relative ack number)
 - Header Length: 32 bytes
 - 0000 0001 0010 = Flags: 0x012 (SYN, ACK)
 - Window size value: 4380
 - [Calculated window size: 4380]
 - Checksum: 0x806d [validation disabled]
 - Urgent pointer: 0
 - options: (12 bytes), Maximum segment size, No-operation (NOP), window scale, SACK permitted, End of Option List (EOL)
 - Maximum segment size: 1460 bytes
 - Kind: Maximum Segment Size (2)
 - Length: 4
 - MSS Value: 1460
 - No-operation (NOP)
 - Window scale: 2 (multiply by 4)
 - TCP SACK Permitted Option: True
 - End of Option List (EOL)
 - [SEQ/ACK analysis]
 - [This is an ACK to the segment in frame: 43]
 - [The RTT to ACK the segment was: 0.041938600 seconds]
 - [iRTT: 0.042457900 seconds]

If you need to check **Selective Acknowledgment** (next topic in this matrix), don't close your trace!

Selective Acknowledgment

Found in the SYN - SYN/ACK. Must be reported as Permitted in both SYN and SYN/ACK. Selective Acknowledgment (SACK) allows for smoother retransmission of data when a packet or packets go missing. Devices can disable this feature, which can lead to performance problems.

If you're behind a proxy, or you're using a NAT, remember to run this test from client to proxy/egress/NAT, and from proxy/egress/NAT to Office 365 for best results! These are different TCP sessions.

Tools

Netmon

What to look for

Selective Acknowledgment (SACK) is another parameter in the SYN-SYN/ACK handshake. You can filter your trace for SYN - SYN/ACK many ways.

Locate the connection in the trace that you're interested in seeing either by scanning the trace, filtering by IP addresses, or by clicking a Conversation ID using the Network Conversations window in Netmon. Once you've found the SYN packet, expand TCP in Netmon, or Transmission Control Protocol in Wireshark in the Frame Details section. Expand TCP Options and then SACK. Locate the related SYN-ACK frame and Expand TCP Options and its SACK field. Make certain SACK is permitted in both SYN and SYN/ACK. Here are SACK values as seen in both Netmon and Wireshark.

Display Filter

tcp.Flags.Syn == 1

Frame Summary - tcp.Flags.Syn== 1

Frame Number	Time Date Local Adjusted	Time Offset	Time Delta	Process Name	Source	Destination	Protocol Name	Description
2	12:16:32 PM 3/4/2015	0.000000	0.000000	IEXPLORE.EXE	10.164.114.89	10.190.224.84	TCP	TCP:Flags=CE....S., SrcPort=51597, DstPort=HTTP
3	12:16:32 PM 3/4/2015	0.2598509	0.2598509	IEXPLORE.EXE	10.190.224.84	10.164.114.89	TCP	TCP:Flags=...A..S., SrcPort=HTTP Alternate(8080)

Frame Details

```

Frame: Number = 2, Captured Frame Length = 66, MediaType = ETHERNET
Ethernet: Etype = Internet IP (IPv4), DestinationAddress:[00-1D-46-C8-DC-00], SourceAddress:[00-18-FE-62-EE-F2]
Ipv4: Src = 10.164.114.89, Dest = 10.190.224.84, Next Protocol = TCP, Packet ID = 12234, Total IP Length = 52
Tcp: Flags=CE....S., SrcPort=51597, DstPort=HTTP Alternate(8080), PayloadLen=0, Seq=2810613925, Ack=0, Win=65535
    SrcPort: 51597
    DstPort: HTTP Alternate(8080)
    SequenceNumber: 2810613925 (0xA78690A5)
    AcknowledgementNumber: 0 (0x0)
    DataOffset: 128 (0x80)
    Flags: CE....S.
    Window: 65535 ( Negotiating scale factor 0x8 ) = 65535
    Checksum: 0xE4F6, Good
    UrgentPointer: 0 (0x0)
    TCPOptions:
        MaxSegmentSize: 1
            type: Maximum Segment Size. 2 (0x2)
            OptionLength: 4 (0x4)
            MaxSegmentSize: 1460 (0x5B4)
        NoOption:
        WindowsScaleFactor: ShiftCount: 8
        NoOption:
        NoOption:
        NoOption:
        SACKPermitted:
            type: SACK permitted. 4 (0x4)
            OptionLength: 2 (0x2)

```

Filter: tcp.flags.syn == 1							Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Time	Info				
1	0.0000000000	10.164.114.89	10.190.224.120	TCP	51387-8080	[SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1				
2	0.0054323000	10.190.224.120	10.164.114.89	TCP	8080-51387	[SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1				
80	0.3560325000	10.164.114.89	10.190.224.120	TCP	51388-8080	[SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1				
81	0.3601182000	10.190.224.120	10.164.114.89	TCP	8080-51388	[SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1				
81	0.4323705000	10.164.114.89	10.190.224.120	TCP	51390-8080	[SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1				
81	0.4323705000	10.164.114.89	10.190.224.120	TCP	8080-51387	[SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1				
Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)										
Ethernet II, Src: Cisco_C8:dC:00 (00:1d:46:c8:dc:00), Dst: Hewlett-62:ee:f2 (00:18:fe:62:ee:f2)										
Internet Protocol Version 4, Src: 10.190.224.120 (10.190.224.120), Dst: 10.164.114.89 (10.164.114.89)										
Transmission Control Protocol, Src Port: 8080 (8080), Dst Port: 51387 (51387), Seq: 0, Ack: 1, Len: 0										
Source Port: 8080 (8080)										
Destination Port: 51387 (51387)										
[Stream index: 0]										
[TCP Segment Len: 0]										
Sequence number: 0 (relative sequence number)										
Acknowledgment number: 1 (relative ack number)										
Header Length: 32 bytes										
[... 0000 0001 0010 = Flags: 0x012 (SYN, ACK)]										
Window size value: 8192										
[calculated window size: 8192]										
Checksum: 0xcc6d [validation disabled]										
Urgent pointer: 0										
Options: (12 bytes), Maximum segment size, No-Operation (NOP), window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted										
Maximum segment size: 1460 bytes										
Kind: Maximum Segment Size (2)										
Length: 4										
MSS Value: 1460										
No-operation (NOP)										
Window scale: 8 (multiply by 256)										
No-operation (NOP)										
No-operation (NOP)										
TCP SACK Permitted Option: True										
Kind: SACK Permitted (4)										
Length: 2										
[SEQ/ACK analysis]										
This is an ACK to the segment in frame: 11										
[The RTT to ACK the segment was: 0.005432300 seconds]										
[iRTT: 0.005982300 seconds]										

DNS Geolocation

Where in the world Office 365 tries to resolve your DNS call affects your connection speed.

In Outlook Online, after the first DNS lookup is completed, the location of that DNS will be used to connect to your nearest datacenter. You'll be connected to an Outlook Online CAS server, which will use the backbone network to connect to the datacenter (dC) where your data is stored. This is faster.

When accessing SharePoint, a user traveling abroad will be directed to their active datacenter - that's the dC whose location is based on their SPO tenant's home-base (so, a dC in the USA if the user is USA-based).

Lync online has active nodes in more than one dC at a time. When requests are sent for Lync online instances, Microsoft's DNS will determine where in the world the request came from, and return IP addresses from the nearest regional dC where Lync online is active.

Tip

Need to know more about how clients connect to Office 365? Take a look at the [Client Connectivity](#) reference article (and its helpful graphics).

Tools

- Ping
- PsPing

What to look for

Requests for name resolution from the client's DNS servers to Microsoft's DNS servers should in most cases result in Microsoft DNS returning the IP address of a regional datacenter (dC). What does this mean for you? If your headquarters are in Bengaluru, India, but you're traveling in the United States, when your browser makes a request for Outlook Online, Microsoft's DNS servers should hand you IP addresses to datacenters in the United States - a regional datacenter. If mail is needed from Outlook, that data will travel across Microsoft's quick backbone network between the datacenters.

DNS works fastest when name resolution is done as close to the user location as possible. If you're in Europe, you want to go to a Microsoft DNS in Europe, and (ideally) deal with a datacenter in Europe. Performance from a client in Europe going to DNS and a datacenter in America will be slower.

Run the Ping tool against outlook.office365.com to determine where in the world your DNS request is being routed. If you are in Europe, you should see a reply from something like outlook-emeawest.office365.com. In the Americas, expect something like outlook-namnorthwest.office365.com.

Open the command prompt on the client computer (via Start > Run > cmd or Windows key > type cmd). Type ping outlook.office365.com and press ENTER. Remember, to specify -4 if you want to specify to ping via IPv4. You might fail to get a reply from the ICMP packets, but you should see the name of the DNS to which the request was routed. If you want to see the latency numbers for this connection try PsPing to the IP address of the server that is returned by ping.

```
C:\Perf>ping outlook.office365.com
Pinging outlook-namnorthwest.office365.com [132.245.64.146] with 32 bytes of data:
Reply from 132.245.64.146: bytes=32 time=28ms TTL=240

Ping statistics for 132.245.64.146:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 28ms, Maximum = 28ms, Average = 28ms
```

```
C:\>Perf>psping 132.245.64.146:443
PsPing v2.01 - PsPing - ping, latency, bandwidth measurement utility
Copyright (C) 2012-2014 Mark Russinovich
Sysinternals - www.sysinternals.com

TCP connect to 132.245.64.146:443:
5 iterations <warmup 1> connecting test:
Connecting to 132.245.64.146:443 <warmup>: 28.75ms
Connecting to 132.245.64.146:443: 30.10ms
Connecting to 132.245.64.146:443: 31.31ms
Connecting to 132.245.64.146:443: 29.63ms
Connecting to 132.245.64.146:443: 30.15ms

TCP connect statistics for 132.245.64.146:443:
  Sent = 4, Received = 4, Lost = 0 (0% loss),
  Minimum = 29.63ms, Maximum = 31.31ms, Average = 30.30ms
```

Office 365 Application Troubleshooting

Tools

- Netmon
- HTTPWatch
- F12 Console in the browser

We don't cover tools used in application-specific troubleshooting in this network-specific article. But you'll find resources you *can* use [on this page ↗](#).

Related articles

[Managing Office 365 endpoints ↗](#)

[Office 365 endpoints FAQ ↗](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

How to check Windows release health

Article • 06/04/2024 • Applies to:  [Windows 11](#),  [Windows 10](#)

The Windows release health page in the Microsoft 365 admin center enables you to view the latest information on known issues for Windows monthly and feature updates. A known issue is an issue that impacts Windows devices and that has been identified in a Windows monthly update or feature update. The Windows release health page is designed to inform you about known issues. You can use this information to troubleshoot issues your users may be experiencing. You can also determine when, and at what scale, to deploy an update in your organization.

If you're unable to sign in to the Microsoft 365 admin portal, check the [Microsoft 365 service health](#) status page to check for known issues preventing you from signing into your tenant.

To be informed about the latest updates and releases, follow [@WindowsUpdate](#) on Twitter.

Prerequisites

Ensure the following prerequisites are met to display the Windows release health page in the Microsoft 365 admin center:

- One of the following licenses:
 - Windows 10/11 Enterprise E3 or E5 (included in Microsoft 365 F3, E3, or E5)
 - Windows 10/11 Education A3 or A5 (included in Microsoft 365 A3 or A5)
- Sign into the Microsoft 365 admin center using an [admin role](#).
 - Most roles containing the word `administrator` give you access to the Windows release health page such as [Helpdesk Administrator](#) and [Service Support Administrator](#). For more information, see [Assign admin roles in the Microsoft 365 admin center](#).

Note

Currently, Windows release health is available for Government Community Cloud (GCC) tenants, but isn't available for GCC High and DoD.

How to review Windows release health information

1. Go to the [Microsoft 365 admin center](#) and sign in with an admin account.
2. To view Windows release health in the Microsoft 365 Admin Center, go to **Health > Windows release health**.
3. On the **Windows release health** page, you have access to known issue information for all supported versions of the Windows operating system.

The **All versions** tab (the default view) shows all Windows products with access to their posted known issues.

The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar has a navigation menu with items like Home, Users, Devices, Groups, Roles, Resources, Billing, Support, Settings, Setup, Reports, Health, Service health, Windows release health (which is selected and highlighted in blue), and Message center. The main content area is titled "Windows release health". At the top of this area are three tabs: "All versions" (which is selected and highlighted in blue), "Known Issues", and "History". Below the tabs is a sub-header: "Find information about known issues for currently supported versions of the Windows operating system." A table follows, listing supported Windows versions along with "View" links for each. The columns are "Version ↓", "Active and recently resolved", and "History". The listed versions are: Windows 10, version 20H2 and Windows Server, version 20H2; Windows 10, version 2004 and Windows Server, version 2004; Windows 10, version 1909 and Windows Server, version 1909; Windows 10, version 1809 and Windows Server 2019; Windows 10, version 1803; and Windows 10, version 1607 and Windows Server 2016.

Version ↓	Active and recently resolved	History
Windows 10, version 20H2 and Windows Server, version 20H2	View	View
Windows 10, version 2004 and Windows Server, version 2004	View	View
Windows 10, version 1909 and Windows Server, version 1909	View	View
Windows 10, version 1809 and Windows Server 2019	View	View
Windows 10, version 1803	View	View
Windows 10, version 1607 and Windows Server 2016	View	View

A known issue is an issue that has been identified in a Windows monthly update or feature update that impacts Windows devices. The **Active and recently resolved** column provides a link to the **Known issues** tab filtered to the version selected. Selecting the **Known issues** tab shows known issues that are active or resolved within the last 30 days.

The screenshot shows the Microsoft 365 admin center interface. On the left, there's a navigation sidebar with various options like Home, Users, Devices, Groups, Roles, Resources, Billing, Support, Settings, Setup, Reports, Health, Service health, Windows release health (which is selected and highlighted in blue), and Message center. The main content area is titled "Windows release health". At the top of this area, there are three tabs: "All versions", "Known Issues" (which is active and highlighted with a blue border), and "History". Below the tabs, a message says: "View information about known issues that are active or have been resolved in the last thirty days. For issues older than thirty days, see the History tab." There's a search bar and a filter button for "Windows 10, version 20H2 and Windows Server, version 20H2". The main part of the screen is a table listing known issues:

Issue title	Status
Memory or disk space error when opening documents in Microsoft Office apps	Resolved
Error when attempting to print to certain printers	Resolved
Errors or issues during or after updating devices with Conexant ISST audio drivers	Confirmed
Errors or issues during or after updating devices with certain Conexant audio drivers	Confirmed
Automatic input of Furigana might not work as expected	Mitigated

The **History** tab shows the history of known issues that have been resolved for up to 6 months.

This screenshot is similar to the previous one but shows the "History" tab selected. The main content area is titled "Windows release health". The tabs at the top are "All versions", "Known Issues" (highlighted with a blue border), and "History" (which is active). A message below the tabs says: "View information about known issues that have been resolved over the past six months." There's a search bar and a filter button for "Past 6 months" and "Windows 10, version 20H2 and Windows Server, versi". The main part of the screen is a table listing known issues:

Issue title	Originating KB
Memory or disk space error when opening documents in Microsoft Office apps	KB4601382
Error when attempting to print to certain printers	KB5000802
Some games might fail to open, or you might receive an error	KB4598291
You might receive an error when accessing the sign-in options or users MMC snap-in	N/A
Stop error when plugging in a Thunderbolt NVMe SSD	N/A
Certificates may not be present after updating to a newer version of Windows 10	N/A

The known issue summary provides the following information:

- **Title** - A summary of the problem.
- **Version** - The name of the affected Windows product version.
- **Status** - The current status of the issue.
- **Originating KB** - The KB number where the issue was first identified.

- **Originating build** - The build number for the KB.

Select the **Issue title** to access more information, including a link to the history of all status updates posted while we work on a solution. For example:

The screenshot shows the Microsoft 365 admin center interface. On the left, there's a navigation menu with options like Home, Users, Devices, Groups, Roles, Resources, Billing, Support, Settings, Setup, Reports, Health, Service health, Windows release health, and Message center. The 'Windows release health' section is currently selected. In the main content area, a specific issue is detailed under the heading 'Stop error when plugging in a Thunderbolt NVMe SSD'. The issue is identified by the ID WI225974, is for Windows 10, version 20H2 and Windows Server, version 20H2, and was last updated on December 11, 2020 at 5:46 PM. It was resolved on November 30, 2020 at 2:00 PM. The status is 'Resolved'. The 'Issue title' is 'Stop error when plugging in a Thunderbolt NVMe SSD'. The 'User impact' section notes that devices using Thunderbolt SSDs may receive a stop error "DRIVER_VERIFIER_DMA_VIOLATION (e6)" when plugging an SSD in. A link 'Is this post helpful?' is provided. At the bottom, there's a 'Latest message' section with a link to 'View history'.

Sign up for email notifications

You can sign up for email notifications about Windows known issues and informational updates. Notifications include changes in issue status, new workarounds, and issue resolutions. To subscribe to notifications:

1. Go to the [Windows release health page ↗](#).
2. Select **Preferences > Email**, then select **Send me email notifications about Windows release health**.
3. Specify the following information:
 - Email address for the notifications
 - Each admin account can specify up to two email addresses under their email preferences
 - Windows versions to be notified about
4. Select **Save** when you're finished specifying email addresses and Windows versions. It may take up to 8 hours for these changes to take effect.

Note

When a single known issue affects multiple versions of Windows, you'll receive only one email notification, even if you've selected notifications for multiple versions. Duplicate emails won't be sent.

Working with the Windows updates API in Microsoft Graph

If you'd like to develop an alternative way to get information on known issues documented within the Windows release health section in the admin center, you can use the Windows updates API in [Microsoft Graph](#).

The Windows updates API has current and historical known issues data for any supported Windows product. You can check if an issue is confirmed, and if a resolution is available before calling support or spending time troubleshooting.

The Windows updates API also has product lifecycle information. For instance, you can search for end of servicing dates for all supported Windows versions and editions you manage in your organization. For more information on how to access these known issue and lifecycle data, see [Microsoft Graph product resource type](#).

ⓘ Note

These Windows data sets are currently under the [Microsoft Graph REST API beta endpoint reference](#).

Status definitions

In the **Windows release health** experience, every known issue is assigned as status.

Those statuses are defined as follows:

[+] Expand table

Status	Definition
Reported	An issue has been brought to the attention of the Windows teams. At this stage, there's no confirmation that users are affected.
Investigating	The issue is believed to affect users and efforts are underway to gather more information about the issue's scope, mitigation steps, and root cause.

Status	Definition
Confirmed	After close review, Microsoft has determined the issue is affecting Windows users, and progress is being made on mitigation steps and root cause.
Mitigated	A workaround is available and communicated to Windows customers for a known issue. A known issue stays in this state until a KB article is released by Microsoft to resolve the known issue.
Mitigated: External	A workaround is available and communicated to Windows customers for a known issue caused by a software or driver from a third-party software or device manufacturer. A known issue stays in this state until the issue is resolved by Microsoft or the third-party.
Resolved	A solution was released by Microsoft and was documented in a KB article that resolves the known issue once it's deployed in the customer's environment.
Resolved: External	A solution was released by Microsoft or a third-party that resolves the known issue once it's deployed in the customer's environment.

Known issue history

The Windows release health page lets you view the history of all status updates posted for a specific known issue. To view all past updates posted for a given issue, select **View history** on the issue detail page.

Stop error when plugging in a Thunderbolt NVMe SSD

WI225974, Windows 10, version 20H2 and Windows Server, version 20H2
Last updated: December 11, 2020 5:46 PM
Resolved time: November 30, 2020 2:00 PM

Status
Resolved

User impact
Devices using Thunderbolt SSDs may receive a stop error "DRIVER_VERIFIER_DMA_VIOLATION (e6)" when plugging an SSD in.

[Is this post helpful?](#)

Latest message [View history](#)

An incompatibility issue has been found with Windows 10, version 2004 or Windows 10, version 20H2 when using an Thunderbolt NVMe Solid State Disk (SSD). On affected devices, when plugging in a Thunderbolt NVMe SSD you might receive a

A list of all status updates posted in the selected time frame is displayed. You can expand any row to view the specific information provided in that status update.

History: Stop error when plugging in a Thunderbolt NVMe SSD

User impact: Devices using Thunderbolt SSDs may receive a stop error "DRIVER_VERIFIER_DMA_VIOLATION (e6)" when plugging an SSD in.

December 11, 2020 5:46 PM ^

An incompatibility issue has been found with Windows 10, version 2004 or Windows 10, version 20H2 when using an Thunderbolt NVMe Solid State Disk (SSD). On affected devices, when plugging in a Thunderbolt NVMe SSD you might receive a stop error with a blue screen and "DRIVER_VERIFIER_DMA_VIOLATION (e6)" An illegal DMA operation was attempted by a driver being verified." Affected Windows 10 devices will have at least one Thunderbolt port and any currently available version of the driver file stornvme.sys.

To safeguard your update experience, we have applied a compatibility hold on Windows 10 devices with affected drivers from being offered Windows 10, version 2004 or Windows 10, version 20H2. If your organization is using Update Compliance [\[link\]](#), the safeguard IDs is 29991611.

Resolution: This issue was resolved in [KB4586853](#) and the safeguard hold has been removed as of December 11, 2020. Please note, if there are no other safeguards that affect your device, it can take up to 48 hours before the update to Windows 10, version 20H2 or Windows 10, version 2004 is offered.

Affected platforms:

- Client: Windows 10, version 20H2; Windows 10, version 2004

November 30, 2020 2:56 PM ▼

November 30, 2020 2:19 PM ▼

Frequently asked questions

Windows release health coverage

- **What is Windows release health?** Windows release health is a Microsoft informational service created to keep licensed Windows customers aware of identified known issues and important announcements.
- **Microsoft 365 service health content is specific to my tenants and services. Is the content in Windows release health specific to my Windows environment?**
Windows release health doesn't monitor user environments or collect customer environment information. In Windows release health, all known issue content across all supported Windows versions is published to all subscribed customers. Future iterations of the solution may target content based on customer location, industry, or Windows version.
- **Where do I find Windows release health?**
After logging into Microsoft 365 admin center, expand the left-hand menu using ... Show All, select Health to display the Windows release health menu option.
- **Is the Windows release health content published to Microsoft 365 admin center the same as the content on Windows release health on Microsoft Learn?**
No. While the content is similar, you may see more issues and more technical details published to Windows release health on Microsoft 365 admin center to

better support the IT admin. For example, you'll find details to help you diagnose issues in your environment, steps to mitigate issues, and root cause analysis.

- **How often will content be updated?**

To ensure Windows customers have important information as soon as possible, all major known issues are shared with Windows customers on both Microsoft Learn and the Microsoft 365 admin center. We may also update the details available for Windows release health in the Microsoft 365 admin center when we have additional details on workarounds, root cause, or other information to help you plan for updates and handle issues in your environment.

- **Can I share this content publicly or with other Windows customers?**

Windows release health is provided to you as a licensed Windows customer and isn't to be shared publicly.

- **Is the content redundant? How is the content organized in the different tabs?**

Windows release health provides three tabs. The landing **All versions** tab allows you to select a specific version of Windows. The **Known issues** tab shows the list of issues that are active or resolved in the past 30 days. The **History** tab shows a six-month history of known issues that have been resolved.

- **How do I find information for the versions of Windows I'm managing?**

On the **All versions** tab, you can select any Windows version. This action takes you to the **Known issues** tab filtered for the version you selected. The **Known issues** tab provides the list of active known issues and the issues resolved in the last 30 days. This selection persists throughout your session until changed. From the **History** tab, you can view the list of resolved issues for that version. To change versions, use the filter in the tab.

Microsoft 365 Admin Center functions

- **How do I best search for issues impacting my environment?**

You can search Microsoft 365 admin center pages using keywords. For Windows release health, go to the desired product page and search using KB numbers, build numbers, or keywords.

- **How do I add other Windows admins?**

Using the left-hand menu, go to Users, then select the Active Users tab and follow the prompts to add a new user, or assign an existing user, to the role of **Service Support admin**.

- **Why can't I click to the KB article from the Known issues or History tabs?**

Within the issue description, you'll find links to the KB articles. In the known issue

and history tabs, the entire row is a clickable entry to the issue's Details pane.

- Microsoft 365 admin center has a mobile app but I don't see Windows release health under the Health menu. Is this an open issue?

We're working to build the Windows release health experience on mobile devices in a future release.

Help and support

- What should I do if I have an issue with Windows that is not reported in Windows release health?

Seek assistance through Premier support, the [Microsoft Support website](#), or connect with your normal channels for Windows support.

- When reaching out to Support, they asked me for an advisory ID. What is this and where can it?

The advisory ID can be found in the upper left-hand corner of the known issue Details pane. To find it, select the known issue you're seeking help on, select the Details pane, and you'll find the ID under the issue title. The ID is the letters WI followed by a number, similar to WI123456.

- How can I learn more about expanding my use of Microsoft 365 admin center? For more information, see the [Microsoft 365 admin center documentation](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Windows deployment documentation

Learn about deploying and updating Windows devices in your organization.

Plan

CONCEPT

[Plan for Windows 11](#)

[Create a deployment plan](#)

[Plan for volume activation](#)

[Windows compatibility cookbook](#)

Prepare

GET STARTED

[Prepare for Windows 11](#)

[Prepare to deploy Windows updates](#)

[Prepare for Windows Update for Business](#)

[Evaluate and update infrastructure](#)

Deploy

DEPLOY

[Compare Windows Autopilot solutions](#)

[Deploy updates with Intune](#)

[Deploy Windows updates with Configuration Manager](#)

[Optimize and cache content](#)

Use Windows Autopilot

OVERVIEW

[Windows Autopilot device preparation overview](#)

[Windows Autopilot overview](#)

TUTORIAL

[Windows Autopilot scenarios](#)

[Windows Autopilot device preparation scenarios](#)

Use Windows Autopatch

OVERVIEW

[What is Windows Autopatch?](#)

[Prerequisites](#)

[Deployment guide](#)

[See more >](#)

Use Windows Update for Business

HOW-TO GUIDE

[What is Windows Update for Business?](#)

[Configure Windows Update for Business](#)

[Windows Update for Business reports overview](#)

Use tools for upgrade and imaging

REFERENCE

[Customize Windows PE boot images](#)

[Convert a disk from MBR to GPT](#)

[Configure a PXE server to load Windows PE](#)

More resources

DOWNLOAD

[Download and install the Windows ADK](#)

[Deployment tools](#)

WHAT'S NEW

[Windows IT pro blog ↗](#)

[Windows office hours ↗](#)

Deployment guide for Microsoft 365 Apps

Article • 12/14/2023

This guide helps IT Pros plan, deploy, and manage Microsoft 365 Apps in their enterprise environments.

Featured

- [What's new for deploying Microsoft 365 Apps](#)
- [Overview of Cloud Policy](#)
- [Overview of the Office Customization Tool](#)
- [Assess your environment and requirements for deploying Microsoft 365 Apps](#)
- [Plan your enterprise deployment of Microsoft 365 Apps](#)
- [Remove existing MSI versions of Office when upgrading to Microsoft 365 Apps](#)
- [Microsoft FastTrack ↗](#)

Deploy

Learn about your deployment options, how to deploy from a local source, and how to use Microsoft Configuration Manager to deploy Microsoft 365 Apps.

- [Deploy Microsoft 365 Apps from the cloud](#)
- [Deploy Microsoft 365 Apps from a local source](#)
- [Deploy with Configuration Manager \(current branch\)](#)

Manage updates

Learn about the different update channels available for Microsoft 365 Apps and how to use Configuration Manager to manage updates.

- [Overview of update channels for Microsoft 365 Apps](#)
- [Manage updates to Microsoft 365 Apps with Microsoft Configuration Manager](#)

- Change the Microsoft 365 Apps update channel for devices in your organization
- Release information for updates to Microsoft 365 Apps

Reference

Learn about the Office Deployment Tool (ODT), other deployment options, and activation.

- Overview of the Office Deployment Tool
- Configuration options for the Office Deployment Tool
- Overview of deploying languages for Microsoft 365 Apps
- Deploy Microsoft 365 Apps by using Remote Desktop Services
- Overview of licensing and activation in Microsoft 365 Apps
- Overview of shared computer activation for Microsoft 365 Apps

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Surface devices documentation

Harness the power of Surface, Windows, and Office connected together through the cloud.

Surface devices

WHAT'S NEW

[Pre-order Surface Pro or Surface Laptop ↗](#)

[Check out the all-new Surface Laptop and Surface Pro ↗](#)

[Detachable Surface Pro Flex Keyboard](#)

[Surface IT Toolkit](#)

[Introducing Surface Pro 10 & Surface Laptop 6 ↗](#)

[Tested peripherals for Surface Pro 10 & Laptop 6](#)

[NFC support in Surface Pro 10 for Business](#)

[Surface ruggedness testing](#)

[Explore all Surface family products ↗](#)

Get started

GET STARTED

[Explore Surface interactive tour ↗](#)

[Azure Virtual Desktop on Surface](#)

[Remote work solutions with Surface ↗](#)

Microsoft Ignite

VIDEO

[Demystifying AI NPU and Machine Learning within Microsoft Surface ↗](#)

[Advanced Security and Management Solutions for Hybrid Work from Microsoft Surface ↗](#)

Deploy Surface devices

DEPLOY

[Autopilot and Surface devices](#)

[Surface Registration Support for Windows Autopilot](#)

[Surface Deployment Accelerator](#)

Manage Surface devices

HOW-TO GUIDE

[Get started with Surface Enterprise Management Mode \(SEMM\)](#)

[Configure UEFI settings for Surface devices](#)

[Manage DFCI on Surface devices](#)

[Manage and deploy Surface driver and firmware updates](#)

Surface service & repair

CONCEPT

[Surface for Business service and repair](#)

[Downloadable Surface service guides ↗](#)

[Hands-on videos for Surface device repair ↗](#)

Troubleshoot

TRAINING

[Deploy Surface Diagnostic Toolkit for Business](#)

[Top support solutions](#)

Surface driver and firmware lifecycle for Windows-based devices

Surface supported operating systems ↗

Explore security guidance



HOW-TO GUIDE

[Surface security overview](#)

[DMA Protection on Surface devices](#)

[Surface Data Eraser tool](#)

Discover Surface tools



HOW-TO GUIDE

[Surface Diagnostic Toolkit for Business](#)

[SEMM and UEFI](#)

[Battery Limit setting](#)

Surface ROI



TRAINING

[Maximizing ROI with Microsoft Surface](#)

[Total Economic Impact of Microsoft Surface for Education](#)

Participate in Surface Community



TRAINING

[Surface IT Pro blog ↗](#)

[Surface Devices Tech Community ↗](#)

[Microsoft Mechanics Surface videos ↗](#)

Need help?



TRAINING

[Contact Surface Support](#)

[Surface for Business warranty and protection plans ↗](#)

Device management roadmap for Microsoft 365

Article • 07/29/2024

Microsoft 365 for enterprise includes features to help manage devices, and their apps, within your organization. Managing mobile devices helps you secure and protect your organization's resources.

There are two options for device management:

- [Microsoft Intune](#)
- [Basic Mobility and Security](#)

Microsoft Intune

You can use Microsoft Intune to manage access to your organization using mobile device management or mobile application management. Mobile device management is when users "enroll" their devices in Intune. After a device is enrolled, it is a managed device; therefore, it can receive your organization's policies, rules, and settings. 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 organization's policies. But you still need to protect your organization's resources and data. In this scenario, you can protect your apps using mobile application management. For example, you can use a mobile application management policy that requires a user to enter a PIN when accessing SharePoint Online on the device.

You'll also determine how you're going to manage personal devices and organization-owned devices. You might want to treat devices differently, depending on their uses.

Basic Mobility and Security

This is built into Microsoft 365 and helps you secure and manage your users' mobile devices like iPhones, iPads, Androids, and Windows phones. You can create and manage device security policies, remotely wipe a device, and view detailed device reports.

Choose between the two options

To help you better assess which device management option is best for you, see [Choose between Basic Mobility Security and Intune](#).

Based on your assessment, get started managing your devices with:

- [Intune](#)
- [Basic Mobility and Security ↗](#)

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 these articles:

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

How Contoso did device management for Microsoft 365

For information about how a fictional but representative multi-national business deployed their mobile device management infrastructure with Microsoft 365 cloud services, see [Mobile device management for Contoso](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Plan your deployment of Microsoft Edge

Article • 04/04/2024

This article describes the recommended practices for deploying Microsoft Edge in an enterprise environment.

Article content

The following sections provide specific guidance for planning your Microsoft Edge deployment.

- Evaluate your existing browser environment and browser needs
- Make sure your Windows 10 or later devices are ready
- Determine your deployment methodology
 - Deploy to end users by role
 - Deploy to end users by site
- Do site discovery
 - If you've deployed and configured the legacy version of Microsoft Edge
 - If you've configured Internet Explorer as your default browser
 - Analyze site discovery data
- Determine your channel strategy
 - Multiple devices and channels
- Define and configure policies
 - Define your update strategy and policies
- Do app compatibility testing
 - Internal line of business app testing
 - Third party app support
- Deploy Microsoft Edge to a pilot group
- Validate your deployment
- Broad deployment of Microsoft Edge
- See also

Evaluate your existing browser environment and browser needs

Take time to understand your current browser state and project vision to ensure that all project stakeholders are aligned and working towards the same result.

Start by defining your current state:

- Which browsers are currently deployed in your environment?
- Which browser is set as the default browser?
- Do you need to use Internet Explorer for some of your apps?
- Do you use an Enterprise Mode Site List to configure Internet Explorer today?
- What OS platforms are supported in your environment? (Windows 10/11, macOS, Windows 7, Windows Server, etc.)
- What management tools do you use for browser management?
- Who is responsible for browser configuration and management?
- What is your process for validating browser compatibility?

After you understand the current state, you can determine the desired goals for your browser deployment, taking into account answers to the following questions:

- Do you want to [set Microsoft Edge as your default browser](#)?
- How will you [configure Microsoft Edge](#)?
- What features are critical to configure as part of your initial deployment?
- What is the process for addressing any identified compatibility or configuration issues?

You should also understand the [prerequisites](#) for features you're interested in, such as:

- [Windows Defender Application Guard](#)
- [Internet Explorer mode](#)
- [Authentication and sync](#)

With these answers in mind, you're ready to plan your Microsoft Edge deployment.

Make sure your Windows 10 (or later) devices are ready

The Edge Stable channel requires the Latest Cumulative Update (LCU) from October 2019 (or later). If you attempt to deploy to a Windows 10 device that has an older LCU, then the installation fails. For more details about the minimum LCU that must be applied before deploying Edge, see [Windows updates to support the next version of Microsoft Edge](#).

Determine your deployment methodology

After you know your desired end state, you're ready to start planning how to get there. The two main ways to deploy Microsoft Edge are by role, and by site.

Deploy to end users by role

If app compatibility is your main concern, and you don't have a firm grasp on which apps to test, you might want to consider deploying to end users by role. This enables each wave of a phased deployment to provide feedback and insights on apps that might need to have their configuration modified to address compatibility issues.

Deploy to end users by site

If bandwidth is your primary concern, you might want to consider doing application compatibility testing upfront. After you finish testing, deploy to end users by site so you can use caching other software delivery optimizations.

Do site discovery

If you have a dependency on legacy web applications and plan to use Internet Explorer mode (which most customers do), then you probably need to do some more site discovery.

If you've deployed and configured the legacy version of Microsoft Edge

If you've already configured your Enterprise Site List to work for the legacy version of Microsoft Edge, then your work is almost done! The one thing you may need to add is neutral sites.

Neutral sites are typically sites that provide Single Sign-On (SSO). If you navigate to a neutral site from Microsoft Edge, then you want to stay in Microsoft Edge to authenticate. If you navigate to a neutral site in Internet Explorer mode, then you want to stay in Internet Explorer mode to authenticate.

Identify any SSO (or other neutral) sites that you use and add these sites to your Enterprise Site List.

If you've configured Internet Explorer as your default browser

If you're currently only using Internet Explorer, you might not know which sites have upgraded to modern web standards and which still require Internet Explorer. You want

to find these sites and add them to the Enterprise Site List. This list lets you use Internet Explorer mode only on the sites that need it.

💡 Tip

Use the [Enterprise Site Discovery](#) tools to discover the sites that might need Internet Explorer mode. You can collect data on computers running Windows Internet Explorer 8 through Internet Explorer 11 on Windows 10, Windows 8.1, or Windows 7.

Analyze site discovery data

After you collect site data, we recommend the following 4-step process to analyze the data:

1. Sort the data by domain, and then by URL.
2. Define the boundaries of an "app" to configure for Internet Explorer mode. You want to include all the sites and web controls that define the app. But you don't want to include any extra sites and controls by defining the app too broadly. Some sites might be as simple as "http://contoso.com/app1" while others may require you to define multiple sites and pages.
3. Test the app to verify that it doesn't work natively. Many sites offer modern content when they detect a modern browser and only offer legacy content when they detect Internet Explorer.
4. Add the app to your Enterprise Site list if it fails to test.

❗ Note

As a best practice, group all of the sites that comprise an app. If the sites all need to be used to accomplish one task, and if they tend to be updated together, that is a good indication that they should be grouped. This way, when you upgrade an app, it's easier to remove the entire site from Internet Explorer mode and start using a modern browser for that app.

Determine your channel strategy

Microsoft Edge is released in [multiple channels](#).

Note

You can install more than one channel on a device

The Stable Channel is what you want to deploy to most devices. However, you should consider a deployment strategy that includes multiple devices and multiple channels.

Multiple devices and channels

We recommend having a representative subset of devices configured to use the Beta Channel. This channel lets you preview upcoming changes to the browser. You can see if these changes are going to affect your end users or apps.

You might also want to make the Dev Channel (or even the Canary Channel) available to some roles, such as web developers. Consider whether you would like to target some devices with more fluid and rapidly changing channels, or make these channels available for users to opt to install.

Because it's possible to install multiple channels on a device, you can mitigate the risk of testing for users who opted to install a pre-release channel. For example, if you have a user who's using the Beta Channel, and there's a problem, they can switch to the Stable Channel and continue working. This switch unblocks them until the issue can be fixed.

Note

If the user enabled Sync, then their configuration will sync across channels, making it even easier to transition between channels.

Define and configure policies

After you create your Enterprise Site List, we recommend identifying and configuring the policies that you intend to deploy with Microsoft Edge. This action ensures that these policies are applied when you perform your testing.

First, consider the first-run experience you want your users to have. If you want to automatically import settings from the current browser, configure the policy for [AutoImportAtFirstRun](#).

For security policies, we recommend starting with the Microsoft Edge Security Baseline. The Security Baseline can be applied using the [Microsoft Security Baselines Blog](#) or by

using [Microsoft Intune](#).

For other policies, we recommend reviewing the policy configurations for [Microsoft Edge](#) and [Microsoft Edge Updates](#).

Define your update strategy and policies

You also want to determine how you want to do updates after you deploy Microsoft Edge:

- **Allow Microsoft Edge to update itself** (default). If you choose to allow automatic updates of Microsoft Edge, then Microsoft Edge will automatically update itself at the pace determined by one or more channels you deployed.
- **Update Microsoft Edge at your own pace.** If you prefer to have explicit control over when updates are deployed, you can disable automatic updates and deploy them yourself (see the [Update Policy reference](#).) After you disable automatic updates you can deploy updates for each channel using one of the following tools:
 - [Intune](#)
 - [Configuration Manager](#)
 - The deployment tool of your choice.

Regardless of your update strategy, we recommend using a ringed deployment strategy. With automatic updates, this means having a representative sample of users running the Beta Channel, to identify issues with what will become the Stable Channel. With manual updates, this might also include more validation of a pilot group after a new Stable Channel build is released. This is followed by broad deployment.

Note

Microsoft Edge support will only apply to the most recent version of Microsoft Edge in each channel

Do app compatibility testing

Application compatibility for Microsoft Edge is high - so high that Microsoft provides the following compatibility promises:

1. If it works on Microsoft Edge *version 45 and earlier*, it works on Microsoft Edge *version 77 and later*.

2. If it works on Internet Explorer, it works on Microsoft Edge in Internet Explorer mode.
3. If it works on Google Chrome, it works on Microsoft Edge.

If you have an application where we don't meet our compatibility promise, then we stand behind the promise to fix it with [Microsoft App Assure](#).

Internal line of business app testing

Despite our compatibility promise, we know that many organizations must validate some applications for their compliance or risk management reasons. Even though we expect this to be straightforward, it's important to be organized and rigorous in app testing.

There are two ways to do app compatibility testing:

1. Lab testing. Applications are validated in a tightly controlled environment with specific configurations.
2. Pilot testing. Applications are validated by a limited number of users in their daily work environment using their own devices.

Choose the method that is most appropriate for each app, to manage risk without over-investing in compatibility testing.

Third party app support

In addition to their own line of business apps, many organizations use apps provided by external sources. The [Ready for Microsoft Edge](#) article contains a list of web applications that may be in use within your organization. This list provides links to provider support statements for their products when used with Microsoft Edge.

Deploy Microsoft Edge to a pilot group

After you've defined your policies and have finished your initial app compatibility testing, you're ready to deploy to your pilot group. Deploy to your pilot group using one of the following tools:

- [Microsoft Intune for Windows](#), or [Microsoft Intune for macOS](#)
- [Configuration Manager](#).
- Another management tool, download and deploy the [MSI file for Microsoft Edge](#).

Validate your deployment

After you deploy your pilot, you want to capture all the feedback you get from your users.

- Capture feedback on compatibility. Identify sites that belong on the Enterprise Site List that weren't identified during site discovery.
- Capture feedback on the policy configuration. Ensure that users can use key features and do their work while following security guidelines.
- Capture feedback on ease of use and new features. Identify any areas where training should be developed and delivered based on user questions.

Broad deployment of Microsoft Edge

After finishing the pilot and updating your deployment plan with lessons learned from the pilot, you're ready to do a full deployment of Microsoft Edge to all your users. Congratulations!

See also

- [Microsoft Edge Enterprise landing page](#)
- [Video - Deploy Microsoft Edge](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Deployment and update channel example configurations

Article • 08/26/2024

Choosing which update channels to use for Windows 11 and Microsoft 365 Apps can depend on your type of organization and where on the development cycle you want to be deploying and using new features and capabilities. Find the prerelease and production channels that best fit your needs.

Prerelease channels

 Expand table

Customer/Channel Offering	Windows 11	Microsoft 365 Apps for Enterprise (Windows 11)
Right for highly technical users and developers. Be the first to access the latest builds earliest in the development cycle with the newest code. There will be rough edges and some instability.	Dev	N/A
Right for early adopters and IT Pros who want more reliable builds that are still in development. See what's coming up next and help validate new features.	Preview Channel	Preview Channel
Right for those who want early access to upcoming releases. Where companies preview and validate upcoming releases before broad deployment. These are supported.	Release Preview	Current Channel (Preview) Semi-Annual Enterprise Channel (Preview)

Production channels for broad deployment

Click the link in the Example column to step through deployment stages and groups for an example organization.

Customer/Channel Offering	Windows 11	Microsoft 365 Apps for Enterprise (Windows 11)	Example
Right for customers who want the latest releases as soon as they're ready.	Semi-Annual Enterprise Channel	Current Channel	Latest releases
Right for enterprises who want the latest release with more predictability.	Semi-Annual Enterprise Channel	Monthly Enterprise Channel	
Right for enterprises with need for extensive IT testing before each update.	Semi-Annual Enterprise Channel	Semi-Annual Enterprise Channel	

Example of broad deployment for the latest releases

This channel configuration example is for an organization that uses rapid deployment of the latest releases to fit these business priorities:

- Ensure business continuity with Microsoft apps and services.
- Maximize device, service, and data security with the latest features and fixes from Microsoft.
- Maximize user productivity with the latest features from Microsoft.

These goals translate to the IT task of finding the balance between rapid production deployment and early vetting with a representative subset of users and devices to validate functionally before broad deployment.

Our example organization has 5,000 employees in buildings across the world in Europe, Africa, Asia, and the Americas. Seventy percent of the employees use Microsoft 365 E3 and the rest of the organization uses Microsoft 365 E5.

ⓘ Note

This example is designed to show you how you can use deployment stages and groups, which can work for organizations of many types and sizes.

This organization's IT infrastructure:

- Is largely homogeneous, with Windows, Microsoft 365 Apps, and Microsoft cloud services comprising 60% of the installed base. A few legacy systems remain after an intensive, multi-year effort to simplify and streamline the IT infrastructure.
- Is maintained by highly experienced staff and tasked with keeping users and their devices productive and secure by following Microsoft's lead in their releases.

Deployment and update stages

Based on rapid deployment goals of the latest release, this example organization uses a two-step deployment process.

1. **Use a preview or pilot deployment:** Validate and iterate with early adopters, IT staff, users with representative configurations, and training staff.

The early adopters, IT staff, users with representative configurations can validate functionality with other apps and on devices before the new features roll out to the rest of the organization.

Change managers have an early peek at the new features before widespread rollout and can plan messaging and rollout.

Training staff can plan new internal courses or update existing courses for the new features before widespread rollout.

2. **Production deployment:** Roll out to all remaining users by region, department, or other deployment method.

Deployment configuration for Windows 11

The overall goal is to perform a broad deployment of the latest Semi-Annual Channel release after validation of Release Preview Channel changes by a group of representative users and their devices.

See [Windows 11 deployment](#) for more information on Windows 11 deployment methods and strategies.

[] Expand table

Stage	Channel	Deployment group
Pilot	Release Preview Channel <ul style="list-style-type: none"> Purpose: Deployment of feature updates to IT staff and early adopters 	Win11ReleasePreviewChannel (example name) Members are groups containing:

Stage	Channel	Deployment group
	<p>for validation on representative devices and configurations (languages, 3rd party apps).</p> <ul style="list-style-type: none"> • State: Fully compliant and supported for commercial customers and it doesn't count against your support agreements. 	<ul style="list-style-type: none"> • Windows enthusiasts across departments and locations • Staff with configurations that need validation • IT admins and IT deployment staff • Change managers • Internal training staff
Production	Semi-Annual Channel <ul style="list-style-type: none"> • Purpose: Broad deployment of the latest feature updates to the rest of the organization. • State: Fully compliant and supported. 	Win11SemiAnnualChannel (example name) Members are all users that aren't in the Win11ReleasePreviewChannel group.

This organization uses the best practice of deploying the Release Preview Channel payload in the same way as they deploy Semi-Annual Channel releases, such as Windows Update or Windows Server Update Services, and that they apply the same policies for both channel updates.

Ongoing updates process:

1. Release Preview Channel changes are deployed to the Win11ReleasePreviewChannel (example name) deployment group.
2. Win11ReleasePreviewChannel group members confirm that Release Preview Channel changes are working to IT deployment staff, who can provide feedback to Microsoft and wait for the next Release Preview Channel changes for additional validation.
3. Semi-Annual Channel feature changes are deployed to the Win11SemiAnnualChannel deployment group.

ⓘ Note

While the Semi-Annual Channel is the recommended channel, your IT department should utilize their management tools and determine when to deploy the latest Semi-Annual Channel release within their organization and then roll it out in waves.

Deployment configuration for Microsoft 365 Apps

The overall goal is to perform a broad deployment of the latest Current Channel release after validation of Current Channel (Preview) changes by a group of representative users.

See [Microsoft 365 Apps deployment](#) for more information on Microsoft 365 Apps deployment methods and strategies.

[+] [Expand table](#)

Stage	Channel	Deployment group
Pilot	Current Channel (Preview) <ul style="list-style-type: none">• Purpose: {give a group of representative users a sneak peek of new Microsoft 365 Apps features} Deployment of feature updates as soon as they're tested with Current Channel (Preview) users and are production-ready.• State: Fully compliant and supported.• How often: Updates 2-3 times each month.	AppsCurrentChannelPreview (example name) Members are groups containing: <ul style="list-style-type: none">• Office apps enthusiasts across departments and locations• Staff with configurations that need validation• IT admins and IT deployment staff• Change managers• Internal training staff
Production	Current Channel <ul style="list-style-type: none">• Purpose: Broad deployment of the latest feature updates to the rest of the organization.• State: Fully compliant and supported.	AppsCurrentChannel (example name) Members are all users that aren't in the AppsCurrentChannelPreview group.

Ongoing updates process:

1. Current Channel (Preview) changes are deployed to the AppsCurrentChannelPreview deployment group.
2. AppsCurrentChannelPreview group members confirm that Current Channel (Preview) changes are working to IT deployment staff, who can provide feedback to Microsoft and wait for the next Current Channel (Preview) release for additional validation.
3. Current Channel changes are deployed to the AppsCurrentChannel deployment group.

Visual summary

Here are the products, their channels, and the deployment groups used by this example organization.

	Deployment phase	Channel	Deployment group (example names)
Windows 10	Pilot: Test for features and hardware and software compatibility with representative devices.	Release Preview Channel	Win10ReleasePreviewChannel
	Production: Roll out to all other Windows devices.	Semi-Annual Channel	Win10SemiAnnualChannel
Microsoft 365 Apps	Pilot: Test for features and app compatibility with representative users.	Current Channel (Preview)	AppsCurrentChannelPreview
	Production: Roll out to all other users.	Current Channel	AppsCurrentChannel

See also

[Microsoft 365 for enterprise overview](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Manage Microsoft 365 with PowerShell

Article • 12/27/2023

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

PowerShell for Microsoft 365 is a powerful management tool that complements the Microsoft 365 admin center. For example, you can use PowerShell automation to easily manage multiple user accounts and licenses and to create reports.

Select from the following topics to learn how to use PowerShell to manage Microsoft 365:

- **[Get started](#)**

Start here if you're not familiar with PowerShell for Microsoft 365, and you want to install the Microsoft 365 modules and connect to your subscription.

- **[User accounts, licenses, and groups](#)**

Start here if want to learn about using automation commands to manage user accounts, licenses, and groups.

- **[SharePoint](#)**

Start here if you want to use automation commands to manage SharePoint.

- **[Exchange Online](#)**

Start here if you want to manage Exchange Online.

- **[Email migration](#)**

Start here if you want to migrate your email from pre-existing systems.

- **[Security & Compliance Center](#)**

Start here if you want to manage Security & Compliance Center features.

- **[Delegated Access Permissions \(DAP\) partners](#)**

Start here if you want to use Syndication and Cloud Solution Provider (CSP) partners to manage your Microsoft 365 customer tenants.

- **[Skype for Business Online](#)**

Start here to manage Skype for Business Online.

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Get started with PowerShell for Microsoft 365

Article • 01/24/2024

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

You can use commands and scripts in PowerShell for Microsoft 365 to manage Microsoft 365 and streamline your daily work. Use the following information to learn why PowerShell for Microsoft 365 is crucial to managing Microsoft 365, how to connect to your Microsoft 365 subscription and create reports, and where to get more information from the Microsoft 365 community.

Select from these topics:

- **[Why you need to use PowerShell for Microsoft 365](#)**

Start here if you're new to PowerShell for Microsoft 365. Learn why you should use PowerShell for Microsoft 365.

- **[Connect to Microsoft 365 with Microsoft Graph PowerShell](#)**

Start here to connect to your Microsoft 365 subscription by using PowerShell for Microsoft 365 and do administrative tasks from the command line.

- **[Connect to all Microsoft 365 services in a single PowerShell window](#)**

You can manage Microsoft 365 in separate windows for Skype for Business Online, SharePoint Online, Microsoft Exchange Online, and Microsoft 365 accounts and licenses. Or, you can manage them all from a single window. This article explains how.

- **[Use PowerShell to create reports in Microsoft 365](#)**

Start here if you've installed the PowerShell for Microsoft 365 modules and want to learn about using automation commands to create reports quickly.

- **[Cmdlet references for Microsoft 365 services](#)**

Learn about the cmdlets for the PowerShell for Microsoft 365 modules.

- **[Microsoft 365 community resources for PowerShell](#)**

Start here to connect to the PowerShell community and get more information about using PowerShell for Microsoft 365.

Related topics

[Manage Microsoft 365 with PowerShell](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Why you need to use PowerShell for Microsoft 365

Article • 04/15/2024

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

With the Microsoft 365 admin center, you can manage your Microsoft 365 user accounts and licenses. You can also manage your Microsoft 365 services, such as Exchange Online, Teams, and SharePoint. If you instead use PowerShell to manage these services, you can and take advantage of the command-line and scripting language environment for speed, automation, and additional capabilities.

Note

The Azure Active Directory module is being replaced by the Microsoft Graph PowerShell SDK. You can use the Microsoft Graph PowerShell SDK to access all Microsoft Graph APIs. For more information, see [Get started with the Microsoft Graph PowerShell SDK](#). Some PowerShell for Microsoft 365 commands in this article have been updated to use Microsoft Graph PowerShell.

This article shows how to use PowerShell to manage Microsoft 365 to:

- Reveal additional information that you can't see in the Microsoft 365 admin center
- Configure features and settings only possible with PowerShell
- Do bulk operations
- Filter data
- Print or save data
- Manage across services

Keep in mind that PowerShell for Microsoft 365 is a set of modules for Windows PowerShell, which is a command-line environment for Windows-based services and platforms. This environment creates a command-shell language that can be extended with additional modules. It provides a way to execute simple or complex commands or scripts. For example, after you install the PowerShell for Microsoft 365 modules and connect to your Microsoft 365 subscription, you can run the following command to list all the user mailboxes for Microsoft Exchange Online:

You could also get the list of mailboxes by using the Microsoft 365 admin center but counting the items in all the lists for all the sites for all of your web apps isn't easy.

PowerShell for Microsoft 365 is designed to help you manage Microsoft 365, not to replace the Microsoft 365 admin center. Admins need to be able to use PowerShell for Microsoft 365 because there are some configuration procedures that can only be done through PowerShell for Microsoft 365 commands. For these cases, you need to know how to:

- Install the PowerShell for Microsoft 365 modules (done only one time for each administrator computer).
- Connect to your Microsoft 365 subscription (one time for each PowerShell session).
- Gather the information needed to run the required PowerShell for Microsoft 365 commands.
- Run PowerShell for Microsoft 365 commands.

After you learn these basic skills, you don't have to list your mailbox users by using the **Get-Mailbox** command. You also don't have to understand how to create a new command like the command cited previously to count all the items in all the lists for all the sites for all of your web apps. Microsoft and the community of administrators can help you with such tasks as needed.

PowerShell for Microsoft 365 can reveal information that you can't see with the Microsoft 365 admin center

The Microsoft 365 admin center displays much useful information, but it doesn't display all the possible information that Microsoft 365 stores about users, licenses, mailboxes, and sites. Here's an example for *users and groups* in the Microsoft 365 admin center:

<input type="checkbox"/>	DISPLAY NAME ^	USER NAME	STATUS
<input type="checkbox"/>	Alex Darrow	AlexD@litwareinc.onmicrosoft.com	In cloud
<input type="checkbox"/>	Allie Bellew	AllieB@litwareinc.onmicrosoft.com	In cloud
<input type="checkbox"/>	Anne Wallace	AnneW@litwareinc.onmicrosoft.com	In cloud
<input type="checkbox"/>	Aziz Hassouneh	AzizH@litwareinc.onmicrosoft.com	In cloud
<input type="checkbox"/>	Belinda Newman	BelindaN@litwareinc.onmicrosoft.com	In cloud
<input type="checkbox"/>	Bonnie Kearney	BonnieK@litwareinc.onmicrosoft.com	In cloud
<input type="checkbox"/>	Brian Johnson (TAILSPIN)	BrianJ@litwareinc.onmicrosoft.com	In cloud

This view provides the information that you need in many cases. However, there are times when you need more. For example, Microsoft 365 licensing (and the Microsoft 365 features available to a user) depends in part on the user's geographic location. The policies and features that you can extend to a user who lives in the United States might not be the same as those that you can extend to a user in India or Belgium. Follow these steps in the Microsoft 365 admin center to determine a user's geographic location:

1. Double-click the user's **Display Name**.
2. In the user properties display pane, select **details**.
3. In the details display, select **additional details**.
4. Scroll until you find the heading **Country or region**:

ZIP or postal code:

Country or region:

5. Write the user's display name and location on a piece of paper, or copy and paste it into Notepad.

You must repeat this procedure for each user. If you have many users, this process can be tedious. With PowerShell, you can display this information for all of your users by using the following commands.

 **Note**

The Azure Active Directory module is being replaced by the Microsoft Graph PowerShell SDK. You can use the Microsoft Graph PowerShell SDK to access all Microsoft Graph APIs. For more information, see [Get started with the Microsoft Graph PowerShell SDK](#).

First, use a **Microsoft Entra DC admin** or **Cloud Application Admin** account to [connect to your Microsoft 365 tenant](#).

Getting information for a user requires the **User.ReadBasic.All** permission scope or one of the other permissions listed in the '[Assign license](#)' [Graph API reference page](#).

The **Organization.Read.All** permission scope is required to read the licenses available in the tenant.

 **Note**

Azure AD and MSOnline PowerShell modules are deprecated as of March 30, 2024. To learn more, read the [deprecation update](#). After this date, support for these modules are limited to migration assistance to Microsoft Graph PowerShell SDK and security fixes. The deprecated modules will continue to function through March, 30 2025.

We recommend migrating to [Microsoft Graph PowerShell](#) to interact with Microsoft Entra ID (formerly Azure AD). For common migration questions, refer to the [Migration FAQ](#). Note: Versions 1.0.x of MSOnline may experience disruption after June 30, 2024.

PowerShell

```
Connect-MgGraph -Scopes "User.ReadBasic.All"
Get-MgUser -All -Property DisplayName, UsageLocation | Select DisplayName,
UsageLocation
```

Here's an example of the results:

PowerShell

DisplayName	UsageLocation
-----	-----
Bonnie Kearney	GB
Fabrice Canel	BR

Brian Johnson (TAILSPIN)	US
Anne Wallace	US
Alex Darrow	US
David Longmuir	BR

The interpretation of this PowerShell command is: Get all of the users in the current Microsoft 365 subscription (**Get-MgUser**), but only display the name and location for each user (**Select DisplayName, UsageLocation**).

Because PowerShell for Microsoft 365 supports a command-shell language, you can further manipulate the information obtained by the **Get-MgUser** command. For example, maybe you'd like to sort these users by their location, grouping all the Brazilian users together, all the United States users together, and so on. Here's the command:

PowerShell

```
Get-MgUser -All -Property DisplayName, UsageLocation | Select DisplayName,
UsageLocation | Sort UsageLocation, DisplayName
```

Here's an example of the results:

PowerShell

DisplayName	UsageLocation
-----	-----
David Longmuir	BR
Fabrice Canel	BR
Bonnie Kearney	GB
Alex Darrow	US
Anne Wallace	US
Brian Johnson (TAILSPIN)	US

The interpretation of this PowerShell command is: Get all the users in the current Microsoft 365 subscription, but only display the name and location for each user and sort them first by their location and then their name (**Sort UsageLocation, DisplayName**).

You can also use additional filtering. For example, if you only want to see information about users based in Brazil, use this command:

PowerShell

```
Get-MgUser -All -Property DisplayName, Country | Where-Object {$_ .Country -
eq "BR"} | Select DisplayName, Country
```

Here's an example of the results:

PowerShell	
DisplayName	UsageLocation
-----	-----
David Longmuir	BR
Fabrice Canel	BR

The interpretation of this PowerShell command is: Get all the users in the current Microsoft 365 subscription whose location is Brazil (**Where {\$_._UsageLocation -eq "BR"}**) and then display the name and location for each user.

A note about large domains

If you have a large domain with tens of thousands of users, trying some of the examples we show in this article could lead to throttling. Based on factors like computing power and available network bandwidth, you may be trying to do too much at one time. Large organizations might want to split some of these PowerShell operations into two commands.

For example, the following command returns all the user accounts and shows the name and location for each:

PowerShell	
<code>Get-MgUser -All Select DisplayName, UsageLocation</code>	

That works great for smaller domains. But in a large organization, you might want to split that operation into two commands: one command to store the user account information in a variable and another to display the needed information. Here's an example:

PowerShell	
<code>\$x = Get-MgUser -All -Property DisplayName, UsageLocation \$x Select DisplayName, UsageLocation</code>	

The interpretation of this set of PowerShell commands is:

1. Get all the users in the current Microsoft 365 subscription and store the information in a variable named \$x (`$x = Get-MgUser`).
2. Display the contents of the variable \$x, but only include the name and location for each user (`$x | Select DisplayName, UsageLocation`).

Microsoft 365 has features that you can only configure with PowerShell for Microsoft 365

The Microsoft 365 admin center is intended to provide access to common, useful administrative tasks that apply to most environments. In other words, the Microsoft 365 admin center was designed so that the typical administrator can carry out the most-common management tasks. But there are some tasks that can't be done in the admin center.

For example, the Skype for Business Online admin center provides a few options for creating custom meeting invitations:

You can customize Lync meeting invitations to meet your organization's needs. You have one. You can also add legal disclaimers by providing the link to a website with

Logo URL:

Help URL:

Legal URL:

Footer text:

With these settings, you can add a touch of personalization and professionalism to meeting invitations. But there's more to meeting-configuration settings than simply creating custom meeting invitations. For example, by default, meetings allow:

- Anonymous users to gain automatic entrance to each meeting.
- Attendees to record the meeting.
- All users from your organization to be designated as presenters when they join the meeting.

These settings aren't available from the Skype for Business Online admin center. You can control them from PowerShell for Microsoft 365. Here's a command that disables these

three settings:

PowerShell

```
Set-CsMeetingConfiguration -AdmitAnonymousUsersByDefault $False -  
AllowConferenceRecording $False -DesignateAsPresenter "None"
```

 **Note**

To run this command, you must install the [Skype for Business Online PowerShell Module](#).

The interpretation of this PowerShell command is:

1. In the settings for new Skype for Business Online meetings (**Set-CsMeetingConfiguration**), disable allowing anonymous users to gain automatic entrance to meetings (-**AdmitAnonymousUsersByDefault \$False**).
2. Disable the ability for attendees to record meetings (-**AllowConferenceRecording \$False**).
3. Don't designate all users from your organization as presenters (-**DesignateAsPresenter "None"**).

To restore these default settings (enable the options), run this command:

PowerShell

```
Set-CsMeetingConfiguration -AdmitAnonymousUsersByDefault $True -  
AllowConferenceRecording $True -DesignateAsPresenter "Company"
```

There are other similar scenarios as well, which is why administrators should know how to run PowerShell for Microsoft 365 commands.

PowerShell for Microsoft 365 is great for bulk operations

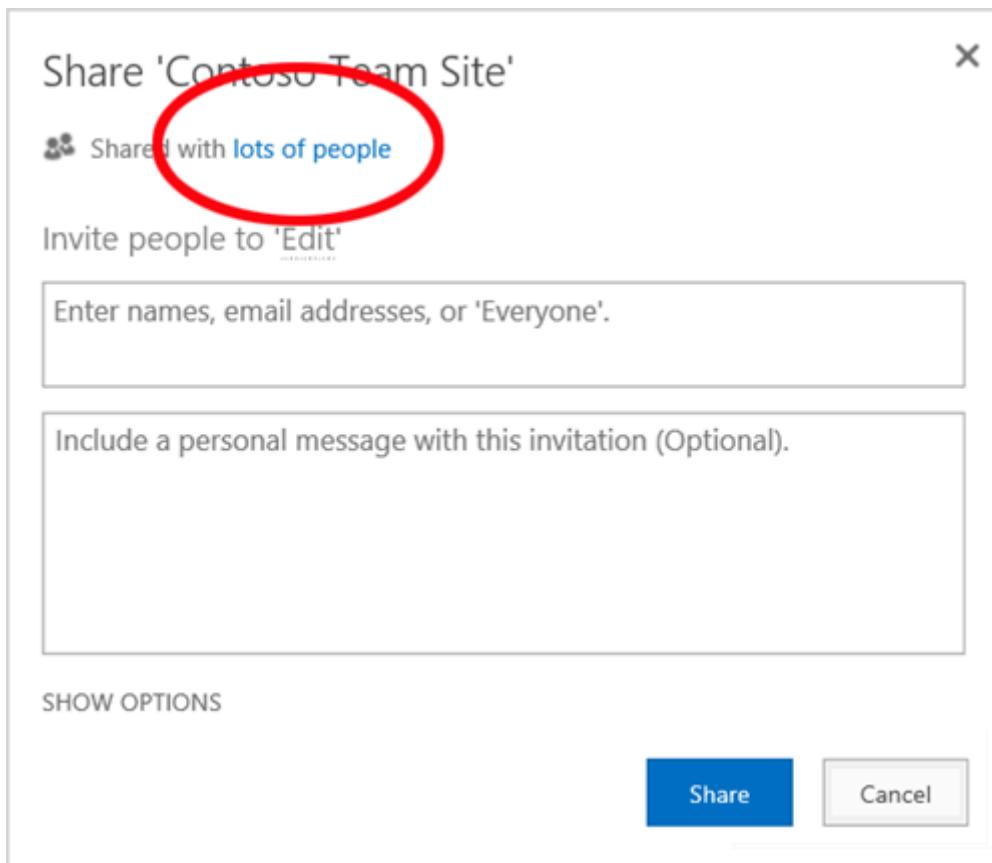
Visual interfaces like the Microsoft 365 admin center are most valuable when you have a single operation to do. For example, if you need to disable one user account, you can use the admin center to quickly locate and clear a checkbox. This may be easier than performing a similar operation in PowerShell.

But if you have to change many things or some selected things within a large set of other things, the Microsoft 365 admin center might not be the best tool. For example,

say you have to change the prefix on thousands of phone numbers or remove the specific user *Ken Myer* from all your SharePoint sites. How would you do that in the Microsoft 365 admin center?

For the last example, say you have several hundred SharePoint sites, and you don't know which ones Ken Meyer is a member of. You would have to start at the Microsoft 365 admin center and then perform this procedure for each site:

1. Select the **URL** of the site.
2. In the **site collection properties** box, select the **Web Site Address** link to open the site.
3. On the site, select **Share**.
4. In the **Share** dialog box, select the link that shows all the users who have permissions to the site:



5. In the **Shared With** dialog box, select **Advanced**.
6. Scroll down the list of users, find and select Ken Myer (assuming he has permissions to the site), and then select **Remove User Permissions**.

This would take a *long* time for several hundred sites.

The alternative is to run the following command in PowerShell for Microsoft 365 to remove Ken Myer from all your sites:

```
PowerShell
```

```
Get-SPOSite | ForEach {Remove-SPOUser -Site $_.Url -LoginName  
"kenmyer@litwareinc.com"}
```

① Note

This command requires that you install the [SharePoint PowerShell module](#).

The interpretation of this PowerShell command is: Get all of the SharePoint sites in the current Microsoft 365 subscription (**Get-SPOSite**) and for each site remove Ken Meyer from the list of users who can access it (**ForEach {Remove-SPOUser -Site \$_.Url ->LoginName "kenmyer@litwareinc.com"}**).

We tell Microsoft 365 to remove Ken Meyer from every site, including those that he doesn't have access to. So the results will show errors for those sites that he doesn't have access to. We can use an additional condition on this command to remove Ken Meyer only from the sites that have him on their sign in list. But the errors that are returned cause no harm to the sites themselves. This command might take a few minutes to run against hundreds of sites, rather than hours of working through the Microsoft 365 admin center.

Here's another bulk operation example. Use this command to add *Bonnie Kearney*, a new SharePoint administrator, to all sites in the organization:

```
PowerShell
```

```
Get-SPOSite | ForEach {Add-SPOUser -Site $_.Url -LoginName  
"bkearney@litwareinc.com" -Group "Members"}
```

The interpretation of this PowerShell command is: Get all the SharePoint sites in the current Microsoft 365 subscription and for each site allow Bonnie Kearney access by adding her sign in name to the Members group of the site (**ForEach {Add-SPOUser -Site \$_.Url -LoginName "bkearney@litwareinc.com" -Group "Members"}**).

PowerShell for Microsoft 365 is great at filtering data

The Microsoft 365 admin center provides several ways to filter your data to easily locate a targeted subset of information. For example, Exchange makes it easy to filter on practically any property of a user mailbox. For example, here's the list of mailboxes for all the users who live in the city of Bloomington:

The screenshot shows the 'Advanced Search -- Webpage Dialog' window. At the top, there are tabs for 'InPrivate' and a URL bar showing 'https://outlook.office365.com/ecp/UsersGroups/EditRecipientAdvFilter.aspx?FeatureSet=Mailboxes'. On the right side of the header are 'Help' and a close button ('X'). Below the header, the text 'advanced search' is displayed. A note says 'Filter out recipients based on these conditions. You can use this filter to add more conditions.' with a 'Learn more' link. To the left of a list of filter options are checkboxes for 'Alias:', 'Display name:', 'Department:', 'Email addresses:', 'First name:', 'Last name:', and 'Recipient types:'. To the right of these checkboxes is a dropdown menu set to 'User mailbox'. Below this section is a search interface with a 'City' dropdown containing 'Bloomington' and an 'add a condition' button. The entire search interface is highlighted with a pink rectangular box. At the bottom right are 'ok' and 'cancel' buttons.

The [Exchange admin center](#) also lets you combine filter criteria. For example, you can find the mailboxes for all the people who live in Bloomington and work in the Finance department.

But there are limitations to what you can do in the Exchange Admin center. For example, you couldn't as easily find the mailboxes of people who live in Bloomington or San Diego, or the mailboxes for all people who don't live in Bloomington.

You can use the following PowerShell for Microsoft 365 command to get a list of mailboxes for all the people who live in Bloomington or San Diego:

```
PowerShell

Get-User | Where {$_.RecipientTypeDetails -eq "UserMailbox" -and ($_.City -eq "San Diego" -or $_.City -eq "Bloomington")} | Select DisplayName, City
```

Here's an example of the results:

PowerShell

DisplayName	City
Alex Darrow	San Diego
Bonnie Kearney	San Diego
Julian Isla	Bloomington
Rob Young	Bloomington

The interpretation of this PowerShell command is: Get all the users in the current Microsoft 365 subscription who have a mailbox in the city of San Diego or Bloomington (`Where {$_.RecipientTypeDetails -eq "UserMailbox" -and ($_.City -eq "San Diego" -or $_.City -eq "Bloomington")}`), and then display the name and city for each (`Select DisplayName, City`).

And here's the command to list all the mailboxes for people who live anywhere except Bloomington:

PowerShell

```
Get-User | Where {$_.RecipientTypeDetails -eq "UserMailbox" -and $_.City -ne "Bloomington"} | Select DisplayName, City
```

Here's an example of the results:

PowerShell

DisplayName	City
MOD Administrator	Redmond
Alex Darrow	San Diego
Allie Bellew	Bellevue
Anne Wallace	Louisville
Aziz Hassouneh	Cairo
Belinda Newman	Charlotte
Bonnie Kearney	San Diego
David Longmuir	Waukesha
Denis Dehenne	Birmingham
Garret Vargas	Seattle
Garth Fort	Tulsa
Janet Schorr	Bellevue

The interpretation of this PowerShell command is: Get all the users in the current Microsoft 365 subscription who have a mailbox not located in the city of Bloomington (`Where {$_.RecipientTypeDetails -eq "UserMailbox" -and $_.City -ne "Bloomington"}`), and then display the name and city for each.

Use wildcards

You can also use wildcard characters in your PowerShell filters to match part of a name. For example, suppose you're looking for a user account. All you can remember is that the user's last name was *Anderson* or maybe *Henderson* or *Jorgenson*.

You could track down that user in the Microsoft 365 admin center by using the search tool and carrying out three different searches:

- One for *Anderson*
- One for *Henderson*
- One for *Jorgenson*

Because all three of these names end in "son", you can tell PowerShell to display all the users whose name ends in "son". Here's the command:

PowerShell

```
Get-User -Filter '{LastName -like "*son"}'
```

The interpretation of this PowerShell command is: Get all the users in the current Microsoft 365 subscription, but use a filter that only lists the users whose last names end in "son" (-Filter '{LastName -like "*son"}'). The * stands for any set of characters, which are letters in the user's last name.

PowerShell for Microsoft 365 makes it easy to print or save data

The Microsoft 365 admin center lets you view lists of data. Here's an example of the Skype for Business Online admin center displaying a list of users who have been enabled for Skype for Business Online:



<input type="checkbox"/>	DISPLAY NAME	USER NAME	LOCATION
<input type="checkbox"/>	Alex Darrow	AlexD@litwareinc.onmicrosoft.com	US
<input type="checkbox"/>	Allie Bellew	AllieB@litwareinc.onmicrosoft.com	US
<input type="checkbox"/>	Anne Wallace	AnneW@litwareinc.onmicrosoft.com	US
<input type="checkbox"/>	Aziz Hassouneh	AzizH@litwareinc.onmicrosoft.com	US
<input type="checkbox"/>	Belinda Newman	BelindaN@litwareinc.onmicrosoft.com	US
<input type="checkbox"/>	Bonnie Kearney	BonnieK@litwareinc.onmicrosoft.com	US
<input type="checkbox"/>	David Longmuir	DavidL@litwareinc.onmicrosoft.com	US
<input type="checkbox"/>	Denis Dehenne	DenisD@litwareinc.onmicrosoft.com	US
<input type="checkbox"/>	Dorena Paschke	DorenaP@litwareinc.onmicrosoft.com	US

To save that information to a file, you must paste it into a document or Microsoft Excel worksheet. Either case might require additional formatting. Additionally, the Microsoft 365 admin center doesn't provide a way to directly print the displayed list.

Fortunately, you can use PowerShell to not only display the list but to save it to a file that can be easily imported into Excel. Here's an example command to save Skype for Business Online user data to a comma-separated values (CSV) file, which can then be easily imported as a table in an Excel worksheet:

PowerShell

```
Get-CsOnlineUser | Select DisplayName, UserPrincipalName, UsageLocation |
Export-Csv -Path "C:\Logs\SfBUsers.csv" -NoTypeInformation
```

Here's an example of the results:

	A	B	C
1	DisplayName	UserPrincipalName	UsageLocation
2	Alex Darrow	AlexD@litwareinc.onmicrosoft.com	US
3	Allie Bellew	AllieB@litwareinc.onmicrosoft.com	US
4	Anne Wallace	AnneW@litwareinc.onmicrosoft.com	US
5	Aziz Hassouneh	AzizH@litwareinc.onmicrosoft.com	US
6	Belinda Newman	BelindaN@litwareinc.onmicrosoft.com	US
7	Bonnie Kearney	BonnieK@litwareinc.onmicrosoft.com	US
8	David Longmuir	DavidL@litwareinc.onmicrosoft.com	US
9	Denis Dehenne	DenisD@litwareinc.onmicrosoft.com	US
10	Garret Vargas	GarretV@litwareinc.onmicrosoft.com	US
11	Garth Fort	GarthF@litwareinc.onmicrosoft.com	US
12	Janet Schorr	JanetS@litwareinc.onmicrosoft.com	US

The interpretation of this PowerShell command is: Get all the Skype for Business Online users in the current Microsoft 365 subscription (**Get-CsOnlineUser**); obtain only the user name, UPN, and location (**Select DisplayName, UserPrincipalName, UsageLocation**); and then save that information in a CSV file named C:\Logs\SfBUsers.csv (**Export-Csv -Path "C:\Logs\SfBUsers.csv" -NoTypeInformation**).

You can also use options to save this list as an XML file or an HTML page. In fact, with additional PowerShell commands, you could save it directly as an Excel file, with any custom formatting you want.

You can also send the output of a PowerShell command that displays a list directly to the default printer in Windows. Here's an example command:

```
PowerShell

Get-CsOnlineUser | Select DisplayName, UserPrincipalName, UsageLocation |
Out-Printer
```

Here's what your printed document will look like:

DisplayName	UserPrincipalName	UsageLocation
Alex Darrow	AlexD@litwareinc.onmicrosoft.com	US
Allie Bellew	AllieB@litwareinc.onmicrosoft.com	US
Anne Wallace	AnneW@litwareinc.onmicrosoft.com	US
Aziz Hassouneh	AzizH@litwareinc.onmicrosoft.com	US
Belinda Newman	BelindaN@litwareinc.onmicrosoft.com	US
Bonnie Kearney	BonnieK@litwareinc.onmicrosoft.com	US
David Longmuir	DavidL@litwareinc.onmicrosoft.com	US
Denis Dehenne	DenisD@litwareinc.onmicrosoft.com	US
Garret Vargas	GarretV@litwareinc.onmicrosoft.com	US
Garth Fort	GarthF@litwareinc.onmicrosoft.com	US
Janet Schorr	JanetS@litwareinc.onmicrosoft.com	US

The interpretation of this PowerShell command is: Get all the Skype for Business Online users in the current Microsoft 365 subscription; obtain only the user name, UPN, and location; and then send that information to the default Windows printer (**Out-Printer**).

The printed document has the same simple formatting as the display in the PowerShell command window. To get a hard copy, just add | **Out-Printer** to the end of the command.

PowerShell for Microsoft 365 lets you manage across server products

The components that make up Microsoft 365 are designed to work together. For example, suppose you add a new user to Microsoft 365, and you specify such information as the user's department and phone number. That information will then be available if you access the user's information in any of the Microsoft 365 services: Skype for Business Online, Exchange, or SharePoint.

But that's for common information that spans the suite of products. Product-specific information, such as information about a user's Exchange mailbox, isn't typically available across the suite. For example, information about whether a user's mailbox is enabled or not is available only in the Exchange admin center.

Suppose you'd like to make a report that shows the following information for all your users:

- The user's display name
- Whether the user is licensed for Microsoft 365
- Whether the user's Exchange mailbox has been enabled
- Whether the user is enabled for Skype for Business Online

You can't easily produce such a report in the Microsoft 365 admin center. Instead, you would have to create a separate document to store the information, such as an Excel worksheet. Then, get all the user names and licensing information from the Microsoft 365 admin center, get mailbox information from the [Exchange admin center](#), get Skype for Business Online information from the Skype for Business Online Admin center, and then combine that information.

The alternative is to use a PowerShell script to compile the report for you.

The following example script is more complicated than the commands you've seen so far in this article. But, it shows the potential of using PowerShell to create information views that are difficult to get otherwise. Here's the script to compile and display the list you need:

PowerShell

```
Connect-MgGraph -Scopes "User.ReadBasic.All"
$x = Get-MgUser -All

foreach ($i in $x)
{
    $y = Get-Mailbox -Identity $i.UserPrincipalName
    $i | Add-Member -MemberType NoteProperty -Name IsMailboxEnabled -Value
$y.IsMailboxEnabled

    $y = Get-CsOnlineUser -Identity $i.UserPrincipalName
    $i | Add-Member -MemberType NoteProperty -Name EnabledForSfB -Value
$y.Enabled
}

$x | Select DisplayName, IsLicensed, IsMailboxEnabled, EnabledforSfB
```

Here's an example of the results:

PowerShell

DisplayName	IsLicensed	IsMailboxEnabled	EnabledForSfB
Bonnie Kearney	True	True	True
Fabrice Canel	True	True	True
Brian Johnson	False	True	False
Anne Wallace	True	True	True
Alex Darrow	True	True	True
David Longmuir	True	True	True
Katy Jordan	False	True	False
Molly Dempsey	False	True	False

The interpretation of this PowerShell script is:

1. Get all the users in the current Microsoft 365 subscription and store the information in a variable that's named \$x (`$x = Get-MgUser`).
2. Start a loop that runs over all the users in the variable \$x (`foreach ($i in $x)`).
3. Define a variable named \$y and store the user's mailbox information in it (`$y = Get-Mailbox -Identity $i.UserPrincipalName`).
4. Add a new property to the user information that's named *IsMailBoxEnabled*. Set it to the value of the IsMailBoxEnabled property of the user's mailbox (`$i | Add-Member -MemberType NoteProperty -Name IsMailboxEnabled -Value $y.IsMailboxEnabled`).
5. Define a variable named \$y, and store the user's Skype for Business Online information in it (`$y = Get-CsOnlineUser -Identity $i.UserPrincipalName`).
6. Add a new property to the user information that's named *EnabledForSfB*. Set it to the value of the Enabled property of the user's Skype for Business Online information (`$i | Add-Member -MemberType NoteProperty -Name EnabledForSfB -Value $y.Enabled`).
7. Display the list of users, but include only their name, whether they're licensed, and the two new properties that indicate whether their mailbox is enabled and whether they're enabled for Skype for Business Online (`$x | Select DisplayName, IsLicensed, IsMailboxEnabled, EnabledforSfB`).

See also

[Get started with PowerShell for Microsoft 365](#)

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Use Windows PowerShell to create reports in Microsoft 365](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Connect to Microsoft 365 with Microsoft Graph PowerShell

Article • 02/01/2024

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Microsoft Graph PowerShell enables you to manage your Microsoft 365 settings from the command line. This article shows you how to install the required software and then connect to your Microsoft 365 organization using the Microsoft Graph PowerShell SDK.

Currently, the Azure Active Directory PowerShell for Graph module doesn't completely replace the functionality of the Microsoft Azure Active Directory module for Windows PowerShell for application proxy management, user, and contact administration. In some cases, you need to use both versions. You can safely install both versions on the same computer.

What do you need to know before you begin?

Note

The Azure Active Directory (AzureAD) PowerShell module is being deprecated and replaced by the Microsoft Graph PowerShell SDK. You can use the Microsoft Graph PowerShell SDK to access all Microsoft Graph APIs. For more information, see [Get started with the Microsoft Graph PowerShell SDK](#).

Also see [Install the Microsoft Graph PowerShell SDK](#) and [Upgrade from Azure AD PowerShell to Microsoft Graph PowerShell](#) for information on how to install and upgrade to Microsoft Graph PowerShell, respectively.

Prerequisites

PowerShell 7 and later is the recommended PowerShell version for use with the Microsoft Graph PowerShell SDK on all platforms. There are no other prerequisites to use the SDK with PowerShell 7 or later.

The following prerequisites are required to use the Microsoft Graph PowerShell SDK with Windows PowerShell.

- Upgrade to PowerShell 5.1 or later

- Install .NET Framework 4.7.2 or later
- Update PowerShellGet to the latest version using `Install-Module PowerShellGet`

The PowerShell script execution policy must be set to remote signed or less restrictive. Use `Get-ExecutionPolicy` to determine the current execution policy. For more information, see [about_Execution_Policies](#). To set the execution policy, run:

```
PowerShell
```

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser
```

Operating system

You must use a 64-bit version of Windows. You can use the following versions of Windows:

- Windows 11, Windows 10, Windows 8.1, Windows 8, or Windows 7 Service Pack 1 (SP1)
- Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2 SP1

 **Note**

For Windows 8.1, Windows 8, Windows 7 Service Pack 1 (SP1), Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2 SP1, download and install the [Windows Management Framework 5.1](#).

To use Microsoft Graph PowerShell, you must use at least PowerShell version 5.1.

 **Note**

These procedures are intended for users who are members of a Microsoft 365 admin role. For more information, see [About admin roles](#).

Connect with Microsoft Graph PowerShell

In this section, you'll learn how to connect to your Microsoft 365 organization using the Microsoft Graph PowerShell SDK. You can visit [Install the Microsoft Graph PowerShell SDK](#) for more guidance.

Step 1: Install the required software

The Microsoft Graph PowerShell SDK is published in the [PowerShell Gallery](#).

These steps are required only one time on your computer. However, you'll likely need to update the software periodically.

Install the Microsoft Graph PowerShell SDK and beta module

The Microsoft Graph PowerShell SDK comes in two modules, `Microsoft.Graph` and `Microsoft.Graph.Beta`, that you'll install separately. These modules call the Microsoft Graph v1.0 and Microsoft Graph beta endpoints, respectively. You can install the two modules on the same PowerShell version.

1. Open a Windows PowerShell Command Prompt window. Depending on the permissions of your logged-in account, you may need to open the PowerShell window in Administrator mode.
2. To install the v1 module of the SDK in PowerShell Core or Windows PowerShell, run the following command:

```
PowerShell  
  
Install-Module Microsoft.Graph -Scope CurrentUser
```

3. Run this command to install the beta module:

```
PowerShell  
  
Install-Module Microsoft.Graph.Beta
```

After the installation is completed, you can verify the installed version with the following command:

```
Azure PowerShell  
  
Get-InstalledModule Microsoft.Graph
```

Step 2: Connect to your Microsoft 365 subscription

The PowerShell SDK supports two types of authentication: delegated access, and app-only access. In this guide, you'll use delegated access to sign in as a user, grant consent

to the SDK to act on your behalf, and call the Microsoft Graph.

For details on using app-only access for unattended scenarios, see [Use app-only authentication with the Microsoft Graph PowerShell SDK](#).

Determine required permission scopes

Each API in the Microsoft Graph is protected by one or more permission scopes. The user logging in must consent to one of the required scopes for the APIs you plan to use. In this example, we'll use the following APIs.

- List users to find the user ID of the logged-in user.
- List joinedTeams to get the Teams the user is a member of.
- List channels to get the channels in a Team.
- Send message to send a message to a Team's channel.

The **User.Read.All** permission scope enables the first two calls, and the **Group.ReadWrite.All** scope enables the rest. These permissions require an admin account.

For more information about how to determine what permission scopes you'll need, see [Using Find-MgGraphCommand](#).

To connect to your Microsoft 365 Organization, run the following command:

PowerShell

```
Connect-MgGraph -Scopes "User.Read.All", "Group.ReadWrite.All"
```

The command prompts you to go to a web page to sign in with your credentials. Once you've done that, the command indicates success with a **Welcome To Microsoft Graph!** message. You only need to sign in once per session.

Tip

You can accretively add permissions by repeating the **Connect-MgGraph** command with the new permission scopes.

See also

- [Manage Microsoft 365 with PowerShell](#)
- [Get started with the Microsoft Graph PowerShell SDK](#)

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Connect to all Microsoft 365 services in a single PowerShell window

Article • 01/23/2024

When you use PowerShell to manage Microsoft 365, you can have multiple PowerShell sessions open at the same time. You might have different PowerShell windows to manage user accounts, SharePoint Online, Exchange Online, Microsoft Teams, Microsoft Defender for Office 365 features (security), and Microsoft Purview compliance features.

This scenario isn't optimal for managing Microsoft 365, because you can't exchange data among those windows for cross-service management. This article describes how to use a single instance of PowerShell to manage Microsoft 365 accounts, Exchange Online, SharePoint Online, Microsoft Teams, and features in Defender for Office 365 Microsoft Purview compliance.

ⓘ Note

This article currently only contains the commands to connect to the Worldwide (+GCC) cloud. Notes provide links to articles about connecting to the other Microsoft 365 clouds.

Before you begin

Before you can manage all of Microsoft 365 from a single instance of PowerShell, consider the following prerequisites:

- The Microsoft 365 work or school account that you use must be a member of a Microsoft 365 admin role. For more information, see [About admin roles](#). This is a requirement for PowerShell for Microsoft 365, but not necessarily for all other Microsoft 365 services.
- You can use the following 64-bit versions of Windows:
 - Windows 11
 - Windows 10
 - Windows 8.1 or Windows 8
 - Windows Server 2019

- Windows Server 2016
 - Windows Server 2012 R2 or Windows Server 2012
 - Windows 7 Service Pack 1 (SP1)*
 - Windows Server 2008 R2 SP1*
- * You need to install Microsoft .NET Framework 4.5.x and then Windows Management Framework 3.0 or 4.0. For more information, see [Windows Management Framework](#).
- You need to install the modules that are required for Microsoft Entra ID, Exchange Online, Defender for Office 365, Microsoft Purview compliance, SharePoint Online, and Teams:
 - [Install the Microsoft Graph PowerShell SDK](#)
 - [SharePoint Online Management Shell](#)
 - [Teams PowerShell Module](#)
 - [Install and maintain the Exchange Online PowerShell module](#)
 - [Teams PowerShell Overview](#)
 - PowerShell must be configured to run signed scripts for Exchange Online, Defender for Office 365, and Microsoft Purview compliance. Run the following command in an elevated PowerShell session (a PowerShell session that you **Run as administrator**).

```
PowerShell
Set-ExecutionPolicy RemoteSigned
```

Connection steps

Follow these steps to connect to all the services in a single PowerShell window.

1. Open Windows PowerShell.
2. Run this command and enter your Microsoft 365 work or school account credentials.

```
PowerShell
$credential = Get-Credential
```

3. Run this command to connect to Microsoft Entra ID by using the Microsoft Graph PowerShell SDK.

 **Note**

The Azure Active Directory (AzureAD) PowerShell module is being deprecated and replaced by the Microsoft Graph PowerShell SDK. You can use the Microsoft Graph PowerShell SDK to access all Microsoft Graph APIs. For more information, see [Get started with the Microsoft Graph PowerShell SDK](#).

Also see [Install the Microsoft Graph PowerShell SDK](#) and [Upgrade from Azure AD PowerShell to Microsoft Graph PowerShell](#) for information on how to install and upgrade to Microsoft Graph PowerShell, respectively.

The Microsoft Graph PowerShell SDK supports two types of authentication: delegated access, and app-only access. In this example, you'll use delegated access to sign in as a user, grant consent to the SDK to act on your behalf, and call the Microsoft Graph.

For details on using app-only access for unattended scenarios, see [Use app-only authentication with the Microsoft Graph PowerShell SDK](#).

Determine required permission scopes

Each API in the Microsoft Graph is protected by one or more permission scopes. The user logging in must consent to one of the required scopes for the APIs you plan to use. In this example, we'll use the following APIs.

- List users to find the user ID of the logged-in user.
- List joinedTeams to get the Teams the user is a member of.
- List channels to get the channels in a Team.
- Send message to send a message to a Team's channel.

The **User.Read.All** permission scope enables the first two calls, and the **Group.ReadWrite.All** scope enables the rest. These permissions require an admin account.

For more information about how to determine what permission scopes you'll need, see [Using Find-MgGraphCommand](#).

Connect to Microsoft Graph

To connect to your Microsoft 365 Organization, run the following command with example permission scopes:

PowerShell

```
Connect-MgGraph -Scopes "User.Read.All","Group.ReadWrite.All"
```

The command prompts you to go to a web page to sign in with your credentials. Once you've done that, the command indicates success with a **Welcome To Microsoft Graph!** message. You only need to sign in once per session. Passing credentials to the `Connect-MgGraph` cmdlet is currently not supported.

 **Tip**

You can accretively add permissions by repeating the `Connect-MgGraph` command with the new permission scopes.

4. Run these commands to connect to SharePoint Online. Specify the organization name for your domain. For example, for "litwareinc.onmicrosoft.com", the organization name value is "litwareinc".

PowerShell

```
$orgName=<for example, litwareinc for litwareinc.onmicrosoft.com>
Import-Module Microsoft.Online.SharePoint.PowerShell -
DisableNameChecking
Connect-SPOService -Url https://$orgName-admin.sharepoint.com -
Credential $Credential
```

5. Run these commands to connect to Exchange Online.

PowerShell

```
Import-Module ExchangeOnlineManagement
Connect-ExchangeOnline -ShowProgress $true
```

 **Note**

To connect to Exchange Online for Microsoft 365 clouds other than Worldwide, see [Connect to Exchange Online PowerShell](#).

6. Run these commands to connect to Security & Compliance PowerShell.

PowerShell

```
$acctName=<UPN of the account, such as  
belindan@litwareinc.onmicrosoft.com>"  
Connect-IPPSession -UserPrincipalName $acctName
```

ⓘ Note

To connect to Security & Compliance PowerShell for Microsoft 365 clouds other than Worldwide, see [Connect to Security & Compliance PowerShell](#).

7. Run these commands to connect to Teams PowerShell.

PowerShell

```
Import-Module MicrosoftTeams  
$credential = Get-Credential  
Connect-MicrosoftTeams -Credential $credential
```

ⓘ Note

Skype for Business Online Connector is currently part of the latest Teams PowerShell module. If you're using the latest Teams PowerShell public release, you don't need to install the Skype for Business Online Connector.

To connect to Microsoft Teams clouds other than *Worldwide*, see [Connect-MicrosoftTeams](#).

Close the PowerShell window

To close down the PowerShell window, run this command to remove the active sessions to SharePoint Online, Teams, Defender for Office 365 and Microsoft Purview compliance:

PowerShell

```
Disconnect-SPOSERVICE; Disconnect-MicrosoftTeams; Disconnect-ExchangeOnline
```

See also

- [Connect to Microsoft 365 with Microsoft Graph PowerShell](#)
- [Manage SharePoint Online with PowerShell](#)

- Manage Microsoft 365 user accounts, licenses, and groups with PowerShell
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Use PowerShell to create reports for Microsoft 365

Article • 06/27/2024

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Many different reports are available in the Microsoft 365 admin center. But these reports only provide so much information, and sometimes you need more. That's when you need PowerShell for Microsoft 365.

These articles describe how to use PowerShell for Microsoft 365 to get information from your Microsoft 365 tenant:

- Get started with reporting using PowerShell for Microsoft 365:
 - [Why you need to use PowerShell for Microsoft 365](#)
- Reports for user accounts and licenses:
 - [View Microsoft 365 licenses and services with PowerShell](#)
 - [View Microsoft 365 licensed and unlicensed users with PowerShell](#)
 - [View Microsoft 365 account license and service details with PowerShell](#)
 - [View Microsoft 365 user accounts with PowerShell](#)
- Reports for SharePoint:
 - [Get started with SharePoint Management Shell](#)
 - [Get-SPOSiteGroup - Gets all the groups on a specified site collection](#)
- Reports for Exchange Online:
 - [Use Exchange Online PowerShell to display mailbox](#)

Related articles

[Manage Microsoft 365 with PowerShell](#)

[Get started with PowerShell for Microsoft 365](#)

[Manage SharePoint with PowerShell](#)

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Cmdlet references for Microsoft 365 services

Article • 06/27/2024

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

This article provides cmdlet references for the various Microsoft 365 services and connection instructions for each Microsoft 365 service that PowerShell supports.

ⓘ Note

To connect to all services at once, see [Connect to all Microsoft 365 services in a single Windows PowerShell window](#).

Microsoft Graph PowerShell cmdlets

The [Microsoft Graph PowerShell](#) for Graph cmdlet reference topics are in the Reference section of the Microsoft Graph PowerShell for Graph documentation.

For Microsoft 365 PowerShell connection instructions, see [Connect to Microsoft 365 with PowerShell](#).

Exchange Online PowerShell cmdlets

Exchange Online cmdlet reference topics are in the Reference section of the [Exchange Online PowerShell](#) documentation.

For connection instructions for Exchange Online PowerShell, see [Connect to Exchange Online PowerShell](#).

ⓘ Note

Reporting cmdlets for other services, such as SharePoint Online, Skype for Business Online, and Microsoft 365 user activity, are available in Exchange Online PowerShell. For more information, see [Reporting cmdlets in Exchange Online](#).

SharePoint Online PowerShell cmdlets

For SharePoint Online cmdlets, see [Index of Windows PowerShell for SharePoint Online cmdlets](#).

For connection instructions for SharePoint Online PowerShell, see [Set up the SharePoint Online Management Shell Windows PowerShell environment](#).

Skype for Business Online PowerShell cmdlets

For Skype for Business Online cmdlet reference topics, see [Skype for Business Online cmdlets](#).

For connection instructions for Skype for Business Online PowerShell, see [Manage Skype for Business Online with PowerShell](#).

Security & Compliance PowerShell cmdlets

The Security & Compliance Center cmdlet references are in the Reference section of the [Security & Compliance PowerShell documentation](#).

For connection instructions for Security & Compliance PowerShell, see [Connect to the Security & Compliance PowerShell](#).

See also

[Manage Microsoft 365 with PowerShell](#)

[Get started with PowerShell for Microsoft 365](#)

Feedback

Was this page helpful?



[Provide product feedback](#)

Microsoft 365 community resources for PowerShell

Article • 07/31/2024

Connect to these communities to reach your peers and get answers for your PowerShell for Microsoft 365 questions.

- [Microsoft 365 Microsoft Tech Community ↗](#)
- [Exchange Server TechNet community forum ↗](#)

See also

[Manage Microsoft 365 with PowerShell](#)

[Get started with PowerShell for Microsoft 365](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Manage Microsoft 365 user accounts, licenses, and groups with PowerShell

Article • 08/22/2024

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Microsoft 365 administrators need to manage user accounts, licenses, and groups. Although you can do most of these tasks in the Microsoft 365 admin center, some are easier in PowerShell.

For more information, see the following articles.

User accounts

- [Create user accounts](#)
- [View user accounts](#)
- [Configure user account properties](#)
- [Assign roles to user accounts](#)
- [Delete and restore user accounts](#)
- [Block user accounts](#)
- [Passwords](#)

Licenses and services

- [View licenses and services](#)
- [View licensed and unlicensed users](#)
- [Assign licenses to user accounts](#)
- [View account license and service details](#)
- [Disable access to services](#)
 - [Disable access to Sway](#)
 - [Disable access to services while assigning user licenses](#)
- [Remove licenses from user accounts](#)

Groups

- [Manage security groups](#)
- [Manage Microsoft 365 groups](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Create Microsoft 365 user accounts with PowerShell

Article • 03/04/2024

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

You can use Microsoft Graph PowerShell to efficiently create user accounts, including multiple accounts.

When you create user accounts in PowerShell, certain account properties are always required. Other properties aren't required but are important. See the following table.

[+] Expand table

Property name	Required?	Description
DisplayName	Yes	This is the display name that's used in Microsoft 365 services. For example, <i>Caleb Sills</i> .
UserPrincipalName	Yes	This is the account name that's used to sign in to Microsoft 365 services. For example, <i>CalebS@contoso.onmicrosoft.com</i> .
FirstName	No	
LastName	No	
LicenseAssignment	No	This is the licensing plan (also known as the license plan or SKU) from which an available license is assigned to the user account. The license defines the Microsoft 365 services that are available to the account. You don't have to assign a license to a user when you create the account, but the account must have a license to access Microsoft 365 services. You have 30 days to license the user account after you create it.
Password	No	If you don't specify a password, a random password is assigned to the user account, and the password is visible in the results of the command. If you specify a password, it needs to be 8 to 16 ASCII text characters of the following types: lowercase letters, uppercase letters, numbers, and symbols.
UsageLocation	No	This is a valid ISO 3166-1 alpha-2 country code. For example, <i>US</i> for the United States, and <i>FR</i> for France. It's important to provide this value, because some Microsoft 365 services aren't available in certain countries/regions. You can't assign a license to a user account unless the account has this value configured. For more information, see About license restrictions .

 Note

Also see [Learn how to create user accounts](#) by using the Microsoft 365 admin center.

For a list of additional resources, see [Manage users and groups](#).

Create Microsoft 365 user accounts with Microsoft Graph PowerShell

 Note

The Azure Active Directory module is being replaced by the Microsoft Graph PowerShell SDK. You can use the Microsoft Graph PowerShell SDK to access all Microsoft Graph APIs. For more information, see [Get started with the Microsoft Graph PowerShell SDK](#).

First, use a **Microsoft Entra DC admin** or **Cloud Application Admin** account to [connect to your Microsoft 365 tenant](#). The cmdlets in this article require the permission scope **User.ReadWrite.All** or one of the other permissions listed in the '[List subscribedSkus](#)' [Graph API reference page](#). Some commands in this article may require different permission scopes, in which case this will be noted in the relevant section.

PowerShell

```
Connect-MgGraph -Scopes "User.ReadWrite.All"
```

Create an individual user account

To create an individual account, use the following syntax:

PowerShell

```
$PasswordProfile = New-Object -TypeName  
Microsoft.Graph.PowerShell.Models.MicrosoftGraphPasswordProfile  
$PasswordProfile.Password = "<user account password>"  
New-MgUser -DisplayName "<display name>" -GivenName "<first name>" -Surname  
"<last name>" -UserPrincipalName <sign-in name> -UsageLocation <ISO 3166-1  
alpha-2 country code> -MailNickname <mailbox name> -PasswordProfile  
$PasswordProfile -AccountEnabled $true
```

This example creates an account for the US user *John Doe*.

PowerShell

```
$PasswordProfile = New-Object -TypeName  
Microsoft.Graph.PowerShell.Models.MicrosoftGraphPasswordProfile  
$PasswordProfile.Password = "3Rv0y1q39/chsy"  
New-MgUser -DisplayName "John Doe" -GivenName "John" -Surname "Doe" -  
UserPrincipalName johnd@contoso.onmicrosoft.com -UsageLocation "US" -  
MailNickname "johnd" -PasswordProfile $PasswordProfile -AccountEnabled $true
```

Create multiple user accounts

1. Create a comma-separated value (CSV) file that contains the required user account information. For example:

PowerShell

```
UserPrincipalName,FirstName,LastName,DisplayName,UsageLocation,MailNick  
name  
ClaudeL@contoso.onmicrosoft.com,Claude,Loiselle,Claude  
Loiselle,US,claudeL  
LynneB@contoso.onmicrosoft.com,Lynne,Baxter,Lynne Baxter,US,lynneB  
ShawnM@contoso.onmicrosoft.com,Shawn,Melendez,Shawn Melendez,US,shawnm
```

ⓘ Note

The column names and their order in the first row of the CSV file are arbitrary. But make sure the order of the data in the rest of the file matches the order of the column names. And use the column names for the parameter values in the PowerShell for Microsoft 365 command.

2. This example creates user accounts from the file *C:\temp\NewAccounts.csv* and logs the results in a file named *C:\temp\NewAccountResults.csv*.

PowerShell

```
# Import the CSV file  
$users = Import-Csv -Path "C:\temp\NewAccounts.csv"  
  
# Create a password profile  
$PasswordProfile = @{  
    Password = 'Password123'  
}  
  
# Loop through each user in the CSV file
```

```
foreach ($user in $users) {
    # Create a new user
    $newUser = New-MgUser -DisplayName $user.DisplayName -GivenName
    $user.FirstName -Surname $user.LastName -UserPrincipalName
    $user.UserPrincipalName -UsageLocation $user.UsageLocation -
    MailNickname $user.MailNickname -PasswordProfile $passwordProfile -
    AccountEnabled

    # Assign a license to the new user
    $e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq
    'SPE_E5'
    Set-MgUserLicense -UserId $newUser.Id -AddLicenses @{$Skuid =
    $e5Sku.SkuId} -RemoveLicenses @()
}

# Export the results to a CSV file
$users | Export-Csv -Path "C:\temp\NewAccountResults.csv" -
NoTypeInformation
```

3. Review the output file to see the results.

See also

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

View Microsoft 365 user accounts with PowerShell

Article • 02/07/2024

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

You can use the Microsoft 365 admin center to view the accounts for your Microsoft 365 tenant. PowerShell for Microsoft 365 enables this but also provides additional functionality.

View user accounts using Microsoft Graph PowerShell

Note

The Azure Active Directory (AzureAD) PowerShell module is being deprecated and replaced by the Microsoft Graph PowerShell SDK. You can use the Microsoft Graph PowerShell SDK to access all Microsoft Graph APIs. For more information, see [Get started with the Microsoft Graph PowerShell SDK](#).

Also see [Install the Microsoft Graph PowerShell SDK](#) and [Upgrade from Azure AD PowerShell to Microsoft Graph PowerShell](#) for information on how to install and upgrade to Microsoft Graph PowerShell, respectively.

1. First, install the required software to use Microsoft Graph PowerShell. See [Connect to Microsoft 365 with Microsoft Graph PowerShell](#) for more information.
2. Then run the following cmdlet to connect to your organization with the required permission scope, which in this case is *User.ReadBasic.All*:

PowerShell

```
# Connect to Microsoft Graph
Connect-Graph -Scopes User.ReadBasic.All
```

View all accounts

To display the full list of user accounts with user ID and user principal name, run this command:

```
PowerShell
```

```
Get-MgUser -All | Select DisplayName,Id,UserPrincipalName
```

You should get information similar to this:

```
PowerShell
```

DisplayName	Id
UserPrincipalName	
Conf Room Adams	6e206948-b2b6-406c-a728-80bbe78e4003
Adams@M365x89521157.OnMicrosoft.com	
Adele Vance	916a6a08-b9d0-44b6-870f-562d8358a314
AdeleV@M365x89521157.OnMicrosoft.com	
MOD Administrator	5710f237-df3f-4bcd-b875-82deb02f98aa
admin@M365x89521157.onmicrosoft.com	
Alex Wilber	8aa561dc-441d-4d74-aeb3-e2be41c116c8
AlexW@M365x89521157.OnMicrosoft.com	
Allan Deyoung	6b629e5e-3cf4-42d0-8007-3a93f0253382
AllanD@M365x89521157.OnMicrosoft.com	
Automate Bot	3a70feb4-9407-47b5-9b61-7526ac0e98d8
AutomateB@M365x89521157.OnMicrosoft.com	
Conf Room Baker	d8cf3fef-1d03-4b9c-9be0-fed44fb87596
Baker@M365x89521157.OnMicrosoft.com	
Bianca Pisani	7fe8c2d1-eb8e-4032-96ba-26242ff0acd9
BiancaP@M365x89521157.OnMicrosoft.com	

View a specific account

To display a specific user account, run the following command. Fill in the sign-in account name of the user account, which is also known as the user principal name (UPN).

Remove the "<" and ">" characters.

```
PowerShell
```

```
Get-MgUser -UserId '<user principal name>'
```

Here's an example:

```
PowerShell
```

```
Get-MgUser -UserId 'BelindaN@litwareinc.onmicrosoft.com'
```

View additional property values for a specific account

By default, the **Get-MgUser** cmdlet only displays the *DisplayName*, *Id*, *Mail*, and *UserPrincipalName* properties of accounts.

To be more selective about the properties to display, use the **Select** cmdlet in combination with the **Get-MgUser** cmdlet. To combine the two cmdlets, use the "pipe" character ("|"), which tells PowerShell to take the results of one command and send it to the next command. Here's an example command that displays the *DisplayName*, *Department*, and *UsageLocation* for every user account:

```
PowerShell
```

```
Get-MgUser -All | Select DisplayName,Department,UsageLocation
```

This command instructs PowerShell to:

1. Get all the information on the user accounts (**Get-MgUser**) and send it to the next command (|).
2. Display only the user account name, department, and usage location (**Select DisplayName, Department, UsageLocation**).

To see all the properties for a specific user account, use the **Select** cmdlet and the wildcard character (*). Here's an example:

```
PowerShell
```

```
Get-MgUser -UserID 'BelindaN@litwareinc.onmicrosoft.com' | Select *
```

As another example, run the following command to check the enabled status of a specific user account:

```
PowerShell
```

```
Get-MgUser -UserID '<sign-in name of the user account>' | Select  
DisplayName,UserPrincipalName,AccountEnabled
```

View account synchronization status

User accounts have two sources:

- Windows Server Active Directory (AD), which are accounts that sync from on-premises AD to the cloud.
- Microsoft Entra accounts, which are created directly in the cloud.

You can use the following command to find accounts that are synchronizing from **on-premise** AD. It instructs PowerShell to get all users who have the attribute *OnPremisesSyncEnabled* set to *True*.

PowerShell

```
Get-MgUser -All -Filter 'OnPremisesSyncEnabled eq true'
```

You can use the following command to find **cloud-only** accounts. It instructs PowerShell to get all users who have the attribute *OnPremisesSyncEnabled* set to *False* or not set (*Null*). An account that was never synced from on-premises AD has *OnPremisesSyncEnabled* set to *Null*. An account that was synced initially from on-premises AD but is no longer being synced has *OnPremisesSyncEnabled* set to *False*.

PowerShell

```
Get-MgUser -All | Where OnPremisesSyncEnabled -ne true  
OnPremisesSyncEnabled````  
  
### View accounts based on a common property
```

To be more selective about the list of accounts to display, you can use the **Where** cmdlet **in** combination with the **Get-MgUser** cmdlet. To combine the two cmdlets, use the "pipe" character ("|"), which tells PowerShell to take the results of one command and send it to the next command. Here is an example command that displays only those user accounts that have an unspecified usage location:

```
```powershell  
Get-MgUser | Where UsageLocation -eq $Null
```

This command instructs PowerShell to:

1. Get all the information on the user accounts (**Get-MgUser**) and send it to the next command (|).
2. Find all the user accounts that have an unspecified usage location (**Where UsageLocation -eq \$Null**). The command instructs PowerShell to only find the set of accounts for which the *UsageLocation* user account property (**UsageLocation**) is not specified (-eq \$Null).

The **UsageLocation** property is only one of many properties associated with a user account. To display all the properties for a specific user account, use the **Select** cmdlet and the wildcard character (\*). Here's an example:

PowerShell

```
Get-MgUser -UserID BelindaN@litwareinc.onmicrosoft.com | Select *
```

For example, **City** is the name of a user account property. You can use the following command to list all accounts of users who live in London:

PowerShell

```
Get-MgUser | Where City -eq "London"
```

### Tip

The syntax for the **Where** cmdlet in these examples is **Where** [user account property name] [comparison operator] [value] **value.**> [comparison operator] is **-eq** for equals, **-ne** for not equals, **-lt** for less than, **-gt** for greater than, and others. [value] is typically a string (a sequence of letters, numbers, and other characters), a numerical value, or **\$Null** for unspecified. For more information, see [Where](#).

## See also

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Get started with PowerShell for Microsoft 365](#)

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Configure Microsoft 365 user account properties with PowerShell

Article • 06/17/2024

*This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.*

You can use the [Microsoft 365 admin center](#) to configure properties for the user accounts of your Microsoft 365 tenant. In PowerShell, you can also do this, plus some other things you can't do in the admin center.

## Configure Microsoft 365 user account properties with Microsoft Graph PowerShell

### Note

The Azure Active Directory module is being replaced by the Microsoft Graph PowerShell SDK. You can use the Microsoft Graph PowerShell SDK to access all Microsoft Graph APIs. For more information, see [Get started with the Microsoft Graph PowerShell SDK](#).

First, use a **Microsoft Entra DC admin** or **Cloud Application Admin** account to [connect to your Microsoft 365 tenant](#). The cmdlets in this article require the permission scope **User.ReadWrite.All** or one of the other permissions listed in the '[List subscribedSkus](#)' [Graph API reference page](#). Some commands in this article may require different permission scopes, in which case this will be noted in the relevant section.

PowerShell

```
Connect-MgGraph -Scopes "User.ReadWrite.All"
```

## Change properties for a specific user account

You identify the account with the **-ObjectID** parameter and set or change specific properties by using additional parameters. Here's a list of the most common parameters:

- **-Department <department name>**

- -DisplayName "<full user name>"
- -FacsimileTelephoneNumber "<fax number>"
- -GivenName "<user first name>"
- -Surname "<user last name>"
- -Mobile "<mobile phone number>"
- -JobTitle "<job title>"
- -PreferredLanguage "<language>"
- -StreetAddress "<street address>"
- -City "<city name>"
- -State "<state name>"
- -PostalCode "<postal code>"
- -Country "<country name>"
- -TelephoneNumber "<office phone number>"
- -UsageLocation "<2-character country or region code>"

This is the ISO 3166-1 alpha-2 (A2) two-letter country or region code.

#### ⓘ Note

Before you can assign licenses to a user account, you must assign a usage location.

To display the User Principal Name (UPN) for your user accounts, run the following command.

PowerShell

```
Get-MgUser -All | Sort-Object UserPrincipalName | Select-Object
UserPrincipalName | More
```

This command instructs PowerShell to:

1. Get all the information on the user accounts (**Get-MgUser**) and send it to the next command (|).

2. Sort the list of UPNs alphabetically (**Sort UserPrincipalName**) and send it to the next command (|).
3. Display just the UPN property for each account (**Select UserPrincipalName**).
4. Display them one screen at a time (**More**).

To display the UPN for an account based on its display name (first and last name), run the following commands. Fill in the `$userName` variable, and remove the < and > characters:

PowerShell

```
$userName=<Display name>
Write-Host (Get-MgUser -All | where {$_.DisplayName -eq
$userName}).UserPrincipalName
```

This example displays the UPN for the user account that has the display name *Caleb Sills*.

PowerShell

```
$userName="Caleb Sills"
Write-Host (Get-MgUser -All | where {$_.DisplayName -eq
$userName}).UserPrincipalName
```

By using a `$upn` variable, you can make changes to individual accounts based on their display name. Here's an example that sets *Belinda Newman*'s usage location to France. But it specifies her display name rather than her UPN:

PowerShell

```
$userName="Belinda Newman"
$upn=(Get-MgUser | where {$_.DisplayName -eq $userName}).UserPrincipalName
Update-MgUser -UserId $upn -UsageLocation "FR"
```

## Change properties for all user accounts

To change properties for all users, you can use a combination of the **Get-MgUser** and **Update-MgUser** cmdlets. The following example changes the usage location for all users to *France*:

PowerShell

```
Get-MgUser | ForEach-Object { Update-MgUser -UserId $_.Id -UsageLocation "FR" }
```

This command instructs PowerShell to:

1. Get all of the information on the user accounts (**Get-MgUser**) and send it to the next command (|).
2. Set the user location to France (**Update-MgUser -UsageLocation FR**).

## Change properties for a specific set of user accounts

To change properties for a specific set of user accounts, you can use a combination of the **Get-MgUser**, **Where**, and **Update-MgUser** cmdlets. The following example changes the usage location for all the users in the Accounting department to *France*:

PowerShell

```
Get-MgUser -All | Where-Object {$_.Department -eq "Accounting"} | ForEach-Object {Update-MgUser -UserId $_.Id -UsageLocation "FR"}
```

This command instructs PowerShell to:

1. Get all the information on the user accounts (**Get-MgUser**), and send it to the next command (|).
2. Find all the user accounts that have their *Department* property set to "Accounting" (**Where {\$\_.Department -eq "Accounting"}**), and send the resulting information to the next command (|).
3. Set the user location to France (**Update-MgUser -UsageLocation FR**).

## See also

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Get started with PowerShell for Microsoft 365](#)

---

## Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

# Assign admin roles to Microsoft 365 user accounts with PowerShell

Article • 06/17/2024

*This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.*

You can easily assign roles to user accounts by using PowerShell for Microsoft 365.

## ⓘ Note

Learn how to [assign admin roles](#) to user accounts with the Microsoft 365 admin center.

For a list of additional resources, see [Manage users and groups](#).

# Assign roles to user accounts using Microsoft Graph PowerShell

## ⓘ Note

The Azure Active Directory module is being replaced by the Microsoft Graph PowerShell SDK. You can use the Microsoft Graph PowerShell SDK to access all Microsoft Graph APIs. For more information, see [Get started with the Microsoft Graph PowerShell SDK](#).

First, use a **Microsoft Entra DC admin** or **Cloud Application Admin** account to [connect to your Microsoft 365 tenant](#). The cmdlets in this article require the permission scope **RoleManagement.ReadWrite.Directory** or one of the other permissions listed in the '[List subscribedSkus](#)' [Graph API reference page](#). Some commands in this article may require different permission scopes, in which case this will be noted in the relevant section.

PowerShell

```
Connect-MgGraph -Scopes "RoleManagement.ReadWrite.Directory"
```

For more information, see [About admin roles](#).

Next, identify the sign-in name of the user account that you want to add to a role (example: fredsm@contoso.com). This is also known as the user principal name (UPN).

Next, determine the name of the role. See [Microsoft Entra built-in roles](#).

### ⓘ Note

Pay attention to the notes in this article. Some role names are different for Azure Active Directory (Azure AD) PowerShell. For example, the *SharePoint Administrator* role in the Microsoft 365 admin center is *SharePoint Service Administrator* in Azure AD PowerShell.

Next, fill in the user UPN and role names and run these commands:

PowerShell

```
$userUPN=<user UPN>
$roleName=<role name>
$role = Get-MgDirectoryRole | Where-Object {$_displayName -eq $roleName}
if ($role -eq $null) {
 $roleTemplate = (Get-MgDirectoryRoleTemplate | Where-Object
{$_displayName -eq $roleName}).id
 New-MgDirectoryRole -DisplayName $roleName -RoleTemplateId $roleTemplate
 $role = Get-MgDirectoryRole | Where-Object {$_displayName -eq
$roleName}
}
$userID = (Get-MgUser -Filter "userPrincipalName eq '$userUPN'").Id
$newRoleMember =@{
 "@odata.id"= "https://graph.microsoft.com/v1.0/users/$userID"
}
New-MgDirectoryRoleMemberByRef -DirectoryRoleId $role.Id -BodyParameter
$newRoleMember
```

Here's an example of a completed command set that assigns the SharePoint Service Administrator role to the *belindan@contoso.com* account:

PowerShell

```
$userUPN="adelev@contoso.com"
$roleName="Exchange Administrator"
$role = Get-MgDirectoryRole | Where-Object {$_displayName -eq $roleName}
if ($role -eq $null) {
 $roleTemplate = (Get-MgDirectoryRoleTemplate | Where-Object
{$_displayName -eq $roleName}).id
 New-MgDirectoryRole -DisplayName $roleName -RoleTemplateId $roleTemplate
 $role = Get-MgDirectoryRole | Where-Object {$_displayName -eq
$roleName}
}
```

```
$userId = (Get-MgUser -Filter "userPrincipalName eq '$userUPN'").Id
$newRoleMember =@{
 "@odata.id"= "https://graph.microsoft.com/v1.0/users/$userId"
}
New-MgDirectoryRoleMemberByRef -DirectoryRoleId $role.Id -BodyParameter
$newRoleMember
```

To display the list of user IDs for a specific admin role, use these commands.

PowerShell

```
$roleName=<role name>
Connect-MgGraph -Scopes "Directory.Read.All"
Get-MgDirectoryRole | Where-Object { $_.DisplayName -eq $roleName } |
ForEach-Object { Get-MgDirectoryRoleMember -DirectoryRoleId $_.Id }
```

## See also

- [Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)
- [Manage Microsoft 365 with PowerShell](#)
- [Get started with PowerShell for Microsoft 365](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

# Delete Microsoft 365 user accounts with PowerShell

Article • 02/20/2024

You can use PowerShell for Microsoft 365 to delete and restore user accounts.

## ⓘ Note

Learn how to [restore a user account](#) by using the Microsoft 365 admin center.

For a list of additional resources, see [Manage users and groups](#).

## Use Microsoft Graph PowerShell to delete a user account

## ⓘ Note

The Azure Active Directory (AzureAD) PowerShell module is being deprecated and replaced by the Microsoft Graph PowerShell SDK. You can use the Microsoft Graph PowerShell SDK to access all Microsoft Graph APIs. For more information, see [Get started with the Microsoft Graph PowerShell SDK](#).

Also see [Install the Microsoft Graph PowerShell SDK](#) and [Upgrade from Azure AD PowerShell to Microsoft Graph PowerShell](#) for information on how to install and upgrade to Microsoft Graph PowerShell, respectively.

For information about how to use different methods to authenticate `Connect-Graph` in an unattended script, see the article [Authentication module cmdlets in Microsoft Graph PowerShell](#).

Deleting a user account requires the `User.ReadWrite.All` permission scope, which is listed in the ['Assign license' Microsoft Graph API reference page](#).

The `User.Read.All` permission scope is required to read the user account details in the tenant.

First, [connect to your Microsoft 365 tenant](#).

```
Connect to your tenant
Connect-MgGraph -Scopes User.Read.All, User.ReadWrite.All
```

After you connect, use the following syntax to remove an individual user account:

PowerShell

```
$userName=<display name>
Get the user
$userId = (Get-MgUser -Filter "displayName eq '$userName'").Id
Remove the user
Remove-MgUser -UserId $userId -Confirm:$false
```

This example removes the user account *Caleb Sills*.

PowerShell

```
$userName="Caleb Sills"
$userId = (Get-MgUser -Filter "displayName eq '$userName'").Id
Remove-MgUser -UserId $userId -Confirm:$false
```

## Restore a user account

To restore a user account using Microsoft Graph PowerShell, first [connect to your Microsoft 365 tenant](#).

To restore a deleted user account, the permission scope *Directory.ReadWrite.All* is required. Connect to the tenant with this permission scope:

PowerShell

```
Connect to your tenant
Connect-MgGraph -Scopes Directory.ReadWrite.All
```

Deleted user accounts no longer exist except as objects in the directory, so you can't search for the user account to restore. Instead, use the following PowerShell script to search the directory for deleted objects of the type *microsoft.graph.user*:

PowerShell

```
$DeletedUsers = Get-MgDirectoryDeletedItem -DirectoryObjectId
microsoft.graph.user -Property '*'
$DeletedUsers = $DeletedUsers.AdditionalProperties['value']
foreach ($deletedUser in $DeletedUsers)
```

```
{
 $deletedUser | Format-Table
}
```

The output of this script, assuming any deleted user objects exist in the directory, will look like this:

PowerShell

Key	Value
businessPhones	{}
displayName	Caleb Sills
givenName	Caleb
mail	Calebs@litware.com
surname	Sills
userPrincipalName	cdea706c3fdc4bbd95925d92d9f71eb8Calebs@litware.com
id	cdea706c-3fdc-4bbd-9592-5d92d9f71eb8

Use the following syntax to restore an individual user account:

PowerShell

```
Input user account ID
$userId = "<id>"
Restore the user
Restore-MgDirectoryDeletedItem -DirectoryObjectId $userId
```

This example restores the user account *calebs@litwareinc.com* using the value for `$userId` from the output of the above script.

PowerShell

```
$userId = "cdea706c-3fdc-4bbd-9592-5d92d9f71eb8"
Restore-MgDirectoryDeletedItem -DirectoryObjectId $userId
```

The output of this command looks like this:

PowerShell

Id	DeletedDateTime
cdea706c-3fdc-4bbd-9592-5d92d9f71eb8	

## See also

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Get started with PowerShell for Microsoft 365](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Block Microsoft 365 user accounts with PowerShell

Article • 02/20/2024

*This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.*

When you block access to a Microsoft 365 account, you prevent anyone from using the account to sign in and access the services and data in your Microsoft 365 organization. You can use PowerShell to block access to individual or multiple user accounts.

## Block access to individual user accounts

### Note

The Azure Active Directory module is being replaced by the Microsoft Graph PowerShell SDK. You can use the Microsoft Graph PowerShell SDK to access all Microsoft Graph APIs. For more information, see [Get started with the Microsoft Graph PowerShell SDK](#).

First, [connect to your Microsoft 365 tenant](#).

Blocking and unblocking user accounts requires the `User.ReadWrite.All` permission scope or one of the other permissions listed in the ['List subscribedSkus' Graph API reference page](#).

### PowerShell

```
Connect-Graph -Scopes User.ReadWrite.All
```

Use the following syntax to block an individual user account:

### PowerShell

```
$params = @{
 accountEnabled = $false
}
Update-MgUser -UserId <sign-in name of the user account> -BodyParameter
$params
```

### Note

The `-UserId` parameter in the **Update-MgUser** cmdlet accepts either the account sign-in name, also known as the User Principal Name, or the account's object ID.

This example blocks access to the user account `fabricec@litwareinc.com`.

PowerShell

```
$params = @{
 accountEnabled = $false
}
Update-MgUser -UserId "fabricec@litwareinc.com" -BodyParameter $params
```

To unblock this user account, run the following command:

PowerShell

```
$params = @{
 accountEnabled = $true
}
Update-MgUser -UserId "fabricec@litwareinc.com" -BodyParameter $params
```

To display the user account UPN based on the user's display name, use the following commands:

PowerShell

```
$userName=<display name>
Write-Host (Get-MgUser -All | where {$_.DisplayName -eq
$userName}).UserPrincipalName
```

This example displays the user account UPN for the user *Caleb Sills*.

PowerShell

```
$userName="Caleb Sills"
Write-Host (Get-MgUser -All | where {$_.DisplayName -eq
$userName}).UserPrincipalName
```

To block an account based on the user's display name, use the following commands:

PowerShell

```
$userName=<display name>
$user = Get-MgUser -Filter "displayName eq '$userName'"
$params = @{


```

```
 accountEnabled = $false
}
Update-MgUser -UserId $user.Id -BodyParameter $params
```

To check the blocked status of a user account use the following command:

PowerShell

```
Get-MgUser -ObjectID <UPN of user account> -Property
"displayName,accountEnabled" | Select displayName, accountEnabled
```

## Block multiple user accounts

To block access for multiple user accounts, create a text file that contains one account sign-in name on each line like this:

PowerShell

```
akol@contoso.com
tjohnston@contoso.com
kakers@contoso.com
```

In the following commands, the example text file is *C:\My Documents\Accounts.txt*. Replace this file name with the path and file name of your text file.

To block access to the accounts listed in the text file, run the following command:

PowerShell

```
$params = @{
 accountEnabled = $false
}
Get-Content "C:\My Documents\Accounts.txt" | ForEach {Update-MgUser -UserId
$_ -BodyParameter $params}
```

To unblock the accounts that are listed in the text file, run the following command:

PowerShell

```
$params = @{
 accountEnabled = $true
}
Get-Content "C:\My Documents\Accounts.txt" | ForEach {Update-MgUser -UserId
$_ -BodyParameter $params}
```

## See also

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Get started with PowerShell for Microsoft 365](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Manage passwords with Microsoft Graph PowerShell

Article • 03/08/2024

*This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.*

You can use Microsoft Graph PowerShell as an alternative to the Microsoft 365 admin center to manage passwords in Microsoft 365.

## ⓘ Note

The Azure Active Directory module is being replaced by the Microsoft Graph PowerShell SDK. You can use the Microsoft Graph PowerShell SDK to access all Microsoft Graph APIs. For more information, see [Get started with the Microsoft Graph PowerShell SDK](#).

First, use a **Microsoft Entra DC admin** or **Cloud Application Admin** account to [connect to your Microsoft 365 tenant](#).

Managing passwords for a user requires the **User.ReadWrite.All** permission scope or one of the other permissions listed in the '[Assign license](#)' Graph API reference page.

PowerShell

```
Connect-Graph -Scopes User.ReadWrite.All
```

Use these commands to set a password and force a user to change their new password the next time they sign in.

PowerShell

```
$userUPN=<user account sign in name, such as belindan@contoso.com>
$newPassword=<new password>
$secPassword = ConvertTo-SecureString $newPassword -AsPlainText -Force
Update-MgUser -UserId $userUPN -PasswordProfile @{
 ForceChangePasswordNextSignIn = $true; Password = $newPassword }
```

## See also

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

## Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

# View Microsoft 365 licenses and services with PowerShell

Article • 02/02/2024

*This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.*

You can use PowerShell for Microsoft 365 to view details about the available licensing plans, licenses, and services in your Microsoft 365 organization. Every Microsoft 365 subscription consists of the following elements:

- **Licensing plans** These are also known as license plans or Microsoft 365 plans. Licensing plans define the Microsoft 365 services that are available to users. Your Microsoft 365 subscription may contain multiple licensing plans. An example licensing plan would be Microsoft 365 E3.
- **Services** These are also known as service plans. Services are the Microsoft 365 products, features, and capabilities that are available in each licensing plan, for example, Exchange Online and Microsoft 365 Apps for enterprise (previously named Office 365 ProPlus). Users can have multiple licenses assigned to them from different licensing plans that grant access to different services.
- **Licenses** Each licensing plan contains the number of licenses that you purchased. You assign licenses to users so they can use the Microsoft 365 services that are defined by the licensing plan. Every user account requires at least one license from one licensing plan so they can sign in Microsoft 365 and use the services.

For more information about the products, features, and services that are available in different Office 365 subscriptions, see [Office 365 Plan Options](#).

## Use the Microsoft Graph PowerShell SDK

### Note

The Azure Active Directory module is being replaced by the Microsoft Graph PowerShell SDK. You can use the Microsoft Graph PowerShell SDK to access all Microsoft Graph APIs. For more information, see [Get started with the Microsoft Graph PowerShell SDK](#).

First, [connect to your Microsoft 365 tenant](#).

Reading subscription license plans requires the **Organization.Read.All** permission scope or one of the other permissions listed in the '[List subscribedSkus](#)' Graph API reference page.

```
PowerShell
```

```
Connect-Graph -Scopes Organization.Read.All
```

To view summary information about your current licensing plans and the available licenses for each plan, run this command:

```
PowerShell
```

```
Get-MgSubscribedSku | Select -Property Sku*, ConsumedUnits -ExpandProperty PrepaidUnits | Format-List
```

The results contain:

- **SkuPartNumber**: Shows the available licensing plans for your organization. For example, `ENTERPRISEPACK` is the license plan name for Office 365 Enterprise E3.
- **Enabled**: Number of licenses that you've purchased for a specific licensing plan.
- **ConsumedUnits**: Number of licenses that you've assigned to users from a specific licensing plan.

To view details about the Microsoft 365 services that are available in all of your license plans, first display a list of your license plans.

```
PowerShell
```

```
Get-MgSubscribedSku
```

Next, store the license plans information in a variable.

```
PowerShell
```

```
$licenses = Get-MgSubscribedSku
```

Next, display the services in a specific license plan.

```
PowerShell
```

```
$licenses[<index>].ServicePlans
```

<index> is an integer that specifies the row number of the license plan from the display of the `Get-MgSubscribedSku | Select SkuPartNumber` command, minus 1.

For example, if the display of the `Get-MgSubscribedSku | Select SkuPartNumber` command is this:

```
PowerShell
```

```
SkuPartNumber

WIN10_VDA_E5
EMSPREMIUM
ENTERPRISEPREMIUM
FLOW_FREE
```

Then the command to display the services for the ENTERPRISEPREMIUM license plan is this:

```
PowerShell
```

```
$licenses[2].ServicePlans
```

ENTERPRISEPREMIUM is the third row. Therefore, the index value is (3 - 1), or 2.

For a complete list of license plans (also known as product names), their included service plans, and their corresponding friendly names, see [Product names and service plan identifiers for licensing](#).

## See also

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# View licensed and unlicensed Microsoft 365 users with PowerShell

Article • 02/02/2024

*This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.*

User accounts in your Microsoft 365 organization may have some, all, or none of the available licenses assigned to them from the licensing plans that are available in your organization. You can use PowerShell for Microsoft 365 to quickly find the licensed and unlicensed users in your organization.

## ⓘ Note

The Azure Active Directory module is being replaced by the Microsoft Graph PowerShell SDK. You can use the Microsoft Graph PowerShell SDK to access all Microsoft Graph APIs. For more information, see [Get started with the Microsoft Graph PowerShell SDK](#).

## Use the Microsoft Graph PowerShell SDK

First, [connect to Microsoft 365 with PowerShell](#).

Reading user properties including license details requires the User.Read.All permission scope or one of the other permissions listed in the ['Get a user' Graph API reference page](#).

The Organization.Read.All permission scope is required to read the licenses available in the tenant.

PowerShell

```
Connect-Graph -Scopes User.Read.All, Organization.Read.All
```

To view the license details of a specific user account, run the following command:

PowerShell

```
Get-MgUserLicenseDetail -UserId "<user sign-in name (UPN)>"
```

For example:

PowerShell

```
Get-MgUserLicenseDetail -UserId "belindan@litwareinc.com"
```

To view the list of all user accounts in your organization that have NOT been assigned any of your licensing plans (unlicensed users), run the following command:

PowerShell

```
Get-MgUser -Filter 'assignedLicenses/$count eq 0' -ConsistencyLevel eventual
-CountVariable unlicensedUserCount -All

Write-Host "Found $unlicensedUserCount unlicensed users."
```

To view the list of all member user accounts (excluding guests) in your organization that have NOT been assigned any of your licensing plans (unlicensed users), run the following command:

PowerShell

```
Get-MgUser -Filter "assignedLicenses/$count eq 0 and userType eq 'Member'"
-ConsistencyLevel eventual -CountVariable unlicensedUserCount -All

Write-Host "Found $unlicensedUserCount unlicensed users (excluding guests)."
```

To view the list of all user accounts in your organization that have been assigned any of your licensing plans (licensed users), run the following command:

PowerShell

```
Get-MgUser -Filter 'assignedLicenses/$count ne 0' -ConsistencyLevel eventual
-CountVariable licensedUserCount -All -Select
UserPrincipalName,DisplayName,AssignedLicenses | Format-Table -Property
UserPrincipalName,DisplayName,AssignedLicenses

Write-Host "Found $licensedUserCount licensed users."
```

To view the list of all user accounts in your organization that have an E5 license assigned, run the following command:

PowerShell

```
$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'

Get-MgUser -Filter "assignedLicenses/any(x:x/skuId eq $($e5sku.SkuId))" -
ConsistencyLevel eventual -CountVariable e5licensedUserCount -All
```

```
Write-Host "Found $e5licensedUserCount E5 licensed users."
```

## See also

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

---

## Feedback

Was this page helpful?



[Provide product feedback ↗](#)

# Assign Microsoft 365 licenses to user accounts with PowerShell

Article • 02/01/2024

*This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.*

Users can't use any Microsoft 365 services until their account has been assigned a license from a licensing plan. You can use PowerShell to quickly assign licenses to unlicensed accounts.

User accounts must first be assigned a location. Specifying a location is a required part of creating a new user account in the [Microsoft 365 admin center](#).

Accounts synchronized from your on-premises Active Directory Domain Services don't by default have a location specified. You can configure a location for these accounts from:

- The Microsoft 365 admin center
- [PowerShell](#)
- The [Azure portal](#) ([Active Directory](#) > [Users](#) > user account > [Profile](#) > [Contact info](#) > [Country or region](#)).

ⓘ Note

[Learn how to assign licenses to user accounts](#) with the Microsoft 365 admin center. For a list of additional resources, see [Manage users and groups](#).

## Assign Microsoft 365 licenses to user accounts with the Microsoft Graph PowerShell SDK

ⓘ Note

The following script uses Microsoft Graph Powershell. For more information, see [Microsoft Graph PowerShell overview](#).

For information about how to use different methods to authenticate `Connect-Graph` in an unattended script, see the article [Authentication module cmdlets in Microsoft Graph PowerShell](#).

First, [connect to your Microsoft 365 tenant](#).

Assigning and removing licenses for a user requires the User.ReadWrite.All permission scope or one of the other permissions listed in the '[Assign license](#)' Microsoft Graph API reference page.

The Organization.Read.All permission scope is required to read the licenses available in the tenant.

PowerShell

```
Connect-MgGraph -Scopes User.ReadWrite.All, Organization.Read.All
```

Run the `Get-MgSubscribedSku` command to view the available licensing plans and the number of available licenses in each plan in your organization. The number of available licenses in each plan is **ActiveUnits** - **WarningUnits** - **ConsumedUnits**. For more information about licensing plans, licenses, and services, see [View licenses and services with PowerShell](#).

To find the unlicensed accounts in your organization, run this command.

PowerShell

```
Get-MgUser -Filter 'assignedLicenses/$count eq 0' -ConsistencyLevel eventual -CountVariable unlicensedUserCount -All
```

To find the unlicensed synchronized users in your organization, run this command.

PowerShell

```
Get-MgUser -Filter 'assignedLicenses/$count eq 0 and OnPremisesSyncEnabled eq true' -ConsistencyLevel eventual -CountVariable unlicensedUserCount -All -Select UserPrincipalName
```

You can only assign licenses to user accounts that have the **UsageLocation** property set to a valid ISO 3166-1 alpha-2 country code. For example, US for the United States, and FR for France. Some Microsoft 365 services aren't available in certain countries/regions. For more information, see [About license restrictions](#).

To find accounts that don't have a **UsageLocation** value, run this command.

PowerShell

```
Get-MgUser -Select Id,DisplayName,Mail,UserPrincipalName,UsageLocation,UserType | where {
```

```
$_.UsageLocation -eq $null -and $_.UserType -eq 'Member' }
```

To set the **UsageLocation** value on an account, run this command.

PowerShell

```
$userUPN=<user sign-in name (UPN)>
$userLoc=<ISO 3166-1 alpha-2 country code>

Update-MgUser -UserId $userUPN -UsageLocation $userLoc
```

For example:

PowerShell

```
Update-MgUser -UserId "belindan@litwareinc.com" -UsageLocation US
```

If you use the **Get-MgUser** cmdlet without using the **-All** parameter, only the first 100 accounts are returned.

## Assigning licenses to user accounts

To assign a license to a user, use the following command in PowerShell.

PowerShell

```
Set-MgUserLicense -UserId $userUPN -AddLicenses @{SkuId = "<SkuId>"} -
RemoveLicenses @()
```

This example assigns a license from the **SPE\_E5** (Microsoft 365 E5) licensing plan to the unlicensed user **belindan@litwareinc.com**:

PowerShell

```
$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'
Set-MgUserLicense -UserId "belindan@litwareinc.com" -AddLicenses @{SkuId =
$e5Sku.SkuId} -RemoveLicenses @()
```

This example assigns **SPE\_E5** (Microsoft 365 E5) and **EMSPREMIUM** (ENTERPRISE MOBILITY + SECURITY E5) to the user **belindan@litwareinc.com**:

PowerShell

```

$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'
$e5EmsSku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'EMSPREMIUM'
$addLicenses = @(
 @{SkuId = $e5Sku.SkuId},
 @{SkuId = $e5EmsSku.SkuId}
)

Set-MgUserLicense -UserId "belinda@litwareinc.com" -AddLicenses $addLicenses
-RemoveLicenses @()

```

This example assigns **SPE\_E5** (Microsoft 365 E5) with the **MICROSOFTBOOKINGS** (Microsoft Bookings) and **LOCKBOX\_ENTERPRISE** (Customer Lockbox) services turned off:

PowerShell

```

$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'
$disabledPlans = $e5Sku.ServicePlans | `
 Where ServicePlanName -in ("LOCKBOX_ENTERPRISE", "MICROSOFTBOOKINGS") |
 Select -ExpandProperty ServicePlanId

$addLicenses = @(
 @{
 SkuId = $e5Sku.SkuId
 DisabledPlans = $disabledPlans
 }
)

Set-MgUserLicense -UserId "belinda@litwareinc.com" -AddLicenses $addLicenses
-RemoveLicenses @()

```

This example updates a user with **SPE\_E5** (Microsoft 365 E5) and turns off the Sway and Forms service plans while leaving the user's existing disabled plans in their current state:

PowerShell

```

$userLicense = Get-MgUserLicenseDetail -UserId "belinda@litwareinc.com"
$userDisabledPlans = $userLicense.ServicePlans | `
 Where ProvisioningStatus -eq "Disabled" | `
 Select -ExpandProperty ServicePlanId

$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'
$newDisabledPlans = $e5Sku.ServicePlans | `
 Where ServicePlanName -in ("SWAY", "FORMS_PLAN_E5") | `
 Select -ExpandProperty ServicePlanId

$disabledPlans = ($userDisabledPlans + $newDisabledPlans) | Select -Unique

$addLicenses = @(

```

```

@{
 SkuId = $e5Sku.SkuId
 DisabledPlans = $disabledPlans
}
)

Set-MgUserLicense -UserId "belinda@litwareinc.com" -AddLicenses $addLicenses
-RemoveLicenses @()

```

This example updates a user with **SPE\_E5** (Microsoft 365 E5) and turns off the Sway and Forms service plans while leaving the user's existing disabled plans in all other subscriptions in their current state:

PowerShell

```

$userLicense = Get-MgUserLicenseDetail -UserId belinda@litwareinc.com

$userDisabledPlans = $userLicense.ServicePlans | Where-Object
ProvisioningStatus -eq "Disabled" | Select -ExpandProperty ServicePlanId

$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'

$newDisabledPlans = $e5Sku.ServicePlans | Where ServicePlanName -in ("SWAY",
"FORMS_PLAN_E5") | Select -ExpandProperty ServicePlanId

$disabledPlans = ($userDisabledPlans + $newDisabledPlans) | Select -Unique

$result=@()
$allPlans = $e5Sku.ServicePlans | Select -ExpandProperty ServicePlanId

foreach($disabledPlan in $disabledPlans)
{
 foreach($allPlan in $allPlans)
 {
 if($disabledPlan -eq $allPlan)
 {
 $property = @{
 Disabled = $disabledPlan
 }
 }
 }
 $result += New-Object psobject -Property $property
}

$finalDisabled = $result | Select-Object -ExpandProperty Disabled

$addLicenses = @(
@{
 SkuId = $e5Sku.SkuId
 DisabledPlans = $finalDisabled
}
)
```

```
)
```

```
Set-MgUserLicense -UserId belinda@litwareinc.com -AddLicenses $addLicenses -
RemoveLicenses @()
```

## Assign licenses to a user by copying the license assignment from another user

This example assigns jamesp@litwareinc.com with the same licensing plan that has been applied to belindan@litwareinc.com:

PowerShell

```
$mgUser = Get-MgUser -UserId "belindan@litwareinc.com" -Property
AssignedLicenses
Set-MgUserLicense -UserId "jamesp@litwareinc.com" -AddLicenses
$mgUser.AssignedLicenses -RemoveLicenses @()
```

## Move a user to a different subscription (license plan)

This example upgrades a user from the SPE\_E3 (Microsoft 365 E3) licensing plan to the SPE\_E5 (Microsoft 365 E5) licensing plan:

PowerShell

```
$e3Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E3'
$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'

Unassign E3
Set-MgUserLicense -UserId "belindan@litwareinc.com" -AddLicenses @{} -
RemoveLicenses @($e3Sku.SkuId)
Assign E5
Set-MgUserLicense -UserId "belindan@litwareinc.com" -AddLicenses @{SkuId =
$e5Sku.SkuId} -RemoveLicenses @()
```

You can verify the change in subscription for the user account with this command.

PowerShell

```
Get-MgUserLicenseDetail -UserId "belindan@litwareinc.com"
```

## See also

[Manage Microsoft 365 with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Get started with the Microsoft Graph PowerShell SDK](#)

[Use the Microsoft Graph `user: assignLicense` and `subscribedSku` APIs](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# View Microsoft 365 account license and service details with PowerShell

Article • 01/30/2024

*This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.*

In Microsoft 365, licenses from licensing plans (also called SKUs or Microsoft 365 plans) give users access to the Microsoft 365 services that are defined for those plans. However, a user might not have access to all the services that are available in a license that's currently assigned to them. You can use PowerShell for Microsoft 365 to view the status of services on user accounts.

For more information about licensing plans, license, and services, see [View licenses and services with PowerShell](#).

## View account license and service details using Microsoft Graph PowerShell

First, [connect to your Microsoft 365 tenant](#).

Reading user properties including license details requires the `User.Read.All` permission scope or one of the other permissions listed in the '['Get a user' Graph API reference page](#)'.

```
PowerShell
```

```
Connect-Graph -Scopes User.ReadWrite.All, Organization.Read.All
```

Next, list the license plans for your tenant with this command.

```
PowerShell
```

```
Get-MgSubscribedSku
```

Use these commands to list the services that are available in each licensing plan.

```
PowerShell
```

```
$allSKUs = Get-MgSubscribedSku -Property SkuPartNumber, ServicePlans
$allSKUs | ForEach-Object {
 Write-Host "Service Plan:" $_.SkuPartNumber
```

```
$_.ServicePlans | ForEach-Object {$_}
}
```

Use these commands to list the licenses that are assigned to a user account.

PowerShell

```
Get-MgUserLicenseDetail -UserId "<user sign-in name (UPN)>"
```

For example:

PowerShell

```
Get-MgUserLicenseDetail -UserId "belindan@litwareinc.com"
```

## To view services for a user account

To view all the Microsoft 365 services that a user has access to, use the following syntax:

PowerShell

```
(Get-MgUserLicenseDetail -UserId <user account UPN> -Property ServicePlans)
[<LicenseIndexNumber>].ServicePlans
```

This example shows the services to which the user BelindaN@litwareinc.com has access. This shows the services that are associated with all licenses that are assigned to her account.

PowerShell

```
(Get-MgUserLicenseDetail -UserId belindan@litwareinc.com -Property
ServicePlans).ServicePlans
```

This example shows the services that user BelindaN@litwareinc.com has access to from the first license that's assigned to her account (the index number is 0).

PowerShell

```
(Get-MgUserLicenseDetail -UserId belindan@litwareinc.com -Property
ServicePlans)[0].ServicePlans
```

To view all the services for a user who has been assigned *multiple licenses*, use the following syntax:

## PowerShell

```
$userUPN=<user account UPN>
$allLicenses = Get-MgUserLicenseDetail -UserId $userUPN -Property
SkuPartNumber, ServicePlans
$allLicenses | ForEach-Object {
 Write-Host "License:" $_.SkuPartNumber
 $_.ServicePlans | ForEach-Object {$_}
}
```

## See also

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Remove Microsoft 365 licenses from user accounts with PowerShell

Article • 02/08/2024

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

## ⓘ Note

[Learn how to remove licenses from user accounts](#) with the Microsoft 365 admin center. For a list of additional resources, see [Manage users and groups](#).

## Use the Microsoft Graph PowerShell SDK

First, [connect to your Microsoft 365 tenant](#).

Assigning and removing licenses for a user requires the User.ReadWrite.All permission scope or one of the other permissions listed in the '[Assign license](#)' Graph API reference page.

The Organization.Read.All permission scope is required to read the licenses available in the tenant.

PowerShell

```
Connect-Graph -Scopes User.ReadWrite.All, Organization.Read.All
```

To view the licensing plan information in your organization, see the following articles:

- [View licenses and services with PowerShell](#)
- [View account license and service details with PowerShell](#)

## Removing licenses from user accounts

To remove licenses from an existing user account, use the following syntax:

PowerShell

```
Set-MgUserLicense -UserId "<Account>" -RemoveLicenses @("<AccountSkuId1>") -
AddLicenses @{}
```

This example removes the **SPE\_E5** (Microsoft 365 E5) licensing plan from the user **BelindaN@litwareinc.com**:

```
PowerShell

$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'
Set-MgUserLicense -UserId "belindan@litwareinc.com" -RemoveLicenses
@($e5Sku.SkuId) -AddLicenses @{}
```

To remove all licenses from a group of existing licensed users, use the following syntax:

```
PowerShell

$licensedUsers = Get-MgUser -Filter 'assignedLicenses/$count ne 0' `
 -ConsistencyLevel eventual -CountVariable licensedUserCount -All `
 -Select UserPrincipalName,DisplayName,AssignedLicenses

foreach($user in $licensedUsers)
{
 $licensesToRemove = $user.AssignedLicenses | Select -ExpandProperty
 SkuId
 $user = Set-MgUserLicense -UserId $user.UserPrincipalName -
 RemoveLicenses $licensesToRemove -AddLicenses @{}
}
```

To remove a specific license from a list of users in a text file, perform the following steps. This example removes the **SPE\_E5** (Microsoft 365 Enterprise E5) license from the user accounts defined in the text file C:\My Documents\Accounts.txt.

1. Create and save a text file to C:\My Documents\Accounts.txt that contains one account on each line like this:

```
PowerShell

akol@contoso.com
tjohnston@contoso.com
kakers@contoso.com
```

2. Use the following command:

```
PowerShell

$x=Get-Content "C:\My Documents\Accounts.txt"
$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'
for ($i=0; $i -lt $x.Count; $i++)
{
 Set-MgUserLicense -UserId $x[$i] -RemoveLicenses @($e5Sku.SkuId) -
```

```
AddLicenses @{}
}
```

Another way to free up a license is by deleting the user account. For more information, see [Delete and restore user accounts with PowerShell](#).

## See also

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

---

## Feedback

Was this page helpful?



[Provide product feedback ↗](#)

# Disable access to Microsoft 365 services with PowerShell

Article • 02/29/2024

*This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.*

When a Microsoft 365 account is assigned a license from a licensing plan, Microsoft 365 services are made available to the user from that license. However, you can control the Microsoft 365 services that the user can access. For example, even though the license allows access to the SharePoint Online service, you can disable access to it. You can use PowerShell to disable access to any number of services for a specific licensing plan for:

- An individual account.
- A group of accounts.
- All accounts in your organization.

## ⓘ Note

There are Microsoft 365 service dependencies that can prevent you from disabling a specified service when other services depend on it.

## Use the Microsoft Graph PowerShell SDK

## ⓘ Note

The Azure Active Directory module is being replaced by the Microsoft Graph PowerShell SDK. You can use the Microsoft Graph PowerShell SDK to access all Microsoft Graph APIs. For more information, see [Get started with the Microsoft Graph PowerShell SDK](#).

First, use a **Microsoft Entra DC admin** or **Cloud Application Admin** account to [connect to your Microsoft 365 tenant](#).

Assigning and removing licenses for a user requires the **User.ReadWrite.All** permission scope or one of the other permissions listed in the '[Assign license](#)' Graph API reference page.

The **Organization.Read.All** permission scope is required to read the licenses available in the tenant.

```
PowerShell
```

```
Connect-Graph -Scopes User.ReadWrite.All, Organization.Read.All
```

Next, use this command to view your available licensing plans, also known as SkuPartNumber:

```
PowerShell
```

```
Get-MgSubscribedSku | Select SkuId, SkuPartNumber, ServicePlans | Sort SkuPartNumber
```

For more information, see [View licenses and services with PowerShell](#).

To see the before and after results of the procedures in this topic, see [View account license and service details with PowerShell](#).

## Disable specific Microsoft 365 services for specific users for a specific licensing plan

To disable a specific set of Microsoft 365 services for users for a specific licensing plan, perform the following steps:

First list the licensing plans available in your tenant using the following command.

```
PowerShell
```

```
Get-MgSubscribedSku | Select SkuPartNumber

SkuPartNumber

EMSPREMIUM
SPE_E5
RIGHTSMANAGEMENT_ADHOC
```

Next, use the SkuPartNumber from the command above, list the service plans available for a given license plan (Sku).

The following example lists all the service plans available for SPE\_E5 (Microsoft 365 E5).

```
PowerShell
```

```
Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5' | select -
```

## ExpandProperty ServicePlans

text

AppliesTo	ProvisioningStatus	ServicePlanId	ServicePlanName
User	Success	b21a6b06-1988-436e-a07b-51ec6d9f52ad	PROJECT_0365_P3
User	Success	64bfa92-2b17-4482-b5e5-a0304429de3e	MICROSOFTENDPOINTDLP
User	Success	199a5c09-e0ca-4e37-8f7c-b05d533e1ea2	MICROSOFTBOOKINGS
User	Success	6db1f1db-2b46-403f-be40-e39395f08dbb	CUSTOMER_KEY
User	Success	4a51bca5-1eff-43f5-878c-177680f191af	WHITEBOARD_PLAN3
User	Success	07699545-9485-468e-95b6-2fca3738be01	FLOW_0365_P3
User	Success	9c0dab89-a30c-4117-86e7-97bda240acd2	POWERAPPS_0365_P3
User	Success	e212cbc7-0961-4c40-9825-01117710dc1	FORMS_PLAN_E5
User	Success	57ff2da0-773e-42df-b2af-ffb7a2317929 TEAMS1	AAD_PREMIUM_P2
User	Success	21b439ba-a0ca-424f-a6cc-52f954a5b111	WIN10_PRO_ENT_SUB
User	Success	eec0eb4f-6444-4f95-aba0-50c24d67f998	YAMMER_ENTERPRISE
User	Success	c1ec4a95-1f05-45b3-a911-aa3fa01094f5 INTUNE_A	SWAY
User	Success	7547a3fe-08ee-4ccb-b430-5077c5041653	SHAREPOINTWAC
User	Success	a23b959c-7ce8-4e57-9140-b90eb88a9e97	SHAREPOINTENTERPRISE
User	Success	e95bec33-7c88-4a70-8e19-b10bd9d0c014	PROJECTWORKMANAGEMENT
User	Success	5dbe027f-2339-4123-9542-606e4d348a72	OFFICESUBSCRIPTION
User	Success	b737dad2-2f6c-4c65-90e3-ca563267e8b9	MCOSTANDARD
User	Success	43de0ff5-c92c-492b-9116-175376d08c38	LOCKBOX_ENTERPRISE
User	Success	9f431833-0334-42de-a7dc-70aa40db46db	EXCHANGE_S_ENTERPRISE
		efb87545-963c-4e0d-99df-69c6916d9eb0	

For a complete list of license plans (also known as product names), their included service plans, and their corresponding friendly names, see [Product names and service plan](#)

[identifiers for licensing](#). (Search using the ServicePlanId to lookup service plan's corresponding friendly name).

The following example assigns **SPE\_E5** (Microsoft 365 E5) with the **MICROSOFTBOOKINGS** (Microsoft Bookings) and **LOCKBOX\_ENTERPRISE** (Customer Lockbox) services turned off:

PowerShell

```
$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'
$disabledPlans = $e5Sku.ServicePlans | `
 Where ServicePlanName -in ("LOCKBOX_ENTERPRISE", "MICROSOFTBOOKINGS") | `
 Select -ExpandProperty ServicePlanId

$addLicenses = @(
 @{
 SkuId = $e5Sku.SkuId
 DisabledPlans = $disabledPlans
 }
)

Set-MgUserLicense -UserId "belinda@litwareinc.com" -AddLicenses $addLicenses
-RemoveLicenses @()
```

The `DisabledPlans` property of the `-AddLicenses` parameter in `Set-MgUserLicense` will overwrite the user's existing `DisabledPlans` value. To preserve the state of existing service plans, the user's current state of service plans must be merged with the new plans that are going to be disabled.

Failing to include the existing `DisabledPlans` will result in the user's previously disabled plan being enabled.

The following example updates a user with **SPE\_E5** (Microsoft 365 E5) and turns off the Sway and Forms service plans while leaving the user's existing disabled plans in their current state:

PowerShell

```
Get the services that have already been disabled for the user.
$userLicense = Get-MgUserLicenseDetail -UserId
"belinda@fdoau.onmicrosoft.com"
$userDisabledPlans = $userLicense.ServicePlans | `
 Where ProvisioningStatus -eq "Disabled" | `
 Select -ExpandProperty ServicePlanId

Get the new service plans that are going to be disabled
$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'
```

```

$newDisabledPlans = $e5Sku.ServicePlans | `
 Where ServicePlanName -in ("SWAY", "FORMS_PLAN_E5") | `
 Select -ExpandProperty ServicePlanId

Merge the new plans that are to be disabled with the user's current state
of disabled plans
$disabledPlans = ($userDisabledPlans + $newDisabledPlans) | Select -Unique

$addLicenses = @(
 @{
 SkuId = $e5Sku.SkuId
 DisabledPlans = $disabledPlans
 }
)

Update user's license
Set-MgUserLicense -UserId "belinda@litwareinc.onmicrosoft.com" -AddLicenses
$addLicenses -RemoveLicenses @()

```

## Related topics

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Disable access to Sway with PowerShell for Microsoft 365

Article • 08/01/2024

*This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.*

The ManageSway.ps1 PowerShell script lets you view and disable services in your Microsoft 365 organization, including Sway. This script automates the procedures that are described in the following topics:

- [View licenses and services with PowerShell](#)
- [Disable access to services with PowerShell](#)

You need to download the two files that are associated with the script:

- The ManageSway.ps1 script at <https://go.microsoft.com/fwlink/?LinkId=785070>
- The help file for the script at <https://go.microsoft.com/fwlink/?LinkId=785072>

---

## Feedback

Was this page helpful?



[Provide product feedback](#)

# Manage security groups with PowerShell

Article • 08/22/2024

*This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.*

You can use PowerShell for Microsoft 365 as an alternative to the Microsoft 365 admin center to manage security groups.

This article describes listing, creating, changing settings, and removing security groups.

When a command block in this article requires that you specify variable values, use these steps.

1. Copy the command block to the clipboard and paste it into Notepad or the PowerShell Integrated Script Environment (ISE).
2. Fill in the variable values and remove the "<" and ">" characters.
3. Run the commands in the PowerShell window or the PowerShell ISE.

## Manage security groups using Microsoft Graph PowerShell

### Note

The Azure Active Directory module is being replaced by the Microsoft Graph PowerShell SDK. You can use the Microsoft Graph PowerShell SDK to access all Microsoft Graph APIs. For more information, see [Get started with the Microsoft Graph PowerShell SDK](#).

First, [connect to your Microsoft 365 tenant](#).

Managing security groups requires the `Group.ReadWrite.All` permission scope or one of the other permissions listed in the '[List subscribedSkus](#)' Graph API reference page. Some commands in this article may require different permission scopes, in which case this will be noted in the relevant section.

PowerShell

```
Connect-Graph -Scopes Group.ReadWrite.All
```

## List your groups

Use this command to list all of your groups.

```
PowerShell
```

```
Get-MgGroup -All
```

Use these commands to display the settings of a specific group by its display name.

```
PowerShell
```

```
$groupName=<display name of the group>
Get-MgGroup -All | Where-Object { $_.DisplayName -eq $groupName }
```

## Create a new group

Use this command to create a new security group.

```
PowerShell
```

```
Connect-MgGraph -Scopes "Group.Create"
New-MgGroup -Description "<group purpose>" -DisplayName "<name>" -
MailEnabled:$false -SecurityEnabled -MailNickname "<email name>"
```

## Display the settings of a group

Display the settings of the group with these commands.

```
PowerShell
```

```
$groupName=<display name of the group>
Get-MgGroup -All | Where-Object { $_.DisplayName -eq $groupName } | Select-
Object *
```

## Remove a security group

Use these commands to remove a security group.

```
PowerShell
```

```
$groupName=<display name of the group>
$group = Get-MgGroup -Filter "displayName eq '$groupName'"
```

```
Remove-MgGroup -GroupId $group.Id
```

## Manage the owners of a security group

Use these commands to display the current owners of a security group.

PowerShell

```
$groupName=<display name of the group>

Connect to Microsoft Graph
Connect-MgGraph -Scopes "GroupMember.Read.All"

Display group owners
Get-MgGroupOwner -GroupId (Get-MgGroup | Where-Object { $_.DisplayName -eq
$groupName }).Id
```

Use these commands to add a user account by its **user principal name (UPN)** to the current owners of a security group.

PowerShell

```
$userUPN=<UPN of the user account to add>
$groupName=<display name of the group>

Connect to Microsoft Graph
Connect-MgGraph -Scopes "Group.ReadWrite.All", "User.ReadBasic.All"

Get the group and user
$group = Get-MgGroup -Filter "displayName eq '$groupName'"
$userId = (Get-MgUser -Filter "userPrincipalName eq '$userUPN'").Id

Add the user as an owner to the group
$newGroupOwner =@{
 "@odata.id"= "https://graph.microsoft.com/v1.0/users/$userId"
}

New-MgGroupOwnerByRef -GroupId $group.Id -BodyParameter $newGroupOwner
```

Use these commands to add a user account by its **display name** to the current owners of a security group.

PowerShell

```
$userName=<Display name of the user account to add>
$groupName=<display name of the group>

Connect to Microsoft Graph
```

```

Connect-MgGraph -Scopes "Group.ReadWrite.All", "Directory.Read.All",
"User.ReadBasic.All"

Get the group and user
$group = Get-MgGroup -All | Where-Object { $_.DisplayName -eq $groupName }
$userId = (Get-MgUser -All | Where-Object { $_.DisplayName -eq $userName
}).Id

Add the user as an owner to the group
$newGroupOwner =@{
 "@odata.id"= "https://graph.microsoft.com/v1.0/users/$userId"
}

New-MgGroupOwnerByRef -GroupId $group.Id -BodyParameter $newGroupOwner

```

Use these commands to remove a user account by its **UPN** from the current owners of a security group.

PowerShell

```

$userUPN=<UPN of the user account to remove>
$groupName=<display name of the group>

Connect to Microsoft Graph
Connect-MgGraph -Scopes "Group.ReadWrite.All", "Directory.ReadWrite.All"

Get the group and user
$group = Get-MgGroup -Filter "displayName eq '$groupName'" | Select-Object -
First 1
$user = Get-MgUser -Filter "userPrincipalName eq '$userUPN'" | Select-Object
-First 1

Remove the user from the group
Remove-MgGroupOwnerByRef -GroupId $group.Id -DirectoryObjectId $user.Id

```

Use these commands to remove a user account by its **display name** from the current owners of a security group.

PowerShell

```

$userName=<Display name of the user account to remove>
$groupName=<display name of the group>
$group = Get-MgGroup | Where-Object { $_.DisplayName -eq $groupName }
$user = Get-MgUser | Where-Object { $_.DisplayName -eq $userName }

Remove-MgGroupOwnerByRef -GroupId $group.Id -DirectoryObjectId $user.Id

```

## See also

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Manage Microsoft 365 Groups with PowerShell

Article • 10/20/2023

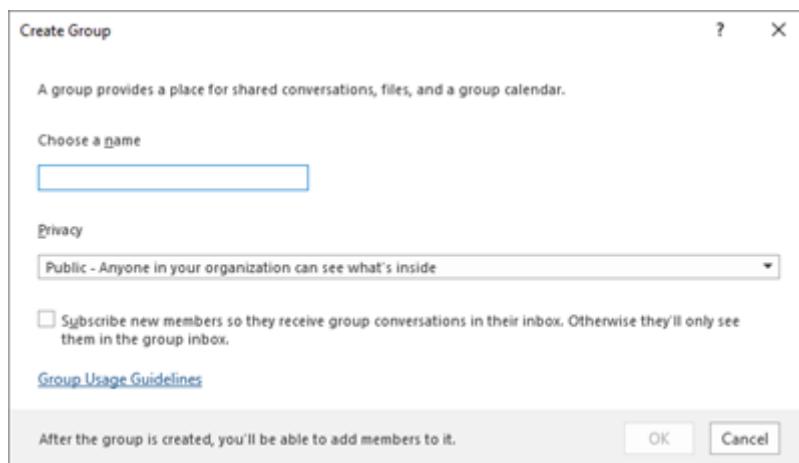
*This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.*

This article provides the steps for doing common management tasks for Groups in Microsoft PowerShell. It also lists the PowerShell cmdlets for Groups. For info about managing SharePoint sites, see [Manage SharePoint Online sites using PowerShell](#).

## Link to your Microsoft 365 Groups usage guidelines

When users [create or edit a group in Outlook](#), you can show them a link to your organization's usage guidelines. For example, if you require a specific prefix or suffix to be added to a group name.

Use the [Microsoft Graph PowerShell](#) to point your users to your organization's usage guidelines for Microsoft 365 groups. Check out [Microsoft Entra cmdlets for configuring group settings](#) and follow the steps in the [Create settings at the directory level](#) to define the usage guideline hyperlink. After you run the Microsoft Entra cmdlet, users see the link to your guidelines when they create or edit a group in Outlook.





## Allow users to Send as the Microsoft 365 Group

If you want to enable your Microsoft 365 groups with Send As permissions, use the [Add-RecipientPermission](#) and [Get-RecipientPermission](#) cmdlets. After you configure the permissions, Microsoft 365 group users can use Outlook or Outlook on the web to send and reply to email as the Microsoft 365 group. Users can go to the group, create a new email, and change the **Send As** field to the group's email address.

(You can also configure Send As permissions in the [Exchange Admin Center](#).)

Replace <GroupAlias> with the alias of the group that you want to update, and <UserAlias> with the alias of the user to whom you want to grant permissions. [Connect to Exchange Online PowerShell](#) and then run the following commands:

```
PowerShell
```

```
$groupAlias = "<GroupAlias>"
$userAlias = "<UserAlias>"
```

```
$groupsRecipientDetails = Get-Recipient -RecipientTypeDetails GroupMailbox -
Identity $groupAlias

Add-RecipientPermission -Identity $groupsRecipientDetails.Name -Trustee
$userAlias -AccessRights SendAs
```

After you run the previous commands, users can go to Outlook or Outlook on the web to send as the group, by adding the group email address to the **From** field.

## Create classifications for Microsoft 365 Groups in your organization

You can create sensitivity labels that the users in your organization can set when they create a Microsoft 365 Group. If you want to classify groups, we recommend using sensitivity labels instead of the previous groups classification feature. For information about using sensitivity labels, see [Use sensitivity labels to protect content in Microsoft Teams, Microsoft 365 groups, and SharePoint sites](#).

### Important

If you're currently using classification labels, they won't be available to users who create groups after sensitivity labels are enabled.

You can still use the previous groups classification feature. You can create classifications that the users in your organization can set when they create a Microsoft 365 Group. For example, you can allow users to set **Standard**, **Secret**, and **Top Secret** on groups they create. Group classifications aren't set by default and you need to create it in order for your users to set it. Use Microsoft Graph PowerShell to point your users to your organization's usage guidelines for Microsoft 365 Groups.

Check out [Microsoft Entra cmdlets for configuring group settings](#) and follow the steps in the **Create settings at the directory level** to define the classification for Microsoft 365 Groups.

### PowerShell

```
$setting["ClassificationList"] = "Low Impact, Medium Impact, High Impact"
```

In order to associate a description to each classification, you can use the settings attribute *ClassificationDescriptions* to define.

```
PowerShell
```

```
$setting["ClassificationDescriptions"] =
"Classification:Description,Classification:Description"
```

Where Classification matches the strings in the ClassificationList.

Example:

```
PowerShell
```

```
$setting["ClassificationDescriptions"] = "Low Impact: General communication,
Medium Impact: Company internal data , High Impact: Data that has regulatory
requirements"
```

After you run the previous Microsoft Graph PowerShell command to set your classification, run the [Set-UnifiedGroup](#) cmdlet if you want to set the classification for a specific group.

```
PowerShell
```

```
Set-UnifiedGroup LowImpactGroup@constoso.com -Classification LowImpact
```

Or create a new group with a classification.

```
PowerShell
```

```
New-UnifiedGroup HighImpactGroup@constoso.com -Classification HighImpact -
AccessType Public
```

Check out [Using PowerShell with Exchange Online](#) and [Connect to Exchange Online PowerShell](#) for more details on using Exchange Online PowerShell.

After these settings are enabled, the group owner can choose a classification from the drop-down menu in Outlook on the Web and Outlook, and save it from the [Edit group](#) page.



## Hide Microsoft 365 Groups from the global address list.

You can specify whether a Microsoft 365 Group appears in the global address list (GAL) and other lists in your organization. For example, if you have a legal department group that you don't want to show up in the address list, you can stop that group from appearing in the GAL. Run the Set-Unified Group cmdlet to hide the group from the address list like this:

PowerShell

```
Set-UnifiedGroup -Identity "Legal Department" -HiddenFromAddressListsEnabled
$true
```

## Allow only internal users to send message to Microsoft 365 Groups

If you don't want users from other organizations to send emails to a Microsoft 365 Group, you can change the settings for that group. It allows only internal users to send an email to your group. If an external user tries to send a message to that group, it's rejected.

Run the Set-UnifiedGroup cmdlet to update this setting, like this:

PowerShell

```
Set-UnifiedGroup -Identity "Internal senders only" -
RequireSenderAuthenticationEnabled $true
```

## Add MailTips to Microsoft 365 Groups

Whenever a sender tries to send an email to a Microsoft 365 Group, a MailTip can be shown to them.

Run the Set-Unified Group cmdlet to add a mailTip to the group:

PowerShell

```
Set-UnifiedGroup -Identity "MailTip Group" -MailTip "This group has a
MailTip"
```

Along with MailTip, you can also set MailTipTranslations, which specify other languages for the MailTip. For example, to have the Spanish translation, run the following command:

PowerShell

```
Set-UnifiedGroup -Identity "MailaTip Group" -MailTip "This group has a
MailTip" -MailTipTranslations "@{Add=ES:Esta caja no se supervisa.}"
```

## Change the display name of the Microsoft 365 Group

The display name specifies the name of the Microsoft 365 Group. You can see this name in your [Exchange admin center](#) or [Microsoft 365 admin center](#). You can edit the display name of the group or assign a display name to an existing Microsoft 365 Group by running the following command:

PowerShell

```
Set-UnifiedGroup -Identity "mygroup@contoso.com" -DisplayName "My new group"
```

# Change the default setting of Microsoft 365 Groups for Outlook to Public or Private

Microsoft 365 Groups in Outlook are created as Private by default. If your organization wants Microsoft 365 Groups to be created as Public by default (or back to Private), use this PowerShell cmdlet syntax:

PowerShell

```
Set-OrganizationConfig -DefaultGroupAccessType Public
```

To set to Private:

PowerShell

```
Set-OrganizationConfig -DefaultGroupAccessType Private
```

To verify the setting:

PowerShell

```
Get-OrganizationConfig | ft DefaultGroupAccessType
```

To learn more, see [Set-OrganizationConfig](#) and [Get-OrganizationConfig](#).

## Microsoft 365 Groups cmdlets

The following cmdlets can be used with Microsoft 365 Groups.

### Tip

User photos for Microsoft 365 Groups are stored in Microsoft Entra ID. To manage user photos for Microsoft 365 Groups, see [Manage user photos in Microsoft Graph PowerShell](#).

[+] Expand table

Cmdlet name	Description
<a href="#">Get-UnifiedGroup</a>	Use this cmdlet to look up existing Microsoft 365 Groups, and to view properties of the group object
<a href="#">Set-UnifiedGroup</a>	Update the properties of a specific Microsoft 365 Group
<a href="#">New-UnifiedGroup</a>	Create a new Microsoft 365 Group. This cmdlet provides a minimal set of parameters. To set values for extended properties, use Set-UnifiedGroup after creating the new group
<a href="#">Remove-UnifiedGroup</a>	Delete an existing Microsoft 365 Group
<a href="#">Get-UnifiedGroupLinks</a>	Retrieve membership and owner information for a Microsoft 365 Group
<a href="#">Add-UnifiedGroupLinks</a>	Add members, owners, and subscribers to an existing Microsoft 365 Group
<a href="#">Remove-UnifiedGroupLinks</a>	Remove owners and members from an existing Microsoft 365 Group
<a href="#">Get-MgGroupPhoto</a>	Used to view information about the user photo that's associated with a Microsoft 365 Group.
<a href="#">Get-MgGroupPhotoContent</a>	Used to download the user photo that's associated with a Microsoft 365 Group.
<a href="#">Set-MgUserPhotoContent</a>	Used to add a user photo to a Microsoft 365 Group.
<a href="#">Remove-MgGroupPhoto</a>	Remove the photo for a Microsoft 365 Group.

## Related articles

[Manage who can create Microsoft 365 Groups](#)

[Manage guest access to Microsoft 365 Groups](#)

[Change static group membership to dynamic in](#)

---

## Feedback

Was this page helpful?



[Provide product feedback](#)

# Manage Folders and Rules feature in Microsoft 365 Groups

Article • 10/30/2023

Users can organize groups emails effectively by creating folders and setting rules inside groups mailbox. Once the folders are created in groups mailbox, users can move and copy messages to different folders manually as well as using **Rules**.

This capability is currently available only in Outlook Web Application.

## Enable Folders and Rules feature for Microsoft 365 Groups in Outlook

Admin can enable the feature with the help of cmdlet `Set-OrganizationConfig -IsGroupFoldersAndRulesEnabled`.

- `[-IsGroupFoldersAndRulesEnabled<Boolean>]` - optional

The `IsGroupFoldersAndRulesEnabled` parameter specifies whether Folders and Rules feature is enabled for the tenant.

Possible values: true/false

Default Value: false

Regardless of whether the `IsGroupFoldersAndRulesEnabled` parameter is turned off, the **Inbox** and **Deleted items** folders will still be shown, if there are any deleted items in the group.

### ⓘ Note

Once the `IsGroupFoldersAndRulesEnabled` parameter is turned off after creating some folder and rules,

- Existing Folders and Rules will keep getting rendered.
- Existing rules will keep on executing.
- Folder Creation/Updation/Deletion will be blocked.

- Message level actions Copy/Move will be blocked.

To enable the **Folders and Rules** feature for Microsoft 365 Groups in Outlook, you can use the following cmdlet:

PowerShell

```
Set-OrganizationConfig -IsGroupFoldersAndRulesEnabled $true
```

Once the feature is enabled, by default, only the group owner has permission to create folders, rename folders, and move and copy messages across folders.

## Enable member permission option

If there's a need for members in the group to create folders and triage messages in groups mailbox, then member permission to edit groups content has to be enabled by the admin at tenant level and group owner at group level respectively.

By default, this setting is set **off** at tenant level and group level

Admin can enable the member permission to the tenant using the cmdlet `IsGroupMemberAllowedToEditContent`.

- `[-IsGroupMemberAllowedToEditContent<Boolean>]` - optional

The `IsGroupMemberAllowedToEditContent` parameter specifies whether group owner can grant permission to members for Folders and Rules feature content edit.

Possible values: True/False

Default value: false

To enable the **Enable member permission** option, you can use the following cmdlet:

PowerShell

```
Set-OrganizationConfig -IsGroupMemberAllowedToEditContent $true
```

Once this option is enabled, group owners can provide group members with the ability to create folders, rename folders, and copy, move, and delete messages by navigating to the group from Outlook > **Settings** > **Edit Group** > and selecting the option **All members will be able to create, edit, move, copy, and delete mail folders and rules within the group**. Group-level member permission is handled by group owners.

### ⓘ Note

Admins can see the current value of the settings using `Get-OrganizationConfig` cmdlet.

## Block “Move” message capability

Admins can block the **Move** message option for all Microsoft 365 groups within a tenant using the cmdlet `Set-OrganizationConfig -BlockMoveMessagesForGroupFold`.

- `[-BlockMoveMessagesForGroupFolders<Boolean>]` – optional

The `BlockMoveMessagesForGroupFolders` parameter specifies whether message the **Move** action is disabled.

Possible values: True/False

Default value: false

To block the **Move** message capability, you can use the following cmdlet:

PowerShell

```
Set-OrganizationConfig -BlockMoveMessagesForGroupFolders $true
```

### ⓘ Note

Creation of the **Move** rule is also disabled when `BlockMoveMessagesForGroupFolders` is enabled.

### ⓘ Note

This is useful if there are mixed set of users using Outlook on Web and Outlook Desktop App. For users on Outlook Desktop App where folders are not available, they can get the messages from group inbox.

## Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

# Manage SharePoint with PowerShell

Article • 05/06/2024

*This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.*

SharePoint administrators have to manage sites, site groups, and users. Although you can do some of these tasks in the Microsoft 365 admin center, others are easier in PowerShell. For more information, see the following articles:

- [Get started with SharePoint Management Shell](#)
- [Create SharePoint sites and add users with PowerShell](#)
- [Manage SharePoint users and groups with PowerShell](#)
- [Manage SharePoint site groups with PowerShell](#)

## See also

- [Manage Microsoft 365 with PowerShell](#)
- [Get started with PowerShell for Microsoft 365](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Create SharePoint sites and add users with PowerShell

Article • 04/15/2024

*This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.*

When you use PowerShell for Microsoft 365 to create SharePoint sites and add users, you can quickly and repeatedly perform tasks faster than you can in the Microsoft 365 admin center. You can also perform tasks that aren't possible to perform in the Microsoft 365 admin center.

## Connect to SharePoint

The procedures in this article require you to connect to SharePoint. For instructions, see [Connect to SharePoint PowerShell](#).

## Step 1: Create new site collections using PowerShell

Create multiple sites using PowerShell and a .csv file that you create using the example code provided and Notepad. For this procedure, you're replacing the placeholder information shown in brackets with your own site- and tenant-specific information. This process lets you create a single file and run a single PowerShell command that uses that file. This makes the actions both repeatable and portable and eliminates many, if not all, errors that can come from typing long commands into the SharePoint Management Shell. There are two parts to this procedure. First you create a .csv file, and then you reference that .csv file using PowerShell, which uses its contents to create the sites.

The PowerShell cmdlet imports the .csv file and pipes it to a loop inside the curly brackets that reads the opening line of the file as column headers. The PowerShell cmdlet then iterates through the remaining records, creates a new site collection for each record, and assigns properties of the site collection according to the column headers.

### Create a .csv file

 Note

The resource quota parameter works only on classic sites. If you use this parameter on a modern site, you may receive a warning message that it has been deprecated.

1. Open Notepad, and paste the following text block into it:

PowerShell

```
Owner,StorageQuota,Url,ResourceQuota,Template,TimeZoneID,Name
owner@tenant.onmicrosoft.com,100,https://tenant.sharepoint.com/sites/Te
amSite01,25,EHS#1,10,Contoso Team Site
owner@tenant.onmicrosoft.com,100,https://tenant.sharepoint.com/sites/B1
og01,25,BLOG#0,10,Contoso Blog
owner@tenant.onmicrosoft.com,150,https://tenant.sharepoint.com/sites/Pr
oject01,25,PROJECTSITE#0,10,Project Alpha
owner@tenant.onmicrosoft.com,150,https://tenant.sharepoint.com/sites/Co
mmunity01,25,COMMUNITY#0,10,Community Site
```

Where *tenant* is the name of your tenant, and *owner* is the user name of the user on your tenant to whom you want to grant the role of primary site admin.

(You can press Ctrl+H when you use Notepad to bulk replace faster.)

2. Save the file on your desktop as **SiteCollections.csv**.

### Tip

Before you use this or any other .csv or Windows PowerShell script file, it's a good practice to make sure that there are no extraneous or nonprinting characters. Open the file in Word, and in the ribbon, click the paragraph icon to show nonprinting characters. There should be no extraneous nonprinting characters. For example, there should be no paragraph marks beyond the final one at the end of the file.

## Run the Windows PowerShell command

1. At the Windows PowerShell prompt, type or copy and paste the following command, and press Enter:

PowerShell

```
Import-Csv C:\users\MyAlias\desktop\SiteCollections.csv | ForEach-
Object {New-SPOSite -Owner $_.Owner -StorageQuota $_.StorageQuota -Url
$_.Url -NoWait -ResourceQuota $_.ResourceQuota -Template $_.Template -
TimeZoneID $_.TimeZoneID -Title $_.Name}
```

Where *MyAlias* equals your user alias

2. Wait for the Windows PowerShell prompt to reappear. It might take a minute or two.
3. At the Windows PowerShell prompt, type or copy and paste the following cmdlet, and press Enter:

```
PowerShell
```

```
Get-SPOSite -Detailed | Format-Table -AutoSize
```

4. Note the new site collections in the list. Using our example CSV file, you would see the following site collections: **TeamSite01**, **Blog01**, **Project01**, and **Community01**.

That's it. You created multiple site collections using the .csv file you created and a single Windows PowerShell command. You're now ready to create and assign users to these sites.

## Step 2: Add users and groups

Now you're going to create users and add them to a site collection group. You'll use a .csv file to bulk upload new groups and users.

The following procedures continue using the example sites TeamSite01, Blog01, Project01, and Community01.

### Create .csv and .ps1 files

1. Open Notepad, and paste the following text block into it:

```
PowerShell
```

```
Site,Group,PermissionLevels
https://tenant.sharepoint.com/sites/Community01,Contoso Project
Leads,Full Control
https://tenant.sharepoint.com/sites/Community01,Contoso Auditors,View
Only
https://tenant.sharepoint.com/sites/Community01,Contoso
Designers,Design
https://tenant.sharepoint.com/sites/TeamSite01,XT1000 Team Leads,Full
Control
https://tenant.sharepoint.com/sites/TeamSite01,XT1000 Advisors>Edit
https://tenant.sharepoint.com/sites/Blog01,Contoso Blog
Designers,Design
https://tenant.sharepoint.com/sites/Blog01,Contoso Blog Editors>Edit
```

```
https://tenant.sharepoint.com/sites/Project01,Project Alpha
Approvers,Full Control
```

Where *tenant* equals your tenant name

2. Save the file to your desktop as **GroupsAndPermissions.csv**.
3. Open a new instance of Notepad, and paste the following text block into it:

PowerShell

```
Group,LoginName,Site
Contoso Project
Leads,username@tenant.onmicrosoft.com,https://tenant.sharepoint.com/sites/Community01
Contoso
Auditors,username@tenant.onmicrosoft.com,https://tenant.sharepoint.com/sites/Community01
Contoso
Designers,username@tenant.onmicrosoft.com,https://tenant.sharepoint.com/sites/Community01
XT1000 Team
Leads,username@tenant.onmicrosoft.com,https://tenant.sharepoint.com/sites/TeamSite01
XT1000
Advisors,username@tenant.onmicrosoft.com,https://tenant.sharepoint.com/sites/TeamSite01
Contoso Blog
Designers,username@tenant.onmicrosoft.com,https://tenant.sharepoint.com/sites/Blog01
Contoso Blog
Editors,username@tenant.onmicrosoft.com,https://tenant.sharepoint.com/sites/Blog01
Project Alpha
Approvers,username@tenant.onmicrosoft.com,https://tenant.sharepoint.com/sites/Project01
```

Where *tenant* equals your tenant name, and *username* equals the user name of an existing user.

4. Save the file to your desktop as **Users.csv**.
5. Open a new instance of Notepad, and paste the following text block into it:

PowerShell

```
Import-Csv C:\users\MyAlias\desktop\GroupsAndPermissions.csv | ForEach-Object {New-SPOSiteGroup -Group $_.Group -PermissionLevels
$_.PermissionLevels -Site $_.Site}
```

```
Import-Csv C:\users\MyAlias\desktop\Users.csv | where {Add-SPOUser -
Group $_.Group -LoginName $_.LoginName -Site $_.Site}
```

Where *MyAlias* equals the user name of the user that is currently logged on.

6. Save the file to your desktop as **UsersAndGroups.ps1**, which is a simple Windows PowerShell script.

You're now ready to run the *UsersAndGroup.ps1* script to add users and groups to multiple site collections.

## Run **UsersAndGroups.ps1** script

1. Return to the SharePoint Management Shell.
2. At the Windows PowerShell command prompt, type or copy and paste the following line, and press Enter:

```
PowerShell

Set-ExecutionPolicy Bypass
```

3. At the confirmation prompt, press **Y**.
4. At the Windows PowerShell command prompt, type or copy and paste the following, and press Enter:

```
PowerShell

c:\users\MyAlias\desktop\UsersAndGroups.ps1
```

Where *MyAlias* equals your user name

5. Wait for the prompt to return before moving on. You'll first see the groups appear as they're created. Then you'll see the group list repeated as users are added.

## See also

[Connect to SharePoint PowerShell](#)

[Manage SharePoint site groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Manage SharePoint users and groups with PowerShell

Article • 05/02/2024

*This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.*

If you're a SharePoint administrator who works with large lists of user accounts or groups and wants an easier way to manage them, you can use PowerShell for Microsoft 365.

Before you begin, the procedures in this article require you to connect to SharePoint. For instructions, see [Connect to SharePoint PowerShell](#)

## Get a list of sites, groups, and users

Before we start to manage users and groups, you need to get lists of your sites, groups, and users. You can then use this information to work through the example in this article.

Get a list of the sites in your tenant with this command:

```
PowerShell
```

```
Get-SPOSite
```

Get a list of the groups in your tenant with this command:

```
PowerShell
```

```
Get-SPOSite | ForEach {Get-SPOSiteGroup -Site $_.Url} | Format-Table
```

Get a list of the users in your tenant with this command:

```
PowerShell
```

```
Get-SPOSite | ForEach {Get-SPOUser -Site $_.Url}
```

## Add a user to the site admins group

You use the `Set-SPOUser` cmdlet to add a user to the list of site admins on a site collection.

## PowerShell

```
$tenant = "<tenant name, such as litwareinc for litwareinc.com>"
$site = "<site name>"
$user = "<user account name, such as opalc>"
Set-SPOUser -Site https://$tenant.sharepoint.com/sites/$site -LoginName
$user@$tenant.com -IsSiteCollectionAdmin $true
```

To use these commands, replace everything within the quotes, including the < and > characters, with the correct names.

For example, this set of commands adds Opal Castillo (user name opalc) to the list of site admins on the ContosoTest site collection in the Contoso tenancy:

## PowerShell

```
$tenant = "contoso"
$site = "contosotest"
$user = "opalc"
Set-SPOUser -Site https://$tenant.sharepoint.com/sites/$site -LoginName
$user@$tenant.com -IsSiteCollectionAdmin $true
```

You can copy and paste these commands into Notepad, change the variable values for \$tenant, \$site, and \$user to actual values from your environment, and then paste this into your SharePoint Management Shell window to run them.

## Add a user to other site collection groups

In this task, we use the `Add-SPOUser` cmdlet to add a user to a SharePoint group on a site collection.

## PowerShell

```
$tenant = "<tenant name, such as litwareinc for litwareinc.com>"
$site = "<site name>"
$user = "<user account name, such as opalc>"
$group = "<group name name, such as Auditors>"
Add-SPOUser -Group $group -LoginName $user@$tenant.com -Site
https://$tenant.sharepoint.com/sites/$site
```

For example, let's add Glen Rife (user name glenr) to the Auditors group on the ContosoTest site collection in the contoso tenancy:

## PowerShell

```
$tenant = "contoso"
$site = "contosotest"
$user = "glenr"
$group = "Auditors"
Add-SPOUser -Group $group -LoginName $user@$tenant.com -Site
https://$tenant.sharepoint.com/sites/$site
```

## Create a site collection group

You use the `New-SPOSiteGroup` cmdlet to create a new SharePoint group and add it to a site collection.

PowerShell

```
$tenant = "<tenant name, such as litwareinc for litwareinc.com>"
$site = "<site name>"
$group = "<group name name, such as Auditors>"
$level = "<permission level, such as View Only>"
New-SPOSiteGroup -Group $group -PermissionLevels $level -Site
https://$tenant.sharepoint.com/sites/$site
```

Group properties, such as permission levels, can be updated later by using the `Set-SPOSiteGroup` cmdlet.

For example, let's add the Auditors group with View Only permissions to the contosotest site collection in the contoso tenancy:

PowerShell

```
$tenant = "contoso"
$site = "contosotest"
$group = "Auditors"
$level = "View Only"
New-SPOSiteGroup -Group $group -PermissionLevels $level -Site
https://$tenant.sharepoint.com/sites/$site
```

## Remove users from a group

Sometimes you have to remove a user from a site or even all sites. Perhaps the employee moves from one division to another or leaves the company. You can do this for one employee easily in the UI, but this isn't easily done when you have to move a complete division from one site to another.

However by using the SharePoint Management Shell and CSV files, this is fast and easy. In this task, you use Windows PowerShell to remove a user from a site collection security group. Then you use a CSV file and remove lots of users from different sites.

We'll be using the 'Remove-SPOUser' cmdlet to remove a single Microsoft 365 user from a site collection group so we can see the command syntax. Here's how the syntax looks:

PowerShell

```
$tenant = "<tenant name, such as litwareinc for litwareinc.com>"
$site = "<site name>"
$user = "<user account name, such as opalc>"
$group = "<group name name, such as Auditors>"
Remove-SPOUser -LoginName $user@$tenant.com -Site
https://$tenant.sharepoint.com/sites/$site -Group $group
```

For example, let's remove Bobby Overby from the site collection Auditors group in the contosotest site collection in the contoso tenancy:

PowerShell

```
$tenant = "contoso"
$site = "contosotest"
$user = "bobbyo"
$group = "Auditors"
Remove-SPOUser -LoginName $user@$tenant.com -Site
https://$tenant.sharepoint.com/sites/$site -Group $group
```

Suppose we wanted to remove Bobby from all the groups he's currently in. Here's how we would do that:

PowerShell

```
$tenant = "contoso"
$user = "bobbyo"
Get-SPOSite | ForEach {Get-SPOSiteGroup -Site $_.Url} | ForEach {Remove-
SPOUser -LoginName $user@$tenant.com -Site $_.Url}
```

### ⚠️ Warning

This is just an example. You should not run this command unless you really have to remove a user from every group, for example if the user leaves the company.

# Automate management of large lists of users and groups

To add a large number of accounts to SharePoint sites and give them permissions, you can use the Microsoft 365 admin center, individual PowerShell commands, or PowerShell and a CSV file. Of these choices, the CSV file is the fastest way to automate this task.

The basic process is to create a CSV file that has headers (columns) that correspond to the parameters that the Windows PowerShell script needs. You can easily create such a list in Excel and then export it as a CSV file. Then, you use a Windows PowerShell script to iterate through records (rows) in the CSV file, adding the users to groups and the groups to sites.

For example, let's create a CSV file to define a group of site collections, groups, and permissions. Next, we'll create a CSV file to populate the groups with users. Finally, we'll create and run a Windows PowerShell script that creates and populates the groups.

The first CSV file adds one or more groups to one or more site collections and will have this structure:

Header:

```
PowerShell
Site,Group,PermissionLevels
```

Item:

```
PowerShell
https://tenant.sharepoint.com/sites/site,group,level
```

Here's an example file:

```
PowerShell
Site,Group,PermissionLevels
https://contoso.sharepoint.com/sites/contosotest,Contoso Project Leads,Full Control
https://contoso.sharepoint.com/sites/contosotest,Contoso Auditors,View Only
https://contoso.sharepoint.com/sites/contosotest,Contoso Designers,Design
https://contoso.sharepoint.com/sites/TeamSite01,XT1000 Team Leads,Full Control
https://contoso.sharepoint.com/sites/TeamSite01,XT1000 Advisors>Edit
https://contoso.sharepoint.com/sites/Blog01,Contoso Blog Designers,Design
```

```
https://contoso.sharepoint.com/sites/Blog01,Contoso Blog Editors>Edit
https://contoso.sharepoint.com/sites/Project01,Project Alpha Approvers,Full
Control
```

The second CSV file adds one or more users to one or more groups and will have this structure:

Header:

```
PowerShell

Group,LoginName,Site
```

Item:

```
PowerShell

group,login,https://tenant.sharepoint.com/sites/site
```

Here's an example file:

```
PowerShell

Group,LoginName,Site
Contoso Project
Leads,bobbyo@contoso.com,https://contoso.sharepoint.com/sites/contosotest
Contoso
Auditors,allieb@contoso.com,https://contoso.sharepoint.com/sites/contosotest
Contoso
Designers,bonniek@contoso.com,https://contoso.sharepoint.com/sites/contosote
st
XT1000 Team
Leads,dorenap@contoso.com,https://contoso.sharepoint.com/sites/TeamSite01
XT1000
Advisors,garthf@contoso.com,https://contoso.sharepoint.com/sites/TeamSite01
Contoso Blog
Designers,janets@contoso.com,https://contoso.sharepoint.com/sites/Blog01
Contoso Blog
Editors,opalc@contoso.com,https://contoso.sharepoint.com/sites/Blog01
Project Alpha
Approvers,robinc@contoso.com,https://contoso.sharepoint.com/sites/Project01
```

For the next step, you must have the two CSV files saved to your drive. Here are example commands that use both CSV files and to add permissions and group membership:

```
PowerShell
```

```
Import-Csv C:\O365Admin\GroupsAndPermissions.csv | ForEach {New-SPOSiteGroup -Group $_.Group -PermissionLevels $_.PermissionLevels -Site $_.Site}
Import-Csv C:\O365Admin\Users.csv | ForEach {Add-SPOUser -Group $_.Group -LoginName $_.LoginName -Site $_.Site}
```

The script imports the CSV file contents and uses the values in the columns to populate the parameters of the **New-SPOSiteGroup** and **Add-SPOUser** commands. In our example, we're saving this file to the O365Admin folder on drive C, but you can save it wherever you want.

Now, let's remove a bunch of people for several groups in different sites using the same CSV file. Here's an example command:

PowerShell

```
Import-Csv C:\O365Admin\Users.csv | ForEach {Remove-SPOUser -LoginName $_.LoginName -Site $_.Site -Group $_.Group}
```

## Generate user reports

You might want to get a report for a few sites and display the users for those sites, their permission level, and other properties. This is how the syntax looks:

PowerShell

```
$tenant = "<tenant name, such as litwareinc for litwareinc.com>"
$site = "<site name>"
Get-SPOUser -Site https://$tenant.sharepoint.com/sites/$site | select * |
Format-table -Wrap -AutoSize | Out-File c\UsersReport.txt -Force -Width 360
-Append
```

This grabs the data for these three sites and writes them to a text file on your local drive. The parameter **-Append** adds new content to an existing file.

For example, let's run a report on the ContosoTest, TeamSite01, and Project01 sites for the Contoso1 tenant:

PowerShell

```
$tenant = "contoso"
$site = "contosotest"
Get-SPOUser -Site https://$tenant.sharepoint.com/sites/$site | Format-Table
-Wrap -AutoSize | Out-File c:\UsersReport.txt -Force -Width 360 -Append
$site = "TeamSite01"
Get-SPOUser -Site https://$tenant.sharepoint.com/sites/$site | Format-Table -
```

```
Wrap -AutoSize | Out-File c:\UsersReport.txt -Force -Width 360 -Append
$site = "Project01"
Get-SPOUser -Site https://$tenant.sharepoint.com/sites/$site | Format-Table
-Wrap -AutoSize | Out-File c:\UsersReport.txt -Force -Width 360 -Append
```

We had to change only the `$site` variable. The `$tenant` variable keeps its value through all three runs of the command.

However, what if you wanted to do this for every site? You can do this without having to type all those websites by using this command:

PowerShell

```
Get-SPOSite | ForEach {Get-SPOUser -Site $_.Url} | Format-Table -Wrap -
AutoSize | Out-File c:\UsersReport.txt -Force -Width 360 -Append
```

This report is fairly simple, and you can add more code to create more specific reports or reports that include more detailed information. But this should give you an idea of how to use the SharePoint Management Shell to manage users in the SharePoint environment.

## See also

[Connect to SharePoint PowerShell](#)

[Manage SharePoint with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Manage SharePoint site groups with PowerShell

Article • 08/13/2024

*This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.*

Although you can use the Microsoft 365 admin center, you can also use PowerShell for Microsoft 365 to manage your SharePoint site groups.

## Before you begin

The procedures in this article require you to connect to SharePoint. For instructions, see [Connect to SharePoint PowerShell](#).

## View SharePoint with PowerShell for Microsoft 365

The SharePoint admin center has some easy-to-use methods for managing site groups. For example, suppose you want to look at the groups, and the group members, for the `https://litwareinc.sharepoint.com/sites/finance` site. Here's what you have to do to:

1. From the SharePoint admin center, select [Active sites](#), and then select the URL of the site.
2. On the site page, select [Settings](#) (located in the upper right-hand corner of the page), and then select [Site permissions](#).

And then repeat the process for the next site you want to look at.

To get a list of the groups with PowerShell for Microsoft 365, you can use the following commands:

PowerShell

```
$siteURL = "https://litwareinc.sharepoint.com/sites/finance"
$x = Get-SPOSiteGroup -Site $siteURL
foreach ($y in $x)
{
 Write-Host $y.Title -ForegroundColor "Yellow"
 Get-SPOSiteGroup -Site $siteURL -Group $y.Title | Select-Object -
 ExpandProperty Users
```

```
 Write-Host
}
```

There are two ways to run this command set in the SharePoint Management Shell command prompt:

- Copy the commands into Notepad (or another text editor), modify the value of the \$siteURL variable, select the commands, and then paste them into the SharePoint Management Shell command prompt. When you do, PowerShell stops at a >> prompt. Press Enter to execute the `foreach` command.
- Copy the commands into Notepad (or another text editor), modify the value of the \$siteURL variable, and then save this text file with a name and the .ps1 extension in a suitable folder. Next, run the script from the SharePoint Management Shell command prompt by specifying its path and file name. Here's an example command:

```
PowerShell
C:\Scripts\SiteGroupsAndUsers.ps1
```

In both cases, you should see something similar to this:

```
PS C:\WINDOWS\system32> C:\scripts\SiteGroupsAndUsers.ps1
Select Admin
Excel Services Viewers
SHAREPOINT\system

Members
alex@litwareinc.com
allieb@litwareinc.com
annew@litwareinc.com
azizh@litwareinc.com
belindan@litwareinc.com
bonniek@litwareinc.com
robinc@litwareinc.com
davidl@litwareinc.com
zrinkam@litwareinc.com

Owners
dorenap@litwareinc.com
fabricec@litwareinc.com
garretv@litwareinc.com
garthf@litwareinc.com
janets@litwareinc.com
juliani@litwareinc.com
junminh@litwareinc.com
SHAREPOINT\system
tonyk@litwareinc.com
zrinkam@litwareinc.com

Visitors
mollyd@litwareinc.com
pavelb@litwareinc.com
sarad@litwareinc.com
```

These are all the groups that were created for the site

<https://litwareinc.sharepoint.com/sites/finance>, and all the users assigned to those

groups. The group names are in yellow to help you separate group names from their members.

As another example, here's a command set that lists the groups, and all the group memberships, for all of your SharePoint sites.

```
PowerShell

$x = Get-SPOSite
foreach ($y in $x)
{
 Write-Host $y.Url -ForegroundColor "Yellow"
 $z = Get-SPOSiteGroup -Site $y.Url
 foreach ($a in $z)
 {
 $b = Get-SPOSiteGroup -Site $y.Url -Group $a.Title
 Write-Host $b.Title -ForegroundColor "Cyan"
 $b | Select-Object -ExpandProperty Users
 Write-Host
 }
}
```

## See also

[Connect to SharePoint PowerShell](#)

[Create SharePoint sites and add users with PowerShell](#)

[Manage SharePoint users and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Connect to Exchange Online PowerShell

Article • 08/21/2023

This article contains instructions for how to connect to Exchange Online PowerShell using the Exchange Online PowerShell module with or without multi-factor authentication (MFA).

The Exchange Online PowerShell module uses modern authentication for connecting to all Exchange-related PowerShell environments in Microsoft 365: Exchange Online PowerShell, Security & Compliance PowerShell, and standalone Exchange Online Protection (EOP) PowerShell. For more information about the Exchange Online PowerShell module, see [About the Exchange Online PowerShell module](#).

To connect to Exchange Online PowerShell for automation, see [App-only authentication for unattended scripts](#) and [Use Azure managed identities to connect to Exchange Online PowerShell](#).

To connect to Exchange Online PowerShell from C#, see [Use C# to connect to Exchange Online PowerShell](#).

## What do you need to know before you begin?

- The requirements for installing and using the module are described in [Install and maintain the Exchange Online PowerShell module](#).

### Note

Remote PowerShell connections are deprecated in Exchange Online PowerShell. For more information, see [Deprecation of Remote PowerShell in Exchange Online](#).

REST API connections in the Exchange Online PowerShell V3 module require the PowerShellGet and PackageManagement modules. For more information, see [PowerShellGet for REST-based connections in Windows](#).

- After you connect, the cmdlets and parameters that you have or don't have access to is controlled by role-based access control (RBAC). For more information, see [Permissions in Exchange Online](#).

To find the permissions that are required to run specific Exchange Online cmdlets, see [Find the permissions required to run any Exchange cmdlet](#).

## 💡 Tip

Having problems? Ask in the [Exchange Online](#) forum.

# Step 1: Load the Exchange Online PowerShell module

## ⓘ Note

If the module is already installed, you can typically skip this step and run `Connect-ExchangeOnline` without manually loading the module first.

After you've [installed the module](#), open a PowerShell window and load the module by running the following command:

```
PowerShell
Import-Module ExchangeOnlineManagement
```

# Step 2: Connect and authenticate

## ⓘ Note

Connect commands will likely fail if the profile path of the account that you used to connect contains special PowerShell characters (for example, `$`). The workaround is to connect using a different account that doesn't have special characters in the profile path.

The command that you need to run uses the following syntax:

```
PowerShell
Connect-ExchangeOnline -UserPrincipalName <UPN> [-ExchangeEnvironmentName
<Value>] [-ShowBanner:$false] [-DelegatedOrganization <String>] [-
SkipLoadingFormatData]
```

For detailed syntax and parameter information, see [Connect-ExchangeOnline](#).

- <UPN> is your account in user principal name format (for example, `navin@contoso.onmicrosoft.com`).
- With the EXO V3 module (v3.0.0 or later) and the [demise of Basic authentication \(remote PowerShell\) connections to Exchange Online](#), you're using REST API cmdlets only. For more information, see [REST API connections in the EXO V3 module](#).
- When you use the *ExchangeEnvironmentName* parameter, you don't need to use the *ConnectionUri* or *AzureADAuthorizationEndPointUrl* parameters. Common values for the *ExchangeEnvironmentName* parameter are described in the following table:

[+] [Expand table](#)

Environment	Value
Microsoft 365 or Microsoft 365 GCC	n/a*
Microsoft 365 GCC High	0365USGovGCCHigh
Microsoft 365 DoD	0365USGovDoD
Office 365 Germany	0365GermanyCloud
Office 365 operated by 21Vianet	0365China

\* The required value `0365Default` is also the default value, so you don't need to use the *ExchangeEnvironmentName* parameter in Microsoft 365 or Microsoft 365 GCC environments.

- The *DelegatedOrganization* parameter specifies the customer organization that you want to manage as an authorized Microsoft Partner. For more information, see the [connection examples later in this article](#).
- Depending on the nature of your organization, you might be able to omit the *UserPrincipalName* parameter in the connection command. Instead, you enter the username and password or select stored credentials after you run the **Connect-ExchangeOnline** command. If it doesn't work, then you need to use the *UserPrincipalName* parameter.
- If you aren't using MFA, you should be able to use the *Credential* parameter instead of the *UserPrincipalName* parameter. First, run the command `$Credential = Get-Credential`, enter your username and password, and then use the variable name for the *Credential* parameter (`-Credential $Credential`). If it doesn't work, then you need to use the *UserPrincipalName* parameter.

- Use the *SkipLoadingFormatData* switch to avoid errors when connecting to Exchange Online PowerShell from within a Windows service.
- Using the module in PowerShell 7 requires version 2.0.4 or later.

The connection examples in the following sections use modern authentication, and are incapable of using Basic authentication.

## Connect to Exchange Online PowerShell with an interactive login prompt

1. The following examples work in Windows PowerShell 5.1 and PowerShell 7 for accounts with or without MFA:

- This example connects to Exchange Online PowerShell in a Microsoft 365 or Microsoft 365 GCC organization:

```
PowerShell

Connect-ExchangeOnline -UserPrincipalName
navin@contoso.onmicrosoft.com
```

- This example connects to Exchange Online PowerShell in a Microsoft GCC High organization:

```
PowerShell

Connect-ExchangeOnline -UserPrincipalName
laura@blueyonderairlines.us -ExchangeEnvironmentName
0365USGovGCCHigh
```

- This example connects to Exchange Online PowerShell in a Microsoft 365 DoD organization:

```
PowerShell

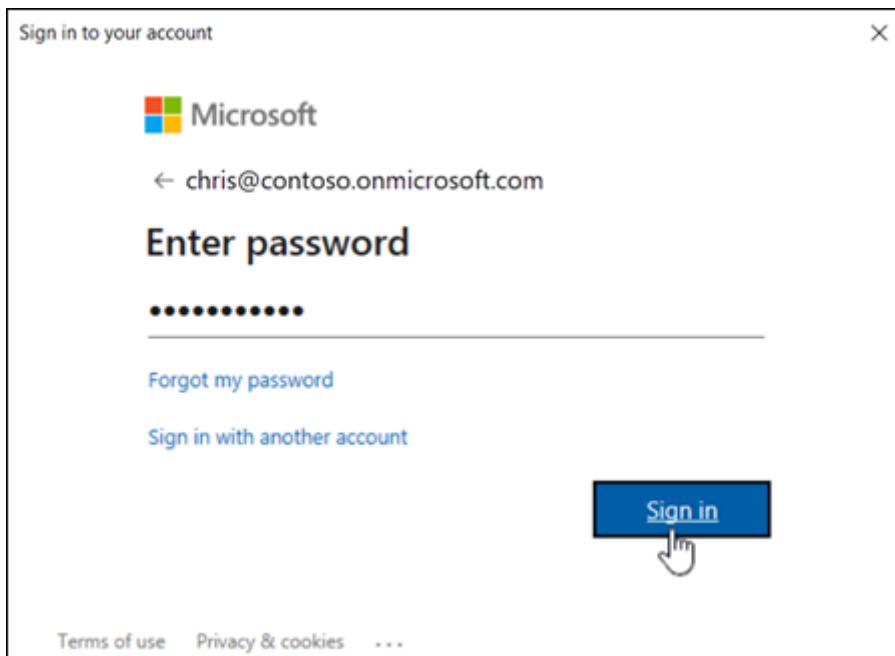
Connect-ExchangeOnline -UserPrincipalName julia@adatum.mil -
ExchangeEnvironmentName 0365USGovDoD
```

- This example connects to Exchange Online PowerShell in an Office 365 Germany organization:

```
PowerShell
```

```
Connect-ExchangeOnline -UserPrincipalName lukas@fabrikam.de -
ExchangeEnvironmentName 0365GermanyCloud
```

2. In the sign-in window that opens, enter your password, and then click **Sign in**.

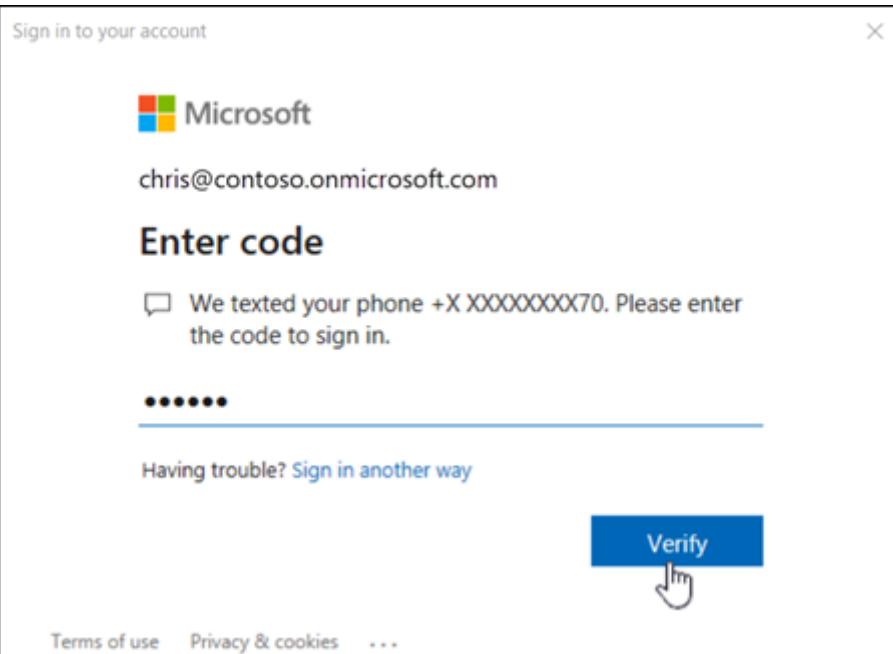


**① Note**

In PowerShell 7, browser-based single sign-on (SSO) is used by default, so the sign-in prompt opens in your default web browser instead of a standalone dialog.

3. **MFA only:** A verification code is generated and delivered based on the response option that's configured for your account (for example, a text message or the Microsoft Authenticator app on your device).

In the verification window that opens, enter the verification code, and then click **Verify**.



## PowerShell 7 exclusive connection methods

- In PowerShell 7 for accounts without MFA, this example prompts for credentials within the PowerShell window:

```
PowerShell

Connect-ExchangeOnline -UserPrincipalName navin@contoso.onmicrosoft.com
-InlineCredential
```

- In PowerShell 7 for accounts with or without MFA, this example uses another computer to authenticate and complete the connection. Typically, you use this method on computers that don't have web browsers (users are unable to enter their credentials in PowerShell 7):

1. Run the following command on the computer where you want to connect:

```
PowerShell

Connect-ExchangeOnline -Device
```

The connection command waits at following output:

To sign in, use a web browser to open the page <https://microsoft.com/devicelogin> and enter the code <XXXXXXXXXX> to authenticate.

Note the <XXXXXXXXXX> code value.

2. On any other device with a web browser and internet access, open <https://microsoft.com/devicelogin> and enter the <XXXXXXXXXX> code value from the previous step.
3. Enter your credentials on the resulting pages.
4. In the confirmation prompt, click **Continue**. The next message should indicate success, and you can close the browser or tab.
5. The command from step 1 continues to connect you to Exchange Online PowerShell.

## Connect to Exchange Online PowerShell without a login prompt (unattended scripts)

For complete instructions, see [App-only authentication for unattended scripts in Exchange Online PowerShell and Security & Compliance PowerShell](#).

## Connect to Exchange Online PowerShell in customer organizations

For more information about partners and customer organizations, see the following topics:

- [What is the Cloud Solution Provider \(CSP\) program?](#)
- [Introduction to granular delegated admin privileges \(GDAP\)](#)

This example connects to customer organizations in the following scenarios:

- Connect to a customer organization using a CSP account.
- Connect to a customer organization using a GDAP.
- Connect to a customer organization as a guest user.

PowerShell

```
Connect-ExchangeOnline -UserPrincipalName navin@contoso.onmicrosoft.com
-DelegatedOrganization adatum.onmicrosoft.com
```

## Connect to Exchange Online PowerShell using managed identity

For more information, see [Use Azure managed identities to connect to Exchange Online PowerShell](#).

- System-assigned managed identity:

```
PowerShell
```

```
Connect-ExchangeOnline -ManagedIdentity -Organization
"cohovinyard.onmicrosoft.com"
```

- User-assigned assigned managed identity:

```
PowerShell
```

```
Connect-ExchangeOnline -ManagedIdentity -Organization
"constoso.onmicrosoft.com" -ManagedIdentityAccountId
<ManagedIdentityAccountIdGuid>
```

## Step 3: Disconnect when you're finished

Be sure to disconnect the session when you're finished. If you close the PowerShell window without disconnecting the session, you could use up all the sessions available to you, and you need to wait for the sessions to expire. To disconnect the session, run the following command:

```
PowerShell
```

```
Disconnect-ExchangeOnline
```

To silently disconnect without a confirmation prompt, run the following command:

```
PowerShell
```

```
Disconnect-ExchangeOnline -Confirm:$false
```

### ⓘ Note

The disconnect command will likely fail if the profile path of the account that you used to connect contains special PowerShell characters (for example, `$`). The workaround is to connect using a different account that doesn't have special characters in the profile path.

# How do you know you've connected successfully?

If you don't receive any errors, you've connected successfully. A quick test is to run an Exchange Online PowerShell cmdlet, for example, **Get-AcceptedDomain**, and see the results.

If you receive errors, check the following requirements:

- A common problem is an incorrect password. Run the connection steps again and pay close attention to the username and password that you use.
- The account that you use to connect to must be enabled for PowerShell access. For more information, see [Enable or disable access to Exchange Online PowerShell](#).
- TCP port 80 traffic needs to be open between your local computer and Microsoft 365. It's probably open, but it's something to consider if your organization has a restrictive internet access policy.
- If your organization uses federated authentication, and your identity provider (IDP) and/or security token service (STS) isn't publicly available, you can't use a federated account to connect to Exchange Online PowerShell. Instead, create and use a non-federated account in Microsoft 365 to connect to Exchange Online PowerShell.
- REST-based connections to Exchange Online PowerShell require the `PowerShellGet` module, and by dependency, the `PackageManagement` module, so you'll receive errors if you try to connect without having them installed. For example, you might see the following error:

The term 'Update-ModuleManifest' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.

For more information about the `PowerShellGet` and `PackageManagement` module requirements, see [PowerShellGet for REST-based connections in Windows](#).

- After you connect, you might receive an error that looks like this:

Could not load file or assembly 'System.IdentityModel.Tokens.Jwt, Version= <Version>, Culture=neutral, PublicKeyToken=<TokenValue>'. Could not find or load a specific file.

This error happens when the Exchange Online PowerShell module conflicts with another module that's imported into the runspace. Try connecting in a new Windows PowerShell window before importing other modules.

## Appendix: Comparison of old and new connection methods

This section attempts to compare older connection methods that have been replaced by the Exchange Online PowerShell module. The Basic authentication and OAuth token procedures are included for historical reference only and are no longer supported.

### Connect without multi-factor authentication

- Exchange Online PowerShell module with interactive credential prompt:

```
PowerShell

Connect-ExchangeOnline -UserPrincipalName admin@contoso.onmicrosoft.com
```

- Exchange Online PowerShell module without interactive credential prompt:

```
PowerShell

$secpasswd = ConvertTo-SecureString '<Password>' -AsPlainText -Force

$o365cred = New-Object System.Management.Automation.PSCredential
("admin@contoso.onmicrosoft.com", $secpasswd)

Connect-ExchangeOnline -Credential $o365cred
```

- Basic authentication:

```
PowerShell

$secpasswd = ConvertTo-SecureString '<Password>' -AsPlainText -Force

$o365cred = New-Object System.Management.Automation.PSCredential
("admin@contoso.onmicrosoft.com", $secpasswd)

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/PowerShell-LiveID/ -
Credential $o365cred -Authentication Basic -AllowRedirection

Import-PSSession $Session
```

- New-PSSession with OAuth token:

```
PowerShell

$oauthTokenAsPassword = ConvertTo-SecureString '<EncodedOAuthToken>' -
AsPlainText -Force

$o365cred = New-Object System.Management.Automation.PSCredential
("admin@contoso.onmicrosoft.com", $oauthTokenAsPassword)

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/PowerShell-LiveID/?
BasicAuthToOAuthConversion=true -Credential $o365cred -Authentication
Basic -AllowRedirection

Import-PSSession $Session
```

## Connect with multi-factor authentication

- Exchange Online PowerShell module with interactive credential prompt:

```
PowerShell

Connect-ExchangeOnline -UserPrincipalName admin@contoso.onmicrosoft.com
```

- Basic authentication: Not available.
- New-PSSession with OAuth token: Not available.

## Connect to a customer organization with a CSP account

- Exchange Online PowerShell module:

```
PowerShell

Connect-ExchangeOnline -UserPrincipalName admin@contoso.onmicrosoft.com
-DelegatedOrganization delegated.onmicrosoft.com
```

- Basic authentication:

```
PowerShell

$secpasswd = ConvertTo-SecureString '<Password>' -AsPlainText -Force

$o365cred = New-Object System.Management.Automation.PSCredential
("admin@contoso.onmicrosoft.com", $secpasswd)
```

```
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/PowerShell-LiveID/?
DelegatedOrg=delegated.onmicrosoft.com&email=SystemMailbox{bb558c35-
97f1-4cb9-8ff7-d53741dc928c}@delegated.onmicrosoft.com -Credential
$o365cred -Authentication Basic -AllowRedirection

Import-PSSession $Session
```

- New-PSSession with OAuth token:

```
PowerShell

$oauthTokenAsPassword = ConvertTo-SecureString '<EncodedOAuthToken>' -
AsPlainText -Force

$o365cred = New-Object System.Management.Automation.PSCredential
("admin@contoso.onmicrosoft.com", $oauthTokenAsPassword)

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/PowerShell-LiveID/?
DelegatedOrg=delegated.onmicrosoft.com&BasicAuthToOAuthConversion=true&
email=SystemMailbox{bb558c35-97f1-4cb9-8ff7-
d53741dc928c}@delegated.onmicrosoft.com -Credential $o365cred -
Authentication Basic -AllowRedirection

Import-PSSession $Session
```

## Connect to a customer organization using GDAP

- Exchange Online PowerShell module:

```
PowerShell

Connect-ExchangeOnline -UserPrincipalName admin@contoso.onmicrosoft.com
-DelegatedOrganization delegated.onmicrosoft.com
```

- Basic authentication:

```
PowerShell

$secpasswd = ConvertTo-SecureString '<Password>' -AsPlainText -Force

$o365cred = New-Object System.Management.Automation.PSCredential
("admin@contoso.onmicrosoft.com", $secpasswd)

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/PowerShell-LiveID/?
DelegatedOrg=delegated.onmicrosoft.com&email=SystemMailbox{bb558c35-
```

```
97f1-4cb9-8ff7-d53741dc928c}@delegated.onmicrosoft.com -Credential
$o365cred -Authentication Basic -AllowRedirection
```

```
Import-PSSession $Session
```

- New-PSSession with OAuth token:

```
PowerShell
```

```
$oauthTokenAsPassword = ConvertTo-SecureString '<EncodedOAuthToken>' -
AsPlainText -Force
```

```
$o365cred = New-Object System.Management.Automation.PSCredential
("admin@contoso.onmicrosoft.com", $oauthTokenAsPassword)
```

```
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/PowerShell-LiveID/?
DelegatedOrg=delegated.onmicrosoft.com&BasicAuthToOAuthConversion=true&
email=SystemMailbox{bb558c35-97f1-4cb9-8ff7-
d53741dc928c}@delegated.onmicrosoft.com -Credential $o365cred -
Authentication Basic -AllowRedirection
```

```
Import-PSSession $Session
```

## Connect to a customer organization as a guest user

- Exchange Online PowerShell module:

```
PowerShell
```

```
Connect-ExchangeOnline -UserPrincipalName admin@contoso.onmicrosoft.com
-DelegatedOrganization delegated.onmicrosoft.com
```

- Basic authentication:

```
PowerShell
```

```
$secpasswd = ConvertTo-SecureString '<Password>' -AsPlainText -Force
```

```
$o365cred = New-Object System.Management.Automation.PSCredential
("admin@contoso.onmicrosoft.com", $secpasswd)
```

```
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/PowerShell-LiveID/?
DelegatedOrg=delegated.onmicrosoft.com&email=SystemMailbox{bb558c35-
97f1-4cb9-8ff7-d53741dc928c}@delegated.onmicrosoft.com -Credential
$o365cred -Authentication Basic -AllowRedirection
```

```
Import-PSSession $Session
```

- New-PSSession with OAuth token:

PowerShell

```
$oauthTokenAsPassword = ConvertTo-SecureString '<EncodedOAuthToken>' -
AsPlainText -Force

$o365cred = New-Object System.Management.Automation.PSCredential
("admin@contoso.onmicrosoft.com" , $oauthTokenAsPassword)

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/PowerShell-LiveID/?
DelegatedOrg=delegated.onmicrosoft.com&BasicAuthToOAuthConversion=true&
email=SystemMailbox{bb558c35-97f1-4cb9-8ff7-
d53741dc928c}@delegated.onmicrosoft.com -Credential $o365cred -
Authentication Basic -AllowRedirection

Import-PSSession $Session
```

## Connect to run unattended scripts

- Exchange Online PowerShell module:
  - Certificate thumbprint:

① Note

The CertificateThumbprint parameter is supported only in Microsoft Windows.

PowerShell

```
Connect-ExchangeOnline -CertificateThumbPrint
"012THISISADEMOTHUMBPRINT" -AppID "36ee4c6c-0812-40a2-b820-
b22ebd02bce3" -Organization "contoso.onmicrosoft.com"
```

- Certificate object:

PowerShell

```
Connect-ExchangeOnline -Certificate <%X509Certificate20bject%> -
AppID "36ee4c6c-0812-40a2-b820-b22ebd02bce3" -Organization
```

```
"contoso.onmicrosoft.com"
```

- Certificate file:

```
PowerShell
```

```
Connect-ExchangeOnline -CertificateFilePath
"C:\Users\navin\Desktop\automation-cert.pfx" -CertificatePassword
(ConvertTo-SecureString -String "<Password>" -AsPlainText -Force) -
AppID "36ee4c6c-0812-40a2-b820-b22ebd02bce3" -Organization
"contoso.onmicrosoft.com"
```

For more information, see [App-only authentication for unattended scripts in Exchange Online PowerShell and Security & Compliance PowerShell](#).

- Basic authentication:

```
PowerShell
```

```
$secpasswd = ConvertTo-SecureString '<Password>' -AsPlainText -Force

$o365cred = New-Object System.Management.Automation.PSCredential
("admin@contoso.onmicrosoft.com", $secpasswd)

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/PowerShell-LiveID/ -
Credential $o365cred -Authentication Basic -AllowRedirection

Import-PSSession $Session
```

- New-PSSession with OAuth token:

```
PowerShell
```

```
$oauthTokenAsPassword = ConvertTo-SecureString '<EncodedOAuthToken>' -
AsPlainText -Force

$o365cred = New-Object System.Management.Automation.PSCredential
("admin@contoso.onmicrosoft.com", $oauthTokenAsPassword)

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/PowerShell-LiveID/?
BasicAuthToOAuthConversion=true&email=SystemMailbox{bb558c35-97f1-4cb9-
8ff7-d53741dc928c}@contoso.onmicrosoft.com -Credential $o365cred -
Authentication Basic -AllowRedirection

Import-PSSession $Session
```

# Connect using managed identity

- Exchange Online PowerShell module:
  - System-assigned managed identity:

PowerShell

```
Connect-ExchangeOnline -ManagedIdentity -Organization
"contoso.onmicrosoft.com"
```

- User-assigned managed identity:

PowerShell

```
Connect-ExchangeOnline -ManagedIdentity -Organization
"contoso.onmicrosoft.com" -ManagedIdentityAccountId
<UserAssignedManagedIdentityPrincipalIdValue>
```

For more information, see [Use Azure managed identities to connect to Exchange Online PowerShell](#).

- Basic authentication: Not available.
- New-PSSession with OAuth token: Not available.

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# How to use PowerShell to migrate email to Microsoft 365

Article • 07/29/2024

*This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.*

Administrators often migrate email from existing systems when they first set up Microsoft 365. The following articles describe how to migrate email by using Windows PowerShell:

- [Use PowerShell to perform a cutover migration to Microsoft 365](#)
- [Use PowerShell to perform an IMAP migration to Microsoft 365](#)
- [Use PowerShell to perform a staged migration to Microsoft 365](#)

## Related topics

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

[Manage SharePoint with PowerShell](#)

[Use Windows PowerShell to create reports in Microsoft 365](#)

[Why you need to use Microsoft 365 PowerShell](#)

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Use PowerShell to perform a cutover migration to Microsoft 365

Article • 02/17/2023

*This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.*

You can migrate the contents of user mailboxes from a source email system to Microsoft 365 all at once by using a cutover migration. This article walks you through the tasks for an email cutover migration by using Exchange Online PowerShell.

By reviewing the topic, [What you need to know about a cutover email migration to Microsoft 365](#), you can get an overview of the migration process. When you're comfortable with the contents of that article, use this one to begin migrating mailboxes from one email system to another.

## ⓘ Note

You can also use the [Exchange admin center](#) to perform a cutover migration. See [Perform a cutover migration of email to Microsoft 365](#).

## What do you need to know before you begin?

Estimated time to complete this task: 2-5 minutes to create a migration batch. After the migration batch is started, the duration of the migration will vary based on the number of mailboxes in the batch, the size of each mailbox, and your available network capacity. For information about other factors that affect how long it takes to migrate mailboxes to Microsoft 365, see [Migration Performance](#).

You need to be assigned permissions before you can perform this procedure or procedures. To see what permissions you need, see the "Migration" entry in a table in the [Recipients Permissions](#) topic.

To use the Exchange Online PowerShell cmdlets, you need to sign in and import the cmdlets into your local Windows PowerShell session. See [Connect to Exchange Online PowerShell](#) for instructions.

For a full list of migration commands, see [Move and migration cmdlets](#).

## Migration steps

# Step 1: Prepare for a cutover migration

- Add your on-premises Exchange organization as an accepted domain of your Microsoft 365 organization. The migration service uses the SMTP address of your on-premises mailboxes to create the Microsoft Online Services user ID and email address for the new Microsoft 365 mailboxes. Migration will fail if your Exchange domain isn't an accepted domain or the primary domain of your Microsoft 365 organization. For more information, see [Verify your domain](#).
- Configure Outlook Anywhere on your on-premises Exchange server. The email migration service uses RPC over HTTP, or Outlook Anywhere, to connect to your on-premises Exchange server. For information about how to set up Outlook Anywhere for Exchange 2010, Exchange 2007, and Exchange 2003, see the following:
  - [Exchange 2010: Enable Outlook Anywhere](#)
  - [Exchange 2007: How to Enable Outlook Anywhere](#)
  - [Exchange 2003: Deployment Scenarios for RPC over HTTP](#)
  - [How to Configure Outlook Anywhere with Exchange 2003](#)

## Important

Your Outlook Anywhere configuration must be configured with a certificate issued by a trusted certification authority (CA). It can't be configured with a self-signed certificate. For more information, see [How to Configure SSL for Outlook Anywhere](#).

- Verify that you can connect to your Exchange organization using Outlook Anywhere. Try one of these methods to test your connection settings:
  - Use Microsoft Outlook from outside your corporate network to connect to your on-premises Exchange mailbox.
  - Use the Microsoft [Exchange Remote Connectivity Analyzer](#) to test your connection settings. Use the Outlook Anywhere (RPC over HTTP) or Outlook Autodiscover tests.
  - Run the following commands in Exchange Online PowerShell.

PowerShell

```
$Credentials = Get-Credential
```

PowerShell

```
Test-MigrationServerAvailability -ExchangeOutlookAnywhere -Autodiscover
-EmailAddress <email address for on-premises administrator> -
Credentials $credentials
```

- **Assign an on-premises user account the necessary permissions to access mailboxes in your Exchange organization.** The on-premises user account that you use to connect to your on-premises Exchange organization (also called the migration administrator) must have the necessary permissions to access the on-premises mailboxes that you want to migrate to Microsoft 365. This user account is used to create a migration endpoint to your on-premises organization.

The following list shows the administrative privileges required to migrate mailboxes using a cutover migration. There are three possible options.

- The migration administrator must be a member of the **Domain Admins** group in Active Directory in the on-premises organization.

Or

- The migration administrator must be assigned the **FullAccess** permission for each on-premises mailbox.

Or

- The migration administrator must be assigned the **Receive As** permission on the on-premises mailbox database that stores the user mailboxes.

- **Disable Unified Messaging.** If the on-premises mailboxes you're migrating are enabled for Unified Messaging (UM), you have to disable UM on the mailboxes before you migrate them. You can then enable UM on the mailboxes after the migration is complete.

- **Security Groups and Delegates** The email migration service cannot detect whether on-premises Active Directory groups are security groups or not, so it cannot provision any migrated groups as security groups in Microsoft 365. If you want to have security groups in your Microsoft 365 tenant, you must first provision an empty mail-enabled security group in your Microsoft 365 tenant before starting the cutover migration. Additionally, this migration method only moves mailboxes, mail users, mail contacts, and mail-enabled groups. If any other Active Directory

object, such as user that is not migrated to Microsoft 365, is assigned as a manager or delegate to an object being migrated, they must be removed from the object before you migrate.

## Step 2: Create a migration endpoint

To migrate email successfully, Microsoft 365 needs to connect and communicate with the source email system. To do this, Microsoft 365 uses a migration endpoint. To create an Outlook Anywhere migration endpoint for cutover migration, first [connect to Exchange Online](#).

For a full list of migration commands, see [Move and migration cmdlets](#).

Run the following commands in Exchange Online PowerShell:

PowerShell

```
$Credentials = Get-Credential
```

The example uses the [Test-MigrationServerAvailability](#) cmdlet to obtain and test the connection settings to the on-premises Exchange server, and then uses those connection settings to create the migration endpoint called "CutoverEndpoint".

PowerShell

```
$TSMA = Test-MigrationServerAvailability -ExchangeOutlookAnywhere -
Autodiscover -EmailAddress administrator@contoso.com -Credentials
$credentials
```

PowerShell

```
New-MigrationEndpoint -ExchangeOutlookAnywhere -Name CutoverEndpoint -
ConnectionSettings $TSMA.ConnectionSettings
```

### ⓘ Note

The [New-MigrationEndpoint](#) cmdlet can be used to specify a database for the service to use by using the **-TargetDatabase** option. Otherwise a database is randomly assigned from the Active Directory Federation Services (AD FS) 2.0 site where the management mailbox is located.

## Verify it worked

In Exchange Online PowerShell, run the following command to display information about the "CutoverEndpoint" migration endpoint:

PowerShell

```
Get-MigrationEndpoint CutoverEndpoint | Format-List
EndpointType,ExchangeServer,UseAutoDiscover,Max*
```

## Step 3: Create the cutover migration batch

You can use the **New-MigrationBatch** cmdlet in Exchange Online PowerShell to create a migration batch for a cutover migration. You can create a migration batch and start it automatically by including the *AutoStart* parameter. Alternatively, you can create the migration batch and then manually start it afterwards by using the **Start-MigrationBatch** cmdlet. This example creates a migration batch called "CutoverBatch" and uses the migration endpoint that was created in the previous step.

PowerShell

```
New-MigrationBatch -Name CutoverBatch -SourceEndpoint CutoverEndpoint -
AutoStart
```

This example also creates a migration batch called "CutoverBatch" and uses the migration endpoint that was created in the previous step. Because the *AutoStart* parameter isn't included, the migration batch has to be manually started on the migration dashboard or by using **Start-MigrationBatch** cmdlet. As previously stated, only one cutover migration batch can exist at a time.

PowerShell

```
New-MigrationBatch -Name CutoverBatch -SourceEndpoint CutoverEndpoint
```

## Verify it worked

To verify that you've successfully created a migration batch for a cutover migration, run the following command in Exchange Online PowerShell to display information about the new migration batch:

PowerShell

```
Get-MigrationBatch | Format-List
```

## Step 4: Start the cutover migration batch

To start the migration batch in Exchange Online PowerShell, run the following command. This will create a migration batch called "CutoverBatch".

PowerShell

```
Start-MigrationBatch -Identity CutoverBatch
```

## Verify it worked

If a migration batch is successfully started, its status on the migration dashboard is specified as Syncing. To verify that you've successfully started a migration batch using Exchange Online PowerShell, run the following command:

PowerShell

```
Get-MigrationBatch -Identity CutoverBatch | Format-List Status
```

## Step 5: Route your email to Microsoft 365

Email systems use a DNS record called an MX record to figure out where to deliver emails. During the email migration process, your MX record was pointing to your source email system. Now that the email migration to Microsoft 365 is complete, it's time to point your MX record at Microsoft 365. This helps make sure that email is delivered to your Microsoft 365 mailboxes. By moving the MX record, you can also turn off your old email system when you're ready.

For many DNS providers, there are specific instructions to change your MX record. If your DNS provider isn't included, or if you want to get a sense of the general directions, [general MX record instructions](#) are provided as well.

It can take up to 72 hours for the email systems of your customers and partners to recognize the changed MX record. Wait at least 72 hours before you proceed to the next task: [Step 6: Delete the cutover migration batch](#).

## Step 6: Delete the cutover migration batch

After you change the MX record and verify that all email is being routed to Microsoft 365 mailboxes, notify the users that their mail is going to Microsoft 365. After this, you can delete the cutover migration batch. Verify the following before you delete the migration batch.

- All users are using Microsoft 365 mailboxes. After the batch is deleted, mail sent to mailboxes on the on-premises Exchange Server isn't copied to the corresponding Microsoft 365 mailboxes.
- Microsoft 365 mailboxes were synchronized at least once after mail began being sent directly to them. To do this, make sure that the value in the Last Synced Time box for the migration batch is more recent than when mail started being routed directly to Microsoft 365 mailboxes.

To delete the "CutoverBatch" migration batch in Exchange Online PowerShell, run the following command:

```
PowerShell
```

```
Remove-MigrationBatch -Identity CutoverBatch
```

## Section 7: Assign user licenses

Activate Microsoft 365 user accounts for the migrated accounts by assigning licenses. If you don't assign a license, the mailbox is disabled when the grace period ends (30 days). To assign a license in the Microsoft 365 admin center, see [Assign or unassign licenses](#).

## Step 8: Complete post-migration tasks

- **Create an Autodiscover DNS record so users can easily get to their mailboxes.**  
After all on-premises mailboxes are migrated to Microsoft 365, you can configure an Autodiscover DNS record for your Microsoft 365 organization to enable users to easily connect to their new Microsoft 365 mailboxes with Outlook and mobile clients. This new Autodiscover DNS record has to use the same namespace that you're using for your Microsoft 365 organization. For example, if your cloud-based namespace is cloud.contoso.com, the Autodiscover DNS record you need to create is autodiscover.cloud.contoso.com.

If you keep your Exchange Server, you should also make sure that Autodiscover DNS CNAME record has to point to Microsoft 365 in both internal and external

DNS after the migration so that the Outlook client will connect to the correct mailbox.

 **Note**

In Exchange 2007, Exchange 2010, and Exchange 2013 you should also set `Set-ClientAccessServer AutodiscoverInternalConnectionURI to Null`.

Microsoft 365 uses a CNAME record to implement the Autodiscover service for Outlook and mobile clients. The Autodiscover CNAME record must contain the following information:

- **Alias:** autodiscover
- **Target:** autodiscover.outlook.com

For more information, see [Add DNS records to connect your domain](#).

- **Decommission on-premises Exchange servers.** After you've verified that all email is being routed directly to the Microsoft 365 mailboxes, and you no longer need to maintain your on-premises email organization or don't plan on implementing a single sign-on (SSO) solution, you can uninstall Exchange from your servers and remove your on-premises Exchange organization.

For more information, see the following:

- [Modify or Remove Exchange 2010](#)
- [How to Remove an Exchange 2007 Organization](#)
- [How to Uninstall Exchange Server 2003](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Use PowerShell to perform an IMAP migration to Microsoft 365

Article • 04/12/2024

*This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.*

As part of the process of deploying Microsoft 365, you can choose to migrate the contents of user mailboxes from an Internet Mail Access Protocol (IMAP) email service to Microsoft 365. This article walks you through the tasks for an email IMAP migration by using Exchange Online PowerShell.

## ⓘ Note

You can also use the [Exchange admin center](#) to perform an IMAP migration. See [Migrate your IMAP mailboxes](#).

## What do you need to know before you begin?

Estimated time to complete this task: 2-5 minutes to create a migration batch. After the migration batch is started, the duration of the migration will vary based on the number of mailboxes in the batch, the size of each mailbox, and your available network capacity. For information about other factors that affect how long it takes to migrate mailboxes to Microsoft 365, see [Migration Performance](#).

You need to be assigned permissions before you can perform this procedure or procedures. To see what permissions you need, see the "Migration" entry in a table in the [Recipients Permissions](#) article.

To use the Exchange Online PowerShell cmdlets, you need to sign in and import the cmdlets into your local Windows PowerShell session. See [Connect to Exchange Online PowerShell](#) for instructions.

For a full list of migration commands, see [Move and migration cmdlets](#).

The following restrictions apply to IMAP migrations:

- Only items in a user's inbox or other mail folders can be migrated. You can't migrate contacts, calendar items, or tasks.
- A maximum of 500,000 items can be migrated from a user's mailbox.

- The maximum message size that can be migrated is 35 MB.

## Migration steps

### Step 1: Prepare for an IMAP migration

- If you have a domain for your IMAP organization, add it as an accepted domain of your Microsoft 365 organization. If you want to use the same domain you already own for your Microsoft 365 mailboxes, you first have to add it as an accepted domain to Microsoft 365. After you have added it, you can create your users in Microsoft 365. For more information, see [Verify your domain](#).
- Add each user to Microsoft 365 so that they have a mailbox. For instructions, see [Add users to Microsoft 365 for business](#).
- Obtain the FQDN of the IMAP server. You need to provide the fully qualified domain name (FQDN) (also called the full computer name) of the IMAP server that you'll migrate mailbox data from when you create an IMAP migration endpoint. Use an IMAP client or the PING command to verify that you can use the FQDN to communicate with the IMAP server over the Internet.
- Configure the firewall to allow IMAP connections. You might have to open ports in the firewall of the organization that hosts the IMAP server so network traffic originating from the Microsoft datacenter during the migration is allowed to enter the organization that hosts the IMAP server. For a list of IP addresses used by Microsoft datacenters, see [Exchange Online URLs and IP Address Ranges](#).
- Assign the administrator account permissions to access mailboxes in your IMAP organization. If you use administrator credentials in the CSV file, the account that you use must have the necessary permissions to access the on-premises mailboxes. The permissions required to access user mailboxes is determined by the particular IMAP server.
- To use the Exchange Online PowerShell cmdlets, you need to sign in and import the cmdlets into your local Windows PowerShell session. See [Connect to Exchange Online PowerShell](#) for instructions.

For a full list of migration commands, see [Move and migration cmdlets](#).

- Verify that you can connect to your IMAP server. Run the following command in Exchange Online PowerShell to test the connection settings to your IMAP server.

PowerShell

```
Test-MigrationServerAvailability -IMAP -RemoteServer <FQDN of IMAP server> -Port <143 or 993> -Security <None, Ssl, or Tls>
```

For the value of the **Port** parameter, it's typical to use 143 for unencrypted or Transport Layer Security (TLS) connections and to use 993 for SSL connections.

## Step 2: Create a CSV file for an IMAP migration batch

Identify the group of users whose mailboxes you want to migrate in an IMAP migration batch. Each row in the CSV file contains information necessary to connect to a mailbox in the IMAP messaging system.

Here are the required attributes for each user:

- **EmailAddress** specifies the user ID for the user's Microsoft 365 mailbox.
- **UserName** specifies the sign in name for the account to use to access the mailbox on the IMAP server.
- **Password** specifies the password for the account in the **UserName** column.

Here's an example of the format for the CSV file. In this example, three mailboxes are migrated:

PowerShell

```
EmailAddress,UserName,Password
terrya@contoso.edu,terry.adams,1091990
annb@contoso.edu,ann.beebe,2111991
paulc@contoso.edu,paul.cannon,3281986
```

For the **UserName** attribute, in addition to the user name, you can use the credentials of an account that has been assigned the necessary permissions to access mailboxes on the IMAP server, the following are some of the specific formats used for some of the IMAP servers:

### Microsoft Exchange:

If you're migrating email from the IMAP implementation for Microsoft Exchange, use the format **Domain/Admin\_UserName/User\_UserName** for the **UserName** attribute in the CSV file. Let's say you're migrating email from Exchange for Terry Adams, Ann Beebe, and Paul Cannon. You have a mail administrator account, where the user name is **mailadmin** and the password is **P@ssw0rd**. Here's what your CSV file would look like:

#### PowerShell

```
EmailAddress,UserName,Password
terrya@contoso.edu,contoso-students/mailadmin/terry.adams,P@ssw0rd
annb@contoso.edu,contoso-students/mailadmin/ann.beebe,P@ssw0rd
paulc@contoso.edu,contoso-students/mailadmin/paul.cannon,P@ssw0rd
```

#### Dovecot:

For IMAP servers that support Simple Authentication and Security Layer (SASL), such as a Dovecot IMAP server, use the format **User\_UserName\*Admin\_UserName**, where the asterisk ( \* ) is a configurable separator character. Let's say you're migrating those same users' email from a Dovecot IMAP server using the administrator credentials **mailadmin** and **P@ssw0rd**. Here's what your CSV file would look like:

#### PowerShell

```
EmailAddress,UserName,Password
terrya@contoso.edu,terry.adams*mailadmin,P@ssw0rd
annb@contoso.edu,ann.beebe*mailadmin,P@ssw0rd
paulc@contoso.edu,paul.cannon*mailadmin,P@ssw0rd
```

#### Mirapoint:

If you're migrating email from Mirapoint Message Server, use the format **#user@domain#Admin\_UserName#** for the administrator credentials. To migrate email from Mirapoint using the administrator credentials **mailadmin** and **P@ssw0rd**, your CSV file would look like this:

#### PowerShell

```
EmailAddress,UserName,Password
terrya@contoso.edu,#terry.adams@contoso-students.edu#mailadmin#,P@ssw0rd
annb@contoso.edu,#ann.beebe@contoso-students.edu#mailadmin#,P@ssw0rd
paulc@contoso.edu,#paul.cannon@contoso-students.edu#mailadmin#,P@ssw0rd
```

#### Courier IMAP:

Some source email systems, such as Courier IMAP, don't support using mailbox admin credentials to migrate mailboxes to Microsoft 365. Instead, you can set up your source email system to use virtual shared folders. By using virtual shared folders, you can use the mailbox admin credentials to access user mailboxes on the source email system. For more information about how to configure virtual shared folders for Courier IMAP, see [Shared Folders](#).

To migrate mailboxes after you set up virtual shared folders on your source email system, you have to include the optional attribute **UserRoot** in the migration file. This attribute specifies the location of each user's mailbox in the virtual shared folder structure on the source email system. For example, the path to Terry's mailbox is /users/terry.adams.

Here's an example of a CSV file that contains the **UserRoot** attribute:

PowerShell

```
EmailAddress,UserName,Password,UserRoot
terrya@contoso.edu,mailadmin,P@ssw0rd,/users/terry.adams
annb@contoso.edu,mailadmin,P@ssw0rd,/users/ann.beebe
paulc@contoso.edu,mailadmin,P@ssw0rd,/users/paul.cannon
```

## Step 3: Create an IMAP migration endpoint

To migrate email successfully, Microsoft 365 needs to connect to and communicate with the source email system. To do this, Microsoft 365 uses a migration endpoint. The migration endpoint also defines the number of mailboxes to migrate simultaneously and the number of mailboxes to synchronize simultaneously during incremental synchronization, which occurs once every 24 hours. To create a migration end point for IMAP migration, first [connect to Exchange Online](#).

For a full list of migration commands, see [Move and migration cmdlets](#).

To create the IMAP migration endpoint called "IMAPEndpoint" in Exchange Online PowerShell, run the following command:

PowerShell

```
New-MigrationEndpoint -IMAP -Name IMAPEndpoint -RemoteServer
imap.contoso.com -Port 993 -Security Ssl
```

You can also add parameters to specify concurrent migrations, concurrent incremental migrations, and the port to use. The following Exchange Online PowerShell command creates an IMAP migration endpoint called "IMAPEndpoint" that supports 50 concurrent migrations and up to 25 concurrent incremental synchronizations. It also configures the endpoint to use port 143 for TLS encryption.

PowerShell

```
New-MigrationEndpoint -IMAP -Name IMAPEndpoint -RemoteServer
imap.contoso.com -Port 143 -Security Tls -MaxConcurrentMigrations
50 -MaxConcurrentIncrementalSyncs 25
```

For more information about the [New-MigrationEndpoint](#) cmdlet, see [New-MigrationEndpoint](#).

## Verify it worked

Run the following command in Exchange Online PowerShell to display information about the "IMAPEndpoint":

PowerShell

```
Get-MigrationEndpoint IMAPEndpoint | Format-List
EndpointType,RemoteServer,Port,Security,Max*
```

## Step 4: Create and start an IMAP migration batch

You can use the [New-MigrationBatch](#) cmdlet to create a migration batch for an IMAP migration. You can create a migration batch and start it automatically by including the *AutoStart* parameter. Alternatively, you can create the migration batch and then start it afterwards by using the [Start-MigrationBatch](#) cmdlet.

The following Exchange Online PowerShell command will automatically start the migration batch called "IMAPBatch1" using the IMAP endpoint called "IMAPEndpoint":

PowerShell

```
New-MigrationBatch -Name IMAPBatch1 -SourceEndpoint IMAPEndpoint -CSVData
([System.IO.File]::ReadAllBytes("C:\Users\Administrator\Desktop\IMAPmigratio
n_1.csv")) -AutoStart
```

## Verify it worked

Run the [Get-MigrationBatch](#) cmdlet to display information about the "IMAPBatch1":

PowerShell

```
Get-MigrationBatch -Identity IMAPBatch1 | Format-List
```

You can also verify that the batch has started by running the following command:

```
Get-MigrationBatch -Identity IMAPBatch1 | Format-List Status
```

## Step 5: Route your email to Microsoft 365

Email systems use a DNS record called an MX record to figure out where to deliver emails. During the email migration process, your MX record was pointing to your source email system. Now that the email migration to Microsoft 365 is complete, it's time to point your MX record at Microsoft 365. This helps make sure that email is delivered to your Microsoft 365 mailboxes. By moving the MX record, you can also turn off your old email system when you're ready.

For many DNS providers, there are specific instructions to change your MX record. If your DNS provider isn't included, or if you want to get a sense of the general directions, [general MX record instructions](#) are provided as well.

It can take up to 72 hours for the email systems of your customers and partners to recognize the changed MX record. Wait at least 72 hours before you proceed to the next task: Step 6: Delete IMAP migration batch.

## Step 6: Delete IMAP migration batch

After you change the MX record and verify that all email is being routed to Microsoft 365 mailboxes, notify the users that their mail is going to Microsoft 365. After this, you can delete the IMAP migration batch. Verify the following before you delete the migration batch.

- All users are using Microsoft 365 mailboxes. After the batch is deleted, mail sent to mailboxes on the on-premises Exchange Server isn't copied to the corresponding Microsoft 365 mailboxes.
- Microsoft 365 mailboxes were synchronized at least once after mail began being sent directly to them. To do this, make sure that the value in the Last Synced Time box for the migration batch is more recent than when mail started being routed directly to Microsoft 365 mailboxes.

To delete the "IMAPBatch1" migration batch from Exchange Online PowerShell, run the following command:

```
Remove-MigrationBatch -Identity IMAPBatch1
```

For more information about the **Remove-MigrationBatch** cmdlet, see[Remove-MigrationBatch](#).

## Verify it worked

Run the following command in Exchange Online PowerShell to display information about the "IMAPBatch1":

PowerShell

```
Get-MigrationBatch IMAPBatch1"
```

The command will return either the migration batch with a status of **Removing**, or it will return an error stating that migration batch couldn't be found, verifying that the batch was deleted.

For more information about the **Get-MigrationBatch** cmdlet, see[Get-MigrationBatch](#).

## See also

[IMAP Migration Troubleshooter](#)

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Use PowerShell to perform a staged migration to Microsoft 365

Article • 06/27/2024

*This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.*

You can migrate the contents of user mailboxes from a source email system to Microsoft 365 over time using a staged migration.

This article walks you through the tasks involved with for a staged email migration using Exchange Online PowerShell. The topic, [What you need to know about a staged email migration](#), gives you an overview of the migration process. When you're comfortable with the contents of that article, use this one to begin migrating mailboxes from one email system to another.

## ⓘ Note

You can also use the [Exchange admin center](#) to perform staged migration. See [Perform a staged migration of email to Microsoft 365](#).

## What do you need to know before you begin?

Estimated time to complete this task: 2-5 minutes to create a migration batch. After the migration batch is started, the duration of the migration will vary based on the number of mailboxes in the batch, the size of each mailbox, and your available network capacity. For information about other factors that affect how long it takes to migrate mailboxes to Microsoft 365, see [Migration Performance](#).

You need to be assigned permissions before you can perform this procedure or procedures. To see what permissions you need, see the "Migration" entry in the [Recipients Permissions](#) topic.

To use the Exchange Online PowerShell cmdlets, you need to sign in and import the cmdlets into your local Windows PowerShell session. See [Connect to Exchange Online PowerShell](#) for instructions.

For a full list of migration commands, see [Move and migration cmdlets](#).

## Migration steps

# Step 1: Prepare for a staged migration

Before you migrate mailboxes to Microsoft 365 by using a staged migration, there are a few changes you must make to your Exchange environment.

**Configure Outlook Anywhere on your on-premises Exchange Server** The email migration service uses Outlook Anywhere (also known as RPC over HTTP), to connect to your on-premises Exchange Server. For information about how to set up Outlook Anywhere for Exchange Server 2007, and Exchange 2003, see the following:

- [Exchange 2007: How to Enable Outlook Anywhere](#)
- [How to configure Outlook Anywhere with Exchange 2003](#)

## Important

You must use a certificate issued by a trusted certification authority (CA) with your Outlook Anywhere configuration. Outlook Anywhere can't be configured with a self-signed certificate. For more information, see [How to configure SSL for Outlook Anywhere](#).

**Optional: Verify that you can connect to your Exchange organization using Outlook Anywhere** Try one of the following methods to test your connection settings.

- Use Outlook from outside your corporate network to connect to your on-premises Exchange mailbox.
- Use the [Microsoft Remote Connectivity Analyzer](#) to test your connection settings. Use the Outlook Anywhere (RPC over HTTP) or Outlook Autodiscover tests.
- Run the following commands in Exchange Online PowerShell:

```
PowerShell
```

```
$Credentials = Get-Credential
```

```
PowerShell
```

```
Test-MigrationServerAvailability -ExchangeOutlookAnywhere -Autodiscover
-EmailAddress <email address for on-premises administrator> -
Credentials $credentials
```

**Set permissions** The on-premises user account that you use to connect to your on-premises Exchange organization (also called the migration administrator) must have the necessary permissions to access the on-premises mailboxes that you want to migrate to Microsoft 365. This user account is used when you connect to your email system by creating a migration endpoint later in this procedure [Step 3: Create a migration endpoint](#).

To migrate the mailboxes, the admin must have one of the following permission sets:

- Be a member of the **Domain Admins** group in Active Directory in the on-premises organization.

or
- Be assigned the **FullAccess** permission for each on-premises mailbox and the **WriteProperty** permission to modify the **TargetAddress** property on the on-premises user accounts.

or
- Be assigned the **Receive As** permission on the on-premises mailbox database that stores user mailboxes and the **WriteProperty** permission to modify the **TargetAddress** property on the on-premises user accounts.

For instructions about how to set these permissions, see [Assign permissions to migrate mailboxes to Microsoft 365](#).

**Disable Unified Messaging (UM)** If UM is turned on for the on-premises mailboxes you're migrating, turn off UM before migration. Turn on UM for the mailboxes after migration is complete. For how-to steps, see [disable unified messaging](#).

**Use directory synchronization to create new users in Microsoft 365.** You use directory synchronization to create all the on-premises users in your Microsoft 365 organization.

You need to license the users after they're created. You have 30 days to add licenses after the users are created. For steps to add licenses, see [Step 8: Complete post-migration tasks](#).

You can use either the Microsoft Entra Synchronization Tool or the Microsoft Azure AD Sync Services to synchronize and create your on-premises users in Microsoft 365. After mailboxes are migrated to Microsoft 365, you manage user accounts in your on-premises organization, and they're synchronized with your Microsoft 365 organization. For more information, see [Directory Integration](#).

## Step 2: Create a CSV file for a staged migration batch

After you identify the users whose on-premises mailboxes you want to migrate to Microsoft 365, you use a comma separated value (CSV) file to create a migration batch. Each row in the CSV file—used by Microsoft 365 to run the migration—contains information about an on-premises mailbox.

### Note

There isn't a limit for the number of mailboxes that you can migrate to Microsoft 365 using a staged migration. The CSV file for a migration batch can contain a maximum of 2,000 rows. To migrate more than 2,000 mailboxes, create additional CSV files and use each file to create a new migration batch.

### Supported attributes

The CSV file for a staged migration supports the following three attributes. Each row in the CSV file corresponds to a mailbox and must contain a value for each of these attributes.

 Expand table

Attribute	Description	Required?
EmailAddress	Specifies the primary SMTP email address, for example, pilarp@contoso.com, for on-premises mailboxes. Use the primary SMTP address for on-premises mailboxes and not user IDs from the Microsoft 365. For example, if the on-premises domain is named contoso.com but the Microsoft 365 email domain is named service.contoso.com, you would use the contoso.com domain name for email addresses in the CSV file.	Required
Password	The password to be set for the new Microsoft 365 mailbox. Any password restrictions that are applied to your Microsoft 365 organization also apply to the passwords included in the CSV file.	Optional
ForceChangePassword	Specifies whether a user must change the password the first time they sign in to their new Microsoft 365 mailbox. Use <b>True</b> or <b>False</b> for the value of this parameter. > [!NOTE]> If you've implemented a single sign-on (SSO) solution by deploying Active Directory Federation Services (AD FS) or greater in your on-premises organization, you	Optional

Attribute	Description	Required?
	must use <b>False</b> for the value of the <b>ForceChangePassword</b> attribute.	

## CSV file format

Here's an example of the format for the CSV file. In this example, three on-premises mailboxes are migrated to Microsoft 365.

The first row, or header row, of the CSV file lists the names of the attributes, or fields, specified in the rows that follow. Each attribute name is separated by a comma.

PowerShell

```
EmailAddress,Password,ForceChangePassword
pilarp@contoso.com,Pa$$w0rd,False
tobyn@contoso.com,Pa$$w0rd,False
briant@contoso.com,Pa$$w0rd,False
```

Each row under the header row represents one user and supplies the information that will be used to migrate the user's mailbox. The attribute values in each row must be in the same order as the attribute names in the header row.

Use any text editor, or an application like Excel , to create the CSV file. Save the file as a .csv or .txt file.

### Note

If the CSV file contains non-ASCII or special characters, save the CSV file with UTF-8 or other Unicode encoding. Depending on the application, saving the CSV file with UTF-8 or other Unicode encoding can be easier when the system locale of the computer matches the language used in the CSV file.

## Step 3: Create a migration endpoint

To migrate email successfully, Microsoft 365 needs to connect and communicate with the source email system. To do this, Microsoft 365 uses a migration endpoint. To create an Outlook Anywhere migration endpoint by using PowerShell, for staged migration, first [connect to Exchange Online](#).

For a full list of migration commands, see [Move and migration cmdlets](#).

To create an Outlook Anywhere migration endpoint called "StagedEndpoint" in Exchange Online PowerShell, run the following commands:

```
PowerShell
```

```
$Credentials = Get-Credential
```

```
PowerShell
```

```
New-MigrationEndpoint -ExchangeOutlookAnywhere -Name StagedEndpoint -
Autodiscover -EmailAddress administrator@contoso.com -Credentials
$Credentials
```

For more information about the **New-MigrationEndpoint** cmdlet, see [New-MigrationEndpoint](#).

#### Note

The **New-MigrationEndpoint** cmdlet can be used to specify a database for the service to use by using the **-TargetDatabase** option. Otherwise a database is randomly assigned from the Active Directory Federation Services (AD FS) 2.0 site where the management mailbox is located.

## Verify it worked

In Exchange Online PowerShell, run the following command to display information about the "StagedEndpoint" migration endpoint:

```
PowerShell
```

```
Get-MigrationEndpoint StagedEndpoint | Format-List
EndpointType, ExchangeServer, UseAutoDiscover, Max*
```

## Step 4: Create and start a stage migration batch

You can use the **New-MigrationBatch** cmdlet in Exchange Online PowerShell to create a migration batch for a cutover migration. You can create a migration batch and start it automatically by including the *AutoStart* parameter. Alternatively, you can create the migration batch and then manually start it afterwards by using the **Start-MigrationBatch** cmdlet. This example creates a migration batch called "StagedBatch1" and uses the migration endpoint that was created in the previous step.

PowerShell

```
New-MigrationBatch -Name StagedBatch1 -SourceEndpoint StagedEndpoint -
AutoStart
```

This example also creates a migration batch called "StagedBatch1" and uses the migration endpoint that was created in the previous step. Because the *AutoStart* parameter isn't included, the migration batch has to be manually started on the migration dashboard or by using **Start-MigrationBatch** cmdlet. As previously stated, only one cutover migration batch can exist at a time.

PowerShell

```
New-MigrationBatch -Name StagedBatch1 -SourceEndpoint StagedEndpoint
```

## Verify it worked

Run the following command in Exchange Online PowerShell to display information about the "StagedBatch1":

PowerShell

```
Get-MigrationBatch -Identity StagedBatch1 | Format-List
```

You can also verify that the batch has started by running the following command:

PowerShell

```
Get-MigrationBatch -Identity StagedBatch1 | Format-List Status
```

For more information about the **Get-MigrationBatch** cmdlet, see [Get-MigrationBatch](#).

## Step 5: Convert on-premises mailboxes to mail-enabled users

After you have successfully migrated a batch of mailboxes, you need some way to let users get to their mail. A user whose mailbox has been migrated now has both a mailbox on-premises and one in Microsoft 365. Users who have a mailbox in Microsoft 365 will stop receiving new mail in their on-premises mailbox.

Because you are not done with your migrations, you are not yet ready to direct all users to Microsoft 365 for their email. So what do you do for those people who have both?

What you can do is change the on-premises mailboxes that you've already migrated to mail-enabled users. When you change from a mailbox to a mail-enabled user, you can direct the user to Microsoft 365 for their email instead of going to their on-premises mailbox.

Another important reason to convert on-premises mailboxes to mail-enabled users is to retain proxy addresses from the Microsoft 365 mailboxes by copying proxy addresses to the mail-enabled users. This lets you manage cloud-based users from your on-premises organization by using Active Directory. Also, if you decide to decommission your on-premises Exchange Server organization after all mailboxes are migrated to Microsoft 365, the proxy addresses you've copied to the mail-enabled users will remain in your on-premises Active Directory.

## Step 6: Delete a staged migration batch

After all mailboxes in a migration batch have been successfully migrated, and you've converted the on-premises mailboxes in the batch to mail-enabled users, you're ready to delete a staged migration batch. Be sure to verify that mail is being forwarded to the Microsoft 365 mailboxes in the migration batch. When you delete a staged migration batch, the migration service cleans up any records related to the migration batch and deletes the migration batch.

To delete the "StagedBatch1" migration batch in Exchange Online PowerShell, run the following command.

```
PowerShell

Remove-MigrationBatch -Identity StagedBatch1
```

For more information about the **Remove-MigrationBatch** cmdlet, see[Remove-MigrationBatch](#).

## Verify it worked

Run the following command in Exchange Online PowerShell to display information about the "IMAPBatch1":

```
PowerShell

Get-MigrationBatch StagedBatch1
```

The command will return either the migration batch with a status of **Removing**, or it will return an error stating that migration batch couldn't be found, verifying that the batch was deleted.

For more information about the **Get-MigrationBatch** cmdlet, see [Get-MigrationBatch](#).

## Step7: Assign licenses to Microsoft 365 users

Activate Microsoft 365 user accounts for the migrated accounts by assigning licenses. If you don't assign a license, the mailbox is disabled when the grace period (30 days) ends. To assign a license in the Microsoft 365 admin center, see [Assign or unassign licenses](#).

## Step 8: Complete post-migration tasks

- **Create an Autodiscover DNS record so users can easily get to their mailboxes.**

After all on-premises mailboxes are migrated to Microsoft 365, you can configure an Autodiscover DNS record for your Microsoft 365 organization to enable users to easily connect to their new Microsoft 365 mailboxes with Outlook and mobile clients. This new Autodiscover DNS record has to use the same namespace that you're using for your Microsoft 365 organization. For example, if your cloud-based namespace is `cloud.contoso.com`, the Autodiscover DNS record you need to create is `autodiscover.cloud.contoso.com`.

Microsoft 365 uses a CNAME record to implement the Autodiscover service for Outlook and mobile clients. The Autodiscover CNAME record must contain the following information:

- **Alias:** autodiscover
- **Target:** `autodiscover.outlook.com`

For more information, see [Add DNS records to connect your domain](#).

- **Decommission on-premises Exchange servers.** After you've verified that all email is being routed directly to the Microsoft 365 mailboxes, and you no longer need to maintain your on-premises email organization or don't plan on implementing an SSO solution, you can uninstall Exchange from your servers and remove your on-premises Exchange organization.

### Note

Decommissioning Exchange can have unintended consequences. Before decommissioning your on-premises Exchange organization, we recommend that

you contact Microsoft Support.

For more information, see the following:

- [Modify or Remove Exchange 2010](#)
  - [How to Remove an Exchange 2007 Organization](#)
  - [How to Uninstall Exchange Server 2003](#)
- 

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# How to manage Microsoft 365 with Windows PowerShell for Delegated Access Permissions partners

Article • 08/23/2024

*This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.*

Delegated Access Permission (DAP) partners are Syndication and Cloud Solution Providers (CSP) Partners. Many are network or telecom providers. They bundle Microsoft 365 subscriptions into their service offerings. When they sell a Microsoft 365 subscription, they're automatically granted Administer On Behalf Of (AOBO) permissions to the customer's tenancies so they can administer and report on those tenancies. These tasks are difficult to do in the Microsoft 365 admin center. It's much easier to use PowerShell for Microsoft 365 to do administrative tasks such as:

- List all the customer **TenantIds** and their domains
- Identify all users in a customer tenancy and their assigned licenses

## ⓘ Note

Some administrative tasks can only be done in PowerShell.

The following articles show how Syndication and CSP partners use PowerShell to administer their customer tenancies:

- [Add a domain to a client tenancy with Windows PowerShell for Delegated Access Permission \(DAP\) partners](#)
- [Connect to Exchange Online PowerShell](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Add a domain to a client tenancy with Windows PowerShell for Delegated Access Permission (DAP) partners

Article • 04/08/2024

*This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.*

You can create and associate new domains with your customer's tenancy with PowerShell for Microsoft 365 faster than using the Microsoft 365 admin center.

Delegated Access Permission (DAP) partners are Syndication and Cloud Solution Providers (CSP) Partners. They're frequently network or telecom providers to other companies. They bundle Microsoft 365 subscriptions into their service offerings to their customers. When they sell a Microsoft 365 subscription, they're automatically granted Administer On Behalf Of (AOBO) permissions to the customer tenancies so they can administer and report on the customer tenancies.

## What do you need to know before you begin?

The procedures in this article require you to connect to [Connect to Microsoft 365 with PowerShell](#).

You also need your partner tenant administrator credentials.

You also need the following information:

- You need the fully qualified domain name (FQDN) that your customer wants.
- You need the customer's **TenantId**.
- The FQDN must be registered with an Internet domain name service (DNS) registrar, such as GoDaddy. For more information on how to publicly register a domain name, see [How to buy a domain name](#).
- You need to know how to add a TXT record to the registered DNS zone for your DNS registrar. For more information on how to add a TXT record, see [Add DNS records to connect your domain](#). If those procedures don't work for you, you'll need to find the procedures for your DNS registrar.

## Create domains

Your customers will likely ask you to create additional domains to associate with their tenancy because they don't want the default <domain>.onmicrosoft.com domain to be the primary one that represents their corporate identities to the world. This procedure walks you through creating a new domain associated with your customer's tenancy.

 **Note**

To perform some of these operations, the partner administrator account you sign in with must be set to **Full administration** for the **Assign administrative access to companies you support** setting found in the details of the admin account in the [Microsoft 365 admin center](#). For more information on managing partner administrator roles, see [Partners: Offer delegated administration](#).

## Create the domain in Microsoft Entra ID

This command creates the domain in Microsoft Entra ID but doesn't associate it with the publicly registered domain. That comes when you prove that you own the publicly registered domain to Microsoft 365 for enterprises.

 **Note**

The Azure Active Directory module is being replaced by the Microsoft Graph PowerShell SDK. You can use the Microsoft Graph PowerShell SDK to access all Microsoft Graph APIs. For more information, see [Get started with the Microsoft Graph PowerShell SDK](#).

First, use a **Microsoft Entra DC admin** or **Cloud Application Admin** account to [connect to your Microsoft 365 tenant](#).

Assigning and removing licenses for a user requires the **Domain.ReadWrite.All** permission scope or one of the other permissions listed in the '[Assign license](#)' Graph API reference page.

 **Note**

Azure AD and MSOnline PowerShell modules are deprecated as of March 30, 2024. To learn more, read the [deprecation update](#). After this date, support for these modules are limited to migration assistance to Microsoft Graph PowerShell SDK and security fixes. The deprecated modules will continue to function through March, 30 2025.

We recommend migrating to [Microsoft Graph PowerShell](#) to interact with Microsoft Entra ID (formerly Azure AD). For common migration questions, refer to the [Migration FAQ](#). Note: Versions 1.0.x of MSOnline may experience disruption after June 30, 2024.

PowerShell

```
Connect-MgGraph -Scopes "Domain.ReadWrite.All"
```

Run the following command to create a new domain:

PowerShell

```
New-MgDomain -Id <customer TenantId> -DomainNameReferences <FQDN of new domain>
```

## Get the data for the DNS TXT verification record

Microsoft 365 generates the specific data that you need to place into the DNS TXT verification record. To get the data, run this command.

PowerShell

```
Import-Module Microsoft.Graph.Identity.DirectoryManagement
(Get-MgDomainVerificationDnsRecord -DomainId <domain ID, i.e. contoso.com> |
Where-Object {$_ .RecordType -eq "Txt"}).AdditionalProperties.text
```

This command gives you output like:

```
MS=ms#####
```

### ⓘ Note

You will need this text to create the TXT record in the publicly registered DNS zone. Be sure to copy and save it.

## Add a TXT record to the publically registered DNS zone

Before Microsoft 365 will start accepting traffic that is directed to the publicly registered domain name, you must prove that you own and have administrator permissions to the domain. You prove you own the domain by creating a TXT record in the domain. A TXT

record doesn't do anything in your domain, and it can be deleted after your ownership of the domain is established. To create the TXT records, follow the procedures at [Add DNS records to connect your domain](#). If those procedures don't work for you, you need to find the procedures for your DNS registrar.

Confirm the successful creation of the TXT record via nslookup. Follow this syntax.

## Console

```
nslookup -type=TXT <FQDN of registered domain>
```

This command gives you output like:

Non-authoritative answer:

FQDN of the registered domain

text=MS=ms#####

# Validate domain ownership in Microsoft 365

In this last step, you validate to Microsoft 365 that you own the publically registered domain. After this step, Microsoft 365 will begin accepting traffic routed to the new domain name. To complete the domain creation and registration process, run this command.

## PowerShell

```
Confirm-MgDomain -DomainId <FQDN of new domain> -InputObject @{TenantId= <customer TenantId>}
```

This command doesn't return any output, so to confirm that the command worked, run this command

PowerShell

```
Get-MgDomain -DomainId <FQDN of new domain>
```

This will return something like this:

## Console

Id	AuthenticationType	AvailabilityStatus			
IsAdminManaged	IsDefault	IsInitial	IsRoot	IsVerified	Manufact

urer				
--	--	--	--	--
contoso.com		Managed		True
True	True	True	True	

## See also

[Help for partners](#) ↗

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

# Connect to Exchange Online PowerShell

Article • 08/21/2023

This article contains instructions for how to connect to Exchange Online PowerShell using the Exchange Online PowerShell module with or without multi-factor authentication (MFA).

The Exchange Online PowerShell module uses modern authentication for connecting to all Exchange-related PowerShell environments in Microsoft 365: Exchange Online PowerShell, Security & Compliance PowerShell, and standalone Exchange Online Protection (EOP) PowerShell. For more information about the Exchange Online PowerShell module, see [About the Exchange Online PowerShell module](#).

To connect to Exchange Online PowerShell for automation, see [App-only authentication for unattended scripts](#) and [Use Azure managed identities to connect to Exchange Online PowerShell](#).

To connect to Exchange Online PowerShell from C#, see [Use C# to connect to Exchange Online PowerShell](#).

## What do you need to know before you begin?

- The requirements for installing and using the module are described in [Install and maintain the Exchange Online PowerShell module](#).

### Note

Remote PowerShell connections are deprecated in Exchange Online PowerShell. For more information, see [Deprecation of Remote PowerShell in Exchange Online](#).

REST API connections in the Exchange Online PowerShell V3 module require the PowerShellGet and PackageManagement modules. For more information, see [PowerShellGet for REST-based connections in Windows](#).

- After you connect, the cmdlets and parameters that you have or don't have access to is controlled by role-based access control (RBAC). For more information, see [Permissions in Exchange Online](#).

To find the permissions that are required to run specific Exchange Online cmdlets, see [Find the permissions required to run any Exchange cmdlet](#).

## 💡 Tip

Having problems? Ask in the [Exchange Online](#) forum.

# Step 1: Load the Exchange Online PowerShell module

## ⓘ Note

If the module is already installed, you can typically skip this step and run `Connect-ExchangeOnline` without manually loading the module first.

After you've [installed the module](#), open a PowerShell window and load the module by running the following command:

```
PowerShell
```

```
Import-Module ExchangeOnlineManagement
```

# Step 2: Connect and authenticate

## ⓘ Note

Connect commands will likely fail if the profile path of the account that you used to connect contains special PowerShell characters (for example, `$`). The workaround is to connect using a different account that doesn't have special characters in the profile path.

The command that you need to run uses the following syntax:

```
PowerShell
```

```
Connect-ExchangeOnline -UserPrincipalName <UPN> [-ExchangeEnvironmentName <Value>] [-ShowBanner:$false] [-DelegatedOrganization <String>] [-SkipLoadingFormatData]
```

For detailed syntax and parameter information, see [Connect-ExchangeOnline](#).

- <UPN> is your account in user principal name format (for example, `navin@contoso.onmicrosoft.com`).
- With the EXO V3 module (v3.0.0 or later) and the [demise of Basic authentication \(remote PowerShell\) connections to Exchange Online](#), you're using REST API cmdlets only. For more information, see [REST API connections in the EXO V3 module](#).
- When you use the *ExchangeEnvironmentName* parameter, you don't need to use the *ConnectionUri* or *AzureADAuthorizationEndPointUrl* parameters. Common values for the *ExchangeEnvironmentName* parameter are described in the following table:

[+] [Expand table](#)

Environment	Value
Microsoft 365 or Microsoft 365 GCC	n/a*
Microsoft 365 GCC High	0365USGovGCCHigh
Microsoft 365 DoD	0365USGovDoD
Office 365 Germany	0365GermanyCloud
Office 365 operated by 21Vianet	0365China

\* The required value `0365Default` is also the default value, so you don't need to use the *ExchangeEnvironmentName* parameter in Microsoft 365 or Microsoft 365 GCC environments.

- The *DelegatedOrganization* parameter specifies the customer organization that you want to manage as an authorized Microsoft Partner. For more information, see the [connection examples later in this article](#).
- Depending on the nature of your organization, you might be able to omit the *UserPrincipalName* parameter in the connection command. Instead, you enter the username and password or select stored credentials after you run the **Connect-ExchangeOnline** command. If it doesn't work, then you need to use the *UserPrincipalName* parameter.
- If you aren't using MFA, you should be able to use the *Credential* parameter instead of the *UserPrincipalName* parameter. First, run the command `$Credential = Get-Credential`, enter your username and password, and then use the variable name for the *Credential* parameter (`-Credential $Credential`). If it doesn't work, then you need to use the *UserPrincipalName* parameter.

- Use the *SkipLoadingFormatData* switch to avoid errors when connecting to Exchange Online PowerShell from within a Windows service.
- Using the module in PowerShell 7 requires version 2.0.4 or later.

The connection examples in the following sections use modern authentication, and are incapable of using Basic authentication.

## Connect to Exchange Online PowerShell with an interactive login prompt

1. The following examples work in Windows PowerShell 5.1 and PowerShell 7 for accounts with or without MFA:

- This example connects to Exchange Online PowerShell in a Microsoft 365 or Microsoft 365 GCC organization:

```
PowerShell

Connect-ExchangeOnline -UserPrincipalName
navin@contoso.onmicrosoft.com
```

- This example connects to Exchange Online PowerShell in a Microsoft GCC High organization:

```
PowerShell

Connect-ExchangeOnline -UserPrincipalName
laura@blueyonderairlines.us -ExchangeEnvironmentName
0365USGovGCCHigh
```

- This example connects to Exchange Online PowerShell in a Microsoft 365 DoD organization:

```
PowerShell

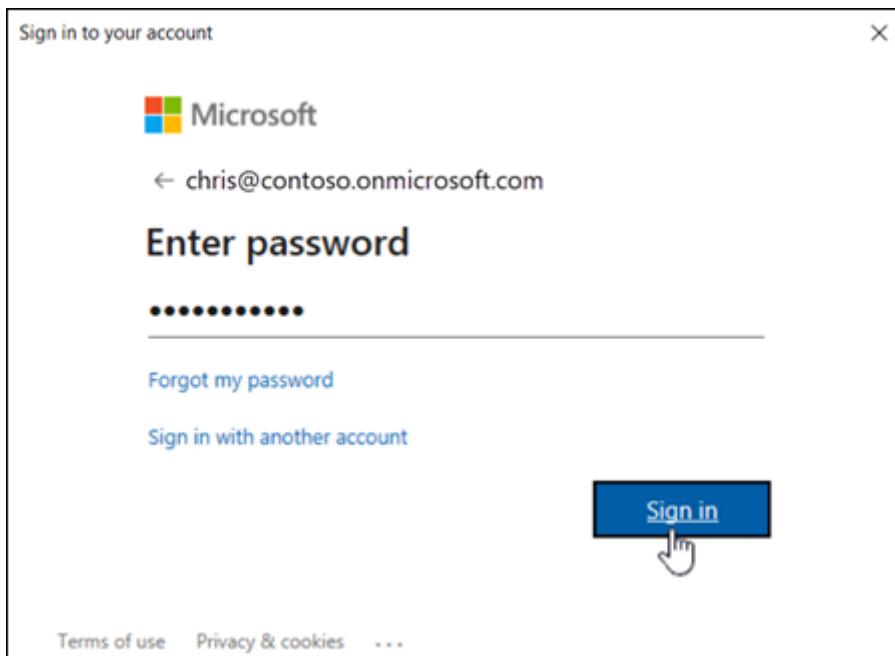
Connect-ExchangeOnline -UserPrincipalName julia@adatum.mil -
ExchangeEnvironmentName 0365USGovDoD
```

- This example connects to Exchange Online PowerShell in an Office 365 Germany organization:

```
PowerShell
```

```
Connect-ExchangeOnline -UserPrincipalName lukas@fabrikam.de -
ExchangeEnvironmentName 0365GermanyCloud
```

2. In the sign-in window that opens, enter your password, and then click **Sign in**.

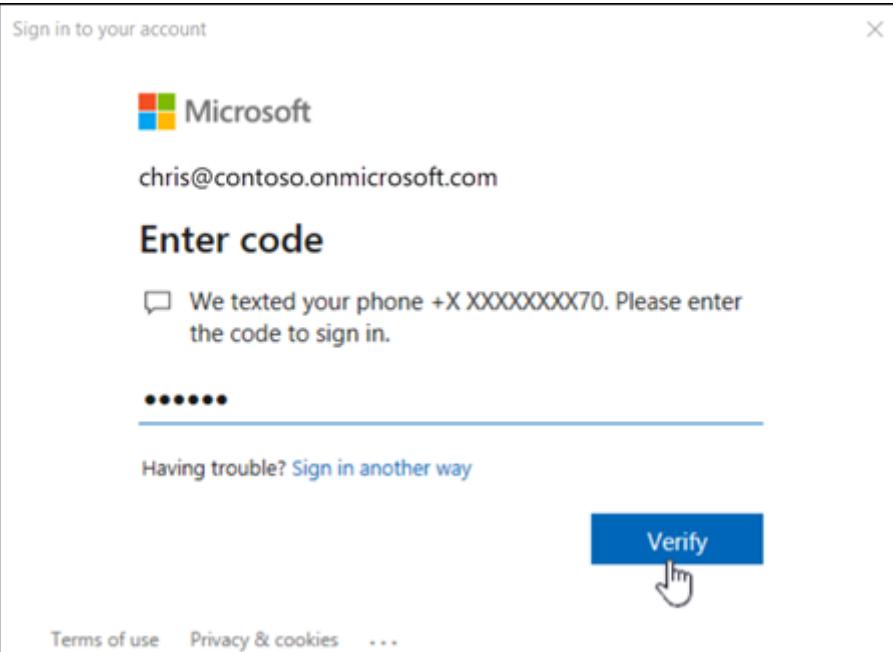


**① Note**

In PowerShell 7, browser-based single sign-on (SSO) is used by default, so the sign-in prompt opens in your default web browser instead of a standalone dialog.

3. **MFA only:** A verification code is generated and delivered based on the response option that's configured for your account (for example, a text message or the Microsoft Authenticator app on your device).

In the verification window that opens, enter the verification code, and then click **Verify**.



## PowerShell 7 exclusive connection methods

- In PowerShell 7 for accounts without MFA, this example prompts for credentials within the PowerShell window:

```
PowerShell

Connect-ExchangeOnline -UserPrincipalName navin@contoso.onmicrosoft.com
-InlineCredential
```

- In PowerShell 7 for accounts with or without MFA, this example uses another computer to authenticate and complete the connection. Typically, you use this method on computers that don't have web browsers (users are unable to enter their credentials in PowerShell 7):

1. Run the following command on the computer where you want to connect:

```
PowerShell

Connect-ExchangeOnline -Device
```

The connection command waits at following output:

To sign in, use a web browser to open the page  
<https://microsoft.com/devicelogin> and enter the code <XXXXXXXXXX> to authenticate.

Note the <XXXXXXXXXX> code value.

2. On any other device with a web browser and internet access, open <https://microsoft.com/devicelogin> and enter the <XXXXXXXXXX> code value from the previous step.
3. Enter your credentials on the resulting pages.
4. In the confirmation prompt, click **Continue**. The next message should indicate success, and you can close the browser or tab.
5. The command from step 1 continues to connect you to Exchange Online PowerShell.

## Connect to Exchange Online PowerShell without a login prompt (unattended scripts)

For complete instructions, see [App-only authentication for unattended scripts in Exchange Online PowerShell and Security & Compliance PowerShell](#).

## Connect to Exchange Online PowerShell in customer organizations

For more information about partners and customer organizations, see the following topics:

- [What is the Cloud Solution Provider \(CSP\) program?](#)
- [Introduction to granular delegated admin privileges \(GDAP\)](#)

This example connects to customer organizations in the following scenarios:

- Connect to a customer organization using a CSP account.
- Connect to a customer organization using a GDAP.
- Connect to a customer organization as a guest user.

PowerShell

```
Connect-ExchangeOnline -UserPrincipalName navin@contoso.onmicrosoft.com
-DelegatedOrganization adatum.onmicrosoft.com
```

## Connect to Exchange Online PowerShell using managed identity

For more information, see [Use Azure managed identities to connect to Exchange Online PowerShell](#).

- System-assigned managed identity:

```
PowerShell
```

```
Connect-ExchangeOnline -ManagedIdentity -Organization
"cohovinyard.onmicrosoft.com"
```

- User-assigned assigned managed identity:

```
PowerShell
```

```
Connect-ExchangeOnline -ManagedIdentity -Organization
"constoso.onmicrosoft.com" -ManagedIdentityAccountId
<ManagedIdentityAccountIdGuid>
```

## Step 3: Disconnect when you're finished

Be sure to disconnect the session when you're finished. If you close the PowerShell window without disconnecting the session, you could use up all the sessions available to you, and you need to wait for the sessions to expire. To disconnect the session, run the following command:

```
PowerShell
```

```
Disconnect-ExchangeOnline
```

To silently disconnect without a confirmation prompt, run the following command:

```
PowerShell
```

```
Disconnect-ExchangeOnline -Confirm:$false
```

### ⓘ Note

The disconnect command will likely fail if the profile path of the account that you used to connect contains special PowerShell characters (for example, `$`). The workaround is to connect using a different account that doesn't have special characters in the profile path.

# How do you know you've connected successfully?

If you don't receive any errors, you've connected successfully. A quick test is to run an Exchange Online PowerShell cmdlet, for example, **Get-AcceptedDomain**, and see the results.

If you receive errors, check the following requirements:

- A common problem is an incorrect password. Run the connection steps again and pay close attention to the username and password that you use.
- The account that you use to connect to must be enabled for PowerShell access. For more information, see [Enable or disable access to Exchange Online PowerShell](#).
- TCP port 80 traffic needs to be open between your local computer and Microsoft 365. It's probably open, but it's something to consider if your organization has a restrictive internet access policy.
- If your organization uses federated authentication, and your identity provider (IDP) and/or security token service (STS) isn't publicly available, you can't use a federated account to connect to Exchange Online PowerShell. Instead, create and use a non-federated account in Microsoft 365 to connect to Exchange Online PowerShell.
- REST-based connections to Exchange Online PowerShell require the `PowerShellGet` module, and by dependency, the `PackageManagement` module, so you'll receive errors if you try to connect without having them installed. For example, you might see the following error:

The term 'Update-ModuleManifest' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.

For more information about the `PowerShellGet` and `PackageManagement` module requirements, see [PowerShellGet for REST-based connections in Windows](#).

- After you connect, you might receive an error that looks like this:

Could not load file or assembly 'System.IdentityModel.Tokens.Jwt, Version= <Version>, Culture=neutral, PublicKeyToken=<TokenValue>'. Could not find or load a specific file.

This error happens when the Exchange Online PowerShell module conflicts with another module that's imported into the runspace. Try connecting in a new Windows PowerShell window before importing other modules.

## Appendix: Comparison of old and new connection methods

This section attempts to compare older connection methods that have been replaced by the Exchange Online PowerShell module. The Basic authentication and OAuth token procedures are included for historical reference only and are no longer supported.

### Connect without multi-factor authentication

- Exchange Online PowerShell module with interactive credential prompt:

```
PowerShell

Connect-ExchangeOnline -UserPrincipalName admin@contoso.onmicrosoft.com
```

- Exchange Online PowerShell module without interactive credential prompt:

```
PowerShell

$secpasswd = ConvertTo-SecureString '<Password>' -AsPlainText -Force

$o365cred = New-Object System.Management.Automation.PSCredential
("admin@contoso.onmicrosoft.com", $secpasswd)

Connect-ExchangeOnline -Credential $o365cred
```

- Basic authentication:

```
PowerShell

$secpasswd = ConvertTo-SecureString '<Password>' -AsPlainText -Force

$o365cred = New-Object System.Management.Automation.PSCredential
("admin@contoso.onmicrosoft.com", $secpasswd)

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/PowerShell-LiveID/ -
Credential $o365cred -Authentication Basic -AllowRedirection

Import-PSSession $Session
```

- New-PSSession with OAuth token:

```
PowerShell

$oauthTokenAsPassword = ConvertTo-SecureString '<EncodedOAuthToken>' -
AsPlainText -Force

$o365cred = New-Object System.Management.Automation.PSCredential
("admin@contoso.onmicrosoft.com", $oauthTokenAsPassword)

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/PowerShell-LiveID/?
BasicAuthToOAuthConversion=true -Credential $o365cred -Authentication
Basic -AllowRedirection

Import-PSSession $Session
```

## Connect with multi-factor authentication

- Exchange Online PowerShell module with interactive credential prompt:

```
PowerShell

Connect-ExchangeOnline -UserPrincipalName admin@contoso.onmicrosoft.com
```

- Basic authentication: Not available.
- New-PSSession with OAuth token: Not available.

## Connect to a customer organization with a CSP account

- Exchange Online PowerShell module:

```
PowerShell

Connect-ExchangeOnline -UserPrincipalName admin@contoso.onmicrosoft.com
-DelegatedOrganization delegated.onmicrosoft.com
```

- Basic authentication:

```
PowerShell

$secpasswd = ConvertTo-SecureString '<Password>' -AsPlainText -Force

$o365cred = New-Object System.Management.Automation.PSCredential
("admin@contoso.onmicrosoft.com", $secpasswd)
```

```

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/PowerShell-LiveID/?
DelegatedOrg=delegated.onmicrosoft.com&email=SystemMailbox{bb558c35-
97f1-4cb9-8ff7-d53741dc928c}@delegated.onmicrosoft.com -Credential
$o365cred -Authentication Basic -AllowRedirection

Import-PSSession $Session

```

- New-PSSession with OAuth token:

```

PowerShell

$oauthTokenAsPassword = ConvertTo-SecureString '<EncodedOAuthToken>' -
AsPlainText -Force

$o365cred = New-Object System.Management.Automation.PSCredential
("admin@contoso.onmicrosoft.com", $oauthTokenAsPassword)

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/PowerShell-LiveID/?
DelegatedOrg=delegated.onmicrosoft.com&BasicAuthToOAuthConversion=true&
email=SystemMailbox{bb558c35-97f1-4cb9-8ff7-
d53741dc928c}@delegated.onmicrosoft.com -Credential $o365cred -
Authentication Basic -AllowRedirection

Import-PSSession $Session

```

## Connect to a customer organization using GDAP

- Exchange Online PowerShell module:

```

PowerShell

Connect-ExchangeOnline -UserPrincipalName admin@contoso.onmicrosoft.com
-DelegatedOrganization delegated.onmicrosoft.com

```

- Basic authentication:

```

PowerShell

$secpasswd = ConvertTo-SecureString '<Password>' -AsPlainText -Force

$o365cred = New-Object System.Management.Automation.PSCredential
("admin@contoso.onmicrosoft.com", $secpasswd)

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/PowerShell-LiveID/?
DelegatedOrg=delegated.onmicrosoft.com&email=SystemMailbox{bb558c35-

```

```
97f1-4cb9-8ff7-d53741dc928c}@delegated.onmicrosoft.com -Credential
$o365cred -Authentication Basic -AllowRedirection
```

```
Import-PSSession $Session
```

- New-PSSession with OAuth token:

```
PowerShell
```

```
$oauthTokenAsPassword = ConvertTo-SecureString '<EncodedOAuthToken>' -
AsPlainText -Force

$o365cred = New-Object System.Management.Automation.PSCredential
("admin@contoso.onmicrosoft.com", $oauthTokenAsPassword)

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/PowerShell-LiveID/?
DelegatedOrg=delegated.onmicrosoft.com&BasicAuthToOAuthConversion=true&
email=SystemMailbox{bb558c35-97f1-4cb9-8ff7-
d53741dc928c}@delegated.onmicrosoft.com -Credential $o365cred -
Authentication Basic -AllowRedirection

Import-PSSession $Session
```

## Connect to a customer organization as a guest user

- Exchange Online PowerShell module:

```
PowerShell
```

```
Connect-ExchangeOnline -UserPrincipalName admin@contoso.onmicrosoft.com
-DelegatedOrganization delegated.onmicrosoft.com
```

- Basic authentication:

```
PowerShell
```

```
$secpasswd = ConvertTo-SecureString '<Password>' -AsPlainText -Force

$o365cred = New-Object System.Management.Automation.PSCredential
("admin@contoso.onmicrosoft.com", $secpasswd)

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/PowerShell-LiveID/?
DelegatedOrg=delegated.onmicrosoft.com&email=SystemMailbox{bb558c35-
97f1-4cb9-8ff7-d53741dc928c}@delegated.onmicrosoft.com -Credential
$o365cred -Authentication Basic -AllowRedirection
```

```
Import-PSSession $Session
```

- New-PSSession with OAuth token:

PowerShell

```
$oauthTokenAsPassword = ConvertTo-SecureString '<EncodedOAuthToken>' -
AsPlainText -Force

$o365cred = New-Object System.Management.Automation.PSCredential
("admin@contoso.onmicrosoft.com" , $oauthTokenAsPassword)

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/PowerShell-LiveID/?
DelegatedOrg=delegated.onmicrosoft.com&BasicAuthToOAuthConversion=true&
email=SystemMailbox{bb558c35-97f1-4cb9-8ff7-
d53741dc928c}@delegated.onmicrosoft.com -Credential $o365cred -
Authentication Basic -AllowRedirection

Import-PSSession $Session
```

## Connect to run unattended scripts

- Exchange Online PowerShell module:
  - Certificate thumbprint:

① Note

The CertificateThumbprint parameter is supported only in Microsoft Windows.

PowerShell

```
Connect-ExchangeOnline -CertificateThumbPrint
"012THISISADEMOTHUMBPRINT" -AppID "36ee4c6c-0812-40a2-b820-
b22ebd02bce3" -Organization "contoso.onmicrosoft.com"
```

- Certificate object:

PowerShell

```
Connect-ExchangeOnline -Certificate <%X509Certificate20bject%> -
AppID "36ee4c6c-0812-40a2-b820-b22ebd02bce3" -Organization
```

```
"contoso.onmicrosoft.com"
```

- Certificate file:

```
PowerShell
```

```
Connect-ExchangeOnline -CertificateFilePath
"C:\Users\navin\Desktop\automation-cert.pfx" -CertificatePassword
(ConvertTo-SecureString -String "<Password>" -AsPlainText -Force) -
AppID "36ee4c6c-0812-40a2-b820-b22ebd02bce3" -Organization
"contoso.onmicrosoft.com"
```

For more information, see [App-only authentication for unattended scripts in Exchange Online PowerShell and Security & Compliance PowerShell](#).

- Basic authentication:

```
PowerShell
```

```
$secpasswd = ConvertTo-SecureString '<Password>' -AsPlainText -Force

$o365cred = New-Object System.Management.Automation.PSCredential
("admin@contoso.onmicrosoft.com", $secpasswd)

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/PowerShell-LiveID/ -
Credential $o365cred -Authentication Basic -AllowRedirection

Import-PSSession $Session
```

- New-PSSession with OAuth token:

```
PowerShell
```

```
$oauthTokenAsPassword = ConvertTo-SecureString '<EncodedOAuthToken>' -
AsPlainText -Force

$o365cred = New-Object System.Management.Automation.PSCredential
("admin@contoso.onmicrosoft.com", $oauthTokenAsPassword)

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/PowerShell-LiveID/?
BasicAuthToOAuthConversion=true&email=SystemMailbox{bb558c35-97f1-4cb9-
8ff7-d53741dc928c}@contoso.onmicrosoft.com -Credential $o365cred -
Authentication Basic -AllowRedirection

Import-PSSession $Session
```

# Connect using managed identity

- Exchange Online PowerShell module:
  - System-assigned managed identity:

PowerShell

```
Connect-ExchangeOnline -ManagedIdentity -Organization
"contoso.onmicrosoft.com"
```

- User-assigned managed identity:

PowerShell

```
Connect-ExchangeOnline -ManagedIdentity -Organization
"contoso.onmicrosoft.com" -ManagedIdentityAccountId
<UserAssignedManagedIdentityPrincipalIdValue>
```

For more information, see [Use Azure managed identities to connect to Exchange Online PowerShell](#).

- Basic authentication: Not available.
- New-PSSession with OAuth token: Not available.

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Install Microsoft Teams PowerShell Module

Article • 06/05/2024 • Applies to: Microsoft Teams

This article explains how to install the Microsoft Teams PowerShell module using PowerShell Gallery.

## Requirements

Microsoft Teams PowerShell module requires Windows PowerShell 5.1 or PowerShell 7.2 or later on all platforms. Install the [latest version of PowerShell](#) available for your operating system.

To check your PowerShell version, run the following command from within a PowerShell session:

```
PowerShell
$PSVersionTable.PSVersion
```

We recommend that you use the `Install-Module` cmdlet to install the Microsoft Teams PowerShell module.

If PowerShell Gallery (PSGallery) isn't configured as a trusted repository for `PowerShellGet`, the first time you use the PSGallery you see the following message:

```
Console

Untrusted repository

You are installing the modules from an untrusted repository. If you trust
this repository, change
its InstallationPolicy value by running the `Set-PSRepository` cmdlet.

Are you sure you want to install the modules from 'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "N"):
```

Answer **Yes** or **Yes to All** to continue with the installation.

## Installing using the PowerShellGallery

Microsoft Teams PowerShell module is currently supported for use with Windows PowerShell 5.1 or PowerShell 7.2 or later. Follow these steps to install the module with Windows PowerShell 5.1 for example:

- Update to [Windows PowerShell 5.1](#). If you're on Windows 10 version 1607 or higher, you already have PowerShell 5.1 installed.
- Install [.NET Framework 4.7.2](#) or later.
- Run the following command to install the latest PowerShellGet:

```
PowerShell
```

```
Install-Module -Name PowerShellGet -Force -AllowClobber
```

- Install the Teams PowerShell Module.

```
PowerShell
```

```
Install-Module -Name MicrosoftTeams -Force -AllowClobber
```

## Offline Installation

In some environments, it's not possible to connect to the PowerShell Gallery. In those situations, follow these [manual installation steps](#).

## Sign in

To start working with Microsoft Teams PowerShell module, sign in with your Azure credentials.

```
PowerShell
```

```
Connect-MicrosoftTeams
```

## Update Teams PowerShell Module

To update any PowerShell module, you should use the same method used to install the module. For example, if you originally used `Install-Module`, then you should use [Update-Module](#) to get the latest version.

```
PowerShell
```

```
Update-Module MicrosoftTeams
```

### ⚠ Warning

If Teams PowerShell has already been imported into your PowerShell session, updating the module will fail. Close PowerShell and re-open a new elevated PowerShell session.

## Uninstall Teams PowerShell

To uninstall Microsoft Teams PowerShell, open a new PowerShell session and use the below method:

```
PowerShell
```

```
Uninstall-Module MicrosoftTeams

Uninstall all versions of the module
Uninstall-Module MicrosoftTeams -AllVersions
```

## Next Steps

Now you're ready to manage Microsoft Teams using Microsoft Teams PowerShell. See [Managing Teams with Teams PowerShell](#) to get started.

## Related topics

[Managing Teams with Teams PowerShell](#)

[Teams PowerShell Release Notes](#)

[Microsoft Teams cmdlet reference](#)

---

## Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

# Use the Centralized Deployment PowerShell cmdlets to manage add-ins

Article • 04/05/2024

As a Microsoft 365 user admin, you can deploy Office Add-ins to users via the Centralized Deployment feature (see [Deploy Office Add-ins in the admin center](#)). In addition to deploying Office Add-ins via the Microsoft 365 admin center, you can also use Microsoft PowerShell. Install the [O365 Centralized Add-In Deployment Module for Windows PowerShell](#).

After you download the module, open a regular Windows PowerShell window and run the following cmdlet:

PowerShell

```
Import-Module -Name O365CentralizedAddInDeployment
```

## Connect using your admin credentials

Before you can use the Centralized Deployment cmdlets, you need to sign in.

1. Start PowerShell.
2. Connect to PowerShell by using your **User Admin** credentials. Run the following cmdlet.

PowerShell

```
Connect-OrganizationAddInService
```

3. In the sign in prompt that opens, select or enter your Microsoft 365 **User Admin** credentials.

 **Note**

For more information about using PowerShell, see [Connect to Microsoft 365 with PowerShell](#).

## Upload an add-in manifest

Run the **New-OrganizationAddIn** cmdlet to upload an add-in manifest from a path, which can be either a file location or URL. The following example shows a file location for the value of the *ManifestPath* parameter.

PowerShell

```
New-OrganizationAddIn -ManifestPath 'C:\Users\Me\Desktop\taskpane.xml' -
Locale 'en-US'
```

You can also run the **New-OrganizationAddIn** cmdlet to upload an add-in and assign it to users or groups directly by using the *Members* parameter, as shown in the following example. Separate the email addresses of members with a comma.

PowerShell

```
New-OrganizationAddIn -ManifestPath 'C:\Users\Me\Desktop\taskpane.xml' -
Locale 'en-US' -Members 'KathyBonner@contoso.com',
'MaxHargrave@contoso.com'
```

## Upload an add-in from the Office Store

Run the **New-OrganizationAddIn** cmdlet to upload a manifest from the Office Store.

In the following example, the **New-OrganizationAddIn** cmdlet specifies the *AssetId* for an add-in for a United States location and content market.

PowerShell

```
New-OrganizationAddIn -AssetId 'WA104099688' -Locale 'en-US' -ContentMarket
'en-US'
```

To determine the value for the *AssetId* parameter, you can copy it from the URL of the Office Store webpage for the add-in. AssetIds always begin with "WA" followed by a number. For example, in the previous example, the source for the AssetId value of WA104099688 is the Office Store webpage URL for the add-in:

<https://store.office.com/en-001/app.aspx?assetid=WA104099688>.

The values for the *Locale* parameter and the *ContentMarket* parameter are identical and indicate the country/region you're trying to install the add-in from. The format is en-US, fr-FR and so forth.

 Note

Add-ins uploaded from the Office Store will update automatically within a few days of the latest update being available on the Office Store.

## Get details of an add-in

Run the **Get-OrganizationAddIn** cmdlet as shown below to get details of all add-ins uploaded to the tenant, included an add-in's product ID.

PowerShell

```
Get-OrganizationAddIn
```

Run the **Get-OrganizationAddIn** cmdlet with a value for the *ProductId* parameter to specify which add-in you want to retrieve details for.

PowerShell

```
Get-OrganizationAddIn -ProductId 6a75788e-1c6b-4e9b-b5db-5975a2072122
```

To get full details of all the add-ins plus the assigned users and groups, pipe the output of the **Get-OrganizationAddIn** cmdlet to the **Format-List** cmdlet, as shown in the following example.

PowerShell

```
foreach($G in (Get-OrganizationAddIn)){Get-OrganizationAddIn -ProductId
$G.ProductId | Format-List}
```

## Turn on or turn off an add-in

To turn off an add-in so users and groups that are assigned to it will no longer have access, run the **Set-OrganizationAddIn** cmdlet with the *ProductId* parameter and the *Enabled* parameter set to `$false`, as shown in the following example.

PowerShell

```
Set-OrganizationAddIn -ProductId 6a75788e-1c6b-4e9b-b5db-5975a2072122 -
Enabled $false
```

To turn an add-in back on, run the same cmdlet with the *Enabled* parameter set to `$true`.

PowerShell

```
Set-OrganizationAddIn -ProductId 6a75788e-1c6b-4e9b-b5db-5975a2072122 -
Enabled $true
```

## Add or remove users from an add-in

To add users and groups to a specific add-in, run the **Set-OrganizationAddInAssignments** cmdlet with the *ProductId*, *Add*, and *Members* parameters. Separate the email addresses of members with a comma.

PowerShell

```
Set-OrganizationAddInAssignments -ProductId 6a75788e-1c6b-4e9b-b5db-
5975a2072122 -Add -Members 'KathyBonner@contoso.com','sales@contoso.com'
```

To remove users and groups, run the same cmdlet using the *Remove* parameter.

PowerShell

```
Set-OrganizationAddInAssignments -ProductId 6a75788e-1c6b-4e9b-b5db-
5975a2072122 -Remove -Members 'KathyBonner@contoso.com','sales@contoso.com'
```

To assign an add-in to all users on the tenant, run the same cmdlet using the *AssignToEveryone* parameter with the value set to `$true`.

PowerShell

```
Set-OrganizationAddInAssignments -ProductId 6a75788e-1c6b-4e9b-b5db-
5975a2072122 -AssignToEveryone $true
```

To not assign an add-in to everyone and revert to the previously assigned users and groups, you can run the same cmdlet and turn off the *AssignToEveryone* parameter by setting its value to `$false`.

PowerShell

```
Set-OrganizationAddInAssignments -ProductId 6a75788e-1c6b-4e9b-b5db-
5975a2072122 -AssignToEveryone $false
```

## Update an add-in

To update an add-in from a manifest, run the **Set-OrganizationAddIn** cmdlet with the *ProductId*, *ManifestPath*, and *Locale* parameters, as shown in the following example.

PowerShell

```
Set-OrganizationAddIn -ProductId 6a75788e-1c6b-4e9b-b5db-5975a2072122 -
ManifestPath 'C:\Users\Me\Desktop\taskpane.xml' -Locale 'en-US'
```

ⓘ Note

Add-ins uploaded from the Office Store will update automatically within a few days of the latest update being available on the Office Store.

## Delete an add-in

To delete an add-in, run the **Remove-OrganizationAddIn** cmdlet with the *ProductId* parameter, as shown in the following example.

PowerShell

```
Remove-OrganizationAddIn -ProductId 6a75788e-1c6b-4e9b-b5db-5975a2072122
```

## Get detailed help for each cmdlet

You can look at detailed help for each cmdlet by using the **Get-help** cmdlet. For example, the following cmdlet provides detailed information about the **Remove-OrganizationAddIn** cmdlet.

PowerShell

```
Get-help Remove-OrganizationAddIn -Full
```

## Feedback

Was this page helpful?

👍 Yes

👎 No

[Provide product feedback ↗](#)

# Windows and Office 365 deployment lab kit

Article • 08/13/2024

The deployment lab kits for Windows and Office 365 can help you plan, test, and validate your deployment and management of desktops. The labs in the kit include Windows 11 Enterprise, Microsoft 365 Apps, and use of Microsoft Intune and Microsoft Configuration Manager. This kit is highly recommended for organizations preparing for desktop upgrades. As an isolated environment, the lab is also ideal for exploring deployment tool updates and testing your deployment-related automation.

The following lab kits are available for free download:

[Windows 11 lab ↗](#)

## A complete lab environment

The lab provides you with an automatically provisioned virtual lab environment. It includes domain-joined desktop clients, a domain controller, an internet gateway, and a fully configured Configuration Manager instance.

The labs include evaluation versions of the following products:

[+] Expand table

Windows 11 lab
Windows 11 Enterprise, version 23H2
Microsoft Configuration Manager, version 2303
Windows Assessment and Deployment Kit for Windows 11
Windows Server 2022

The labs are designed for you to connect them to trials for the following services:

- Microsoft 365 E5
- Microsoft 365 Apps for enterprise
- Office 365 E5 with Enterprise Mobility + Security (EMS)

## Step-by-step labs

Detailed lab guides take you through multiple deployment and management scenarios. The labs support the latest releases of Intune, Configuration Manager, and Windows 11.

The following sections describe the scenarios supported by the lab guides.

## Plan and prepare infrastructure

- Cloud management gateway
- Tenant attach and co-management
- Endpoint analytics
- Optimize update delivery

## Deploy Windows

- OS deployment task sequences in Configuration Manager
- Windows Autopilot

## Service Windows

- Servicing Windows using group policy
- Servicing Windows using Microsoft Intune
- Servicing Windows with Configuration Manager

## Manage Windows

- Device management for Windows 11 using Microsoft Intune
- Dynamic management with Windows 11
- Deploying Windows apps (Win32) with Intune
- Remote help

## Deploy Microsoft 365 Apps for enterprise

- Cloud managed deployment
- Locally managed deployment
- Microsoft 365 Apps deployment on non-Active Directory-joined devices
- Enterprise managed deployment using Configuration Manager
- Enterprise managed deployment using Microsoft Intune
- Servicing Microsoft 365 Apps for enterprise using Configuration Manager
- Servicing Microsoft 365 Apps for enterprise using Intune

- Line of business (LOB) application deployment and management with Microsoft Intune
- Deploy Microsoft Teams
- Assignment filters

## Managing Microsoft Edge

- Deploy and update Microsoft Edge
- Internet Explorer (IE) mode
- Setup enterprise new tab page

## Security and Compliance

- BitLocker
- Microsoft Defender Antivirus
- Windows Hello for Business
- Credential Guard
- Microsoft Defender Application Guard
- Windows Defender Exploit Guard
- Windows Defender Application Control
- Microsoft Defender for Endpoint

### Note

Please use a broadband internet connection to download this content and allow approximately 30 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 and 300 GB of free space is recommended. The Windows client virtual machines expire 90 days after activation of the lab. New versions of the labs will be published on or before October 30, 2024. For support with this lab, email the lab support alias

[winlab\\_help@microsoft.com](mailto:winlab_help@microsoft.com).

## More guidance

- [Windows client deployment resources and documentation](#)
- [Desktop Deployment series videos from Microsoft Mechanics ↗](#)
- [Microsoft Configuration Manager OS Deployment](#)
- [Deployment guide for Microsoft 365 Apps](#)

- [Getting Started with Intune](#)

## Related resources

- [Introducing Microsoft 365 ↗](#)
  - [Microsoft 365 for business ↗](#)
  - [Introducing Enterprise Mobility + Security ↗](#)
  - [Windows for business ↗](#)
- 

## Feedback

Was this page helpful?



[Provide product feedback ↗](#)

# Microsoft 365 for enterprise for the Contoso Corporation

Article • 04/12/2024

Microsoft 365 for enterprise is the Microsoft premier cloud offering that combines local and cloud-based productivity apps and services with Windows 10 Enterprise and advanced security features. It's a complete, intelligent solution that enables everyone to work together creatively and securely.

Contoso Corporation is a fictional but representative global manufacturing conglomerate with its headquarters in Paris. The company deployed Microsoft 365 for enterprise and addressed major design decisions and implementation details for networking, identity, Windows 10 Enterprise, Microsoft 365 Apps for enterprise, mobile device management, information protection, and security.

The company's overall goal for Microsoft 365 for enterprise is to accelerate its 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 manufacturing, sales, and support organization with more than 100,000 products.

- [Contoso IT infrastructure and needs](#)

Contoso is transitioning from an on-premises, centralized IT infrastructure to a cloud-inclusive setup that incorporates cloud-based personal productivity workloads, applications, and hybrid scenarios.

- [Networking](#)

Contoso network engineers optimized traffic for their on-premises users to their intranet edge and to the closest Microsoft network location on the internet.

- [Identity](#)

The Contoso identity-in-the-cloud solution leverages the company's on-premises Active Directory Domain Services (AD DS) forest. It includes federated authentication with their existing trusted, third-party identity providers.

- [Windows 10 Enterprise](#)

The Contoso infrastructure for Windows 10 Enterprise deploys and automatically installs updates for devices that are running the company's primary PC and device operating system.

- [Microsoft 365 Apps for enterprise](#)

The Contoso infrastructure for Microsoft 365 Apps for enterprise deploys and automatically installs updates for the Microsoft Office suite of productivity software.

- [Mobile device management](#)

With many roaming employees who have both company and personal smart phones and tablets, Contoso uses mobile device management to enroll and secure devices and their data and manage apps.

- [Information protection](#)

To ensure that both common and high-value data are identified, labeled, and subject to layers of security, Contoso enforces its data-security policies with Microsoft 365 for enterprise information protection.

- [Summary of Microsoft 365 for enterprise security](#)

Contoso uses the full spectrum of Microsoft 365 for enterprise security features for identity and access management, threat protection, information protection, and security management.

See these additional IT scenarios and configurations:

- [COVID-19 response and infrastructure for remote and onsite work](#)

Learn how Contoso updated their remote access capability and their new installs and updates infrastructure for remote and onsite workers.

- [Team for a top-secret project](#)

To create a secure collaboration environment for a top-secret project, Contoso used a team with security isolation.

- [Teams voice migration](#)

Learn how Contoso migrated their on-premises users to Microsoft Teams for unified communication, collaboration, and voice.

- Communication compliance offensive language policy

Learn how Contoso quickly configured an offensive language policy for Microsoft Teams, Exchange, and Viva Engage communications.

## Next step

Learn [about the Contoso Corporation](#) and the design considerations that were addressed when they deployed Microsoft 365 for enterprise.

## See also

[Microsoft 365 for enterprise overview](#)

[Test lab guides](#)

---

## Feedback

Was this page helpful?



[Provide product feedback](#) ↗

# Overview of Contoso Corporation

Article • 12/19/2023

The Contoso Corporation is a multinational business with its headquarters in Paris. The company is a manufacturing, sales, and support organization with more than 100,000 products.

## Contoso around the world

Figure 1 shows the headquarters office in Paris and regional hub and satellite offices on various continents.



Figure 1: Contoso offices around the world

Contoso has three tiers of offices:

- Headquarters

Contoso headquarters is a corporate campus on the outskirts of Paris with dozens of buildings for administrative, engineering, and manufacturing facilities. All the Contoso datacenters and its internet presence are housed in the Paris headquarters.

The headquarters has 25,000 workers.

- Regional hubs

Hub offices serve a specific region of the world with 60-percent sales and support staff. Each regional hub is connected to the Paris headquarters through a high-

bandwidth WAN link.

The regional hubs have an average of 2,000 workers.

- Satellite offices

Satellite offices contain 80-percent sales and support staff. They provide an on-site presence for Contoso customers in key cities or subregions. Each satellite office is connected to a regional hub through a high-bandwidth WAN link.

The satellite offices have an average of 250 workers.

About 25 percent of the Contoso workforce is mobile-only. The regional hubs and satellite offices have a higher percentage of these workers. Providing better support for mobile-only workers is an important business goal for Contoso.

## Design considerations for Microsoft 365 for enterprise

The Contoso IT architects identified the following design-requirement factors for deploying Microsoft 365 for 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 Microsoft Endpoint Configuration Manager infrastructure
- A mix of client computing devices that run 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 other confidential personal information to manage and secure
- 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 [on-premises IT infrastructure](#) and how the company's business needs are addressed with Microsoft 365 for enterprise.

## See also

[Microsoft 365 for enterprise overview](#)

[Test lab guides](#)

---

## Feedback

Was this page helpful?



[Provide product feedback ↗](#)

# Contoso IT infrastructure and business needs

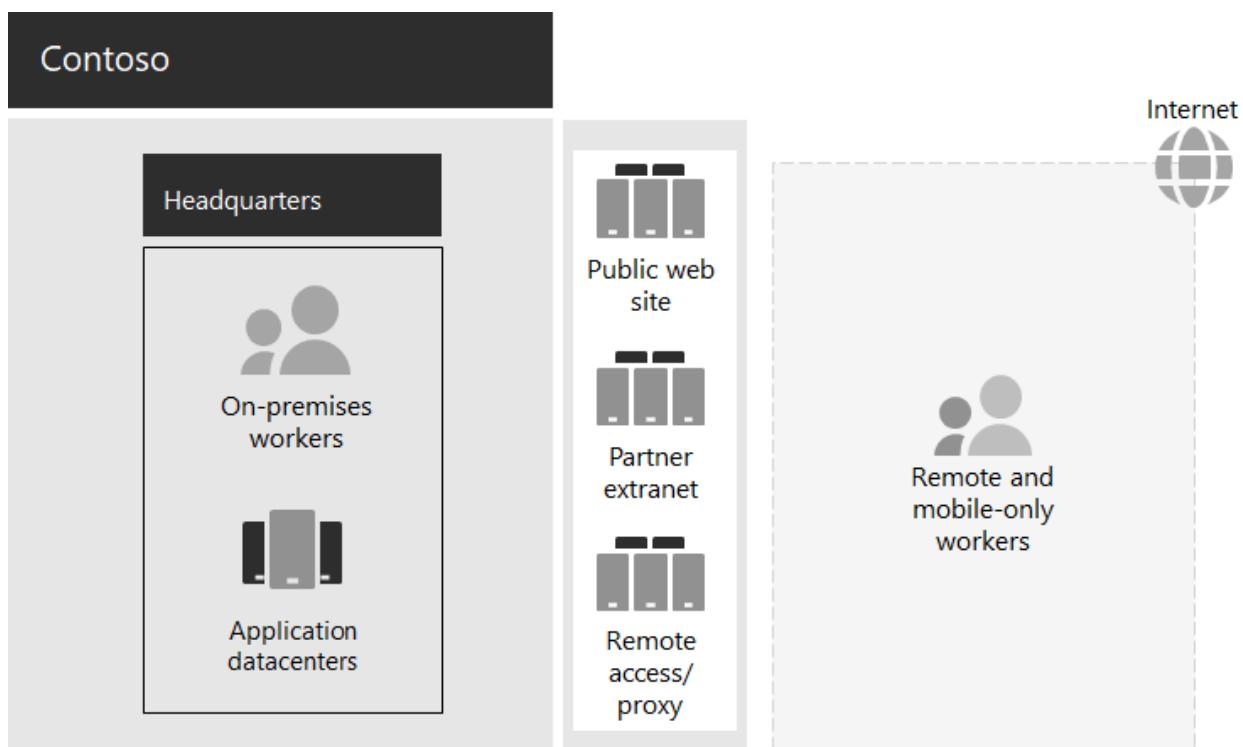
Article • 05/17/2024

Contoso is transitioning from an on-premises, centralized IT infrastructure to a cloud-inclusive setup that incorporates cloud-based personal productivity workloads and applications.

## Existing Contoso IT infrastructure

Contoso uses a mostly centralized on-premises IT infrastructure, with application datacenters in the Paris headquarters.

Here's the headquarters office with application datacenters, a DMZ, and the internet.



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 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 the Contoso headquarters DMZ, different sets of servers provide:

- Hosting for the Contoso public web site, from which customers can order products, parts, supplies, and service.
- Hosting for the Contoso partner extranet for partner communication and collaboration.
- Virtual private network (VPN)-based remote access to the Contoso intranet and web proxying for workers in the Paris headquarters.

## Contoso business needs

Contoso business needs fall into five main categories:

### Productivity

- Make collaboration easier

Replace 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 home 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 multifactor 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 and manufacturing specifications, and employee information.

- Security management

Monitor security posture and detect and respond to threats in real time.

## Remote and mobile access and business partners

- Improve security for remote and mobile workers

Implement 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 commonly accessed resources to the cloud.

- Provide better connectivity and lower overhead for business-to-business (B2B) transactions

Replace an aging and expensive partner extranet with a cloud-based solution that uses federated authentication.

## Compliance

- Adhere to regional regulatory requirements

Ensure compliance 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 IT overhead for managing software running on client PCs and devices

Automate installation of updates to the Windows operating system and Microsoft 365 Apps for enterprise across the organization.

# Mapping Contoso business needs to Microsoft 365 for enterprise

The Contoso IT department determined the following mapping of business needs to Microsoft 365 E5 features prior to deployment:

[+] Expand table

Category	Business need	Microsoft 365 for enterprise products or features
Productivity		
	Make collaboration easier	Microsoft Teams, SharePoint, OneDrive
	Improve productivity for remote and mobile workers	Microsoft 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 Microsoft Entra multifactor authentication (MFA) and Microsoft Entra Privileged Identity Management (PIM) MFA for all user accounts Conditional Access Security Reader Windows Hello Windows Credential Guard
	Threat protection	Advanced Threat Analytics Windows Defender Defender for Office 365 Microsoft Defender for Office 365 Microsoft 365 threat investigation and response
	Information protection	Azure Information Protection Data Loss Prevention (DLP) Windows Information Protection (WIP)

<b>Category</b>	<b>Business need</b>	<b>Microsoft 365 for enterprise products or features</b>
		Microsoft Defender for Cloud Apps Microsoft Intune
	Security management	Microsoft Defender for Cloud 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	Microsoft 365 workloads and cloud-based data
	Improve connectivity and lower overhead for B2B transactions	Federated authentication and cloud-based resources
Compliance		
	Adhere to regional regulatory requirements	GDPR features in Microsoft 365
Management		
	Lower IT overhead for installing client updates	Windows 10 Enterprise updates Microsoft 365 Apps for enterprise updates

## Next step

Learn about the Contoso Corporation [on-premises network](#) and how it was optimized for access and latency to Microsoft 365 cloud-based resources.

## See also

[Microsoft 365 for enterprise overview](#)

[Test lab guides](#)

# Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Networking for the Contoso Corporation

Article • 07/29/2024

To adopt a cloud-inclusive infrastructure, Contoso devised a fundamental shift in how network traffic to cloud services travels. Instead of an internal hub-and-spoke model that focuses network connectivity and traffic for the next level of the office hierarchy, they mapped user locations to local internet egress and local connections to the closest Microsoft 365 network location on the internet.

## Networking infrastructure

These are the network elements that link Contoso offices across the globe:

- Multiprotocol Label Switching (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. The network enables users to access on-premises servers that make up line-of-business applications in the Paris headquarters. 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 wired hosts or wireless access points on subnets, which use the private IP address space.

- Local direct internet access for Microsoft 365 traffic

Each office has a software-defined WAN (SD-WAN) device that has one or 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 a local DNS 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 the Contoso networking infrastructure and its connections to the internet.

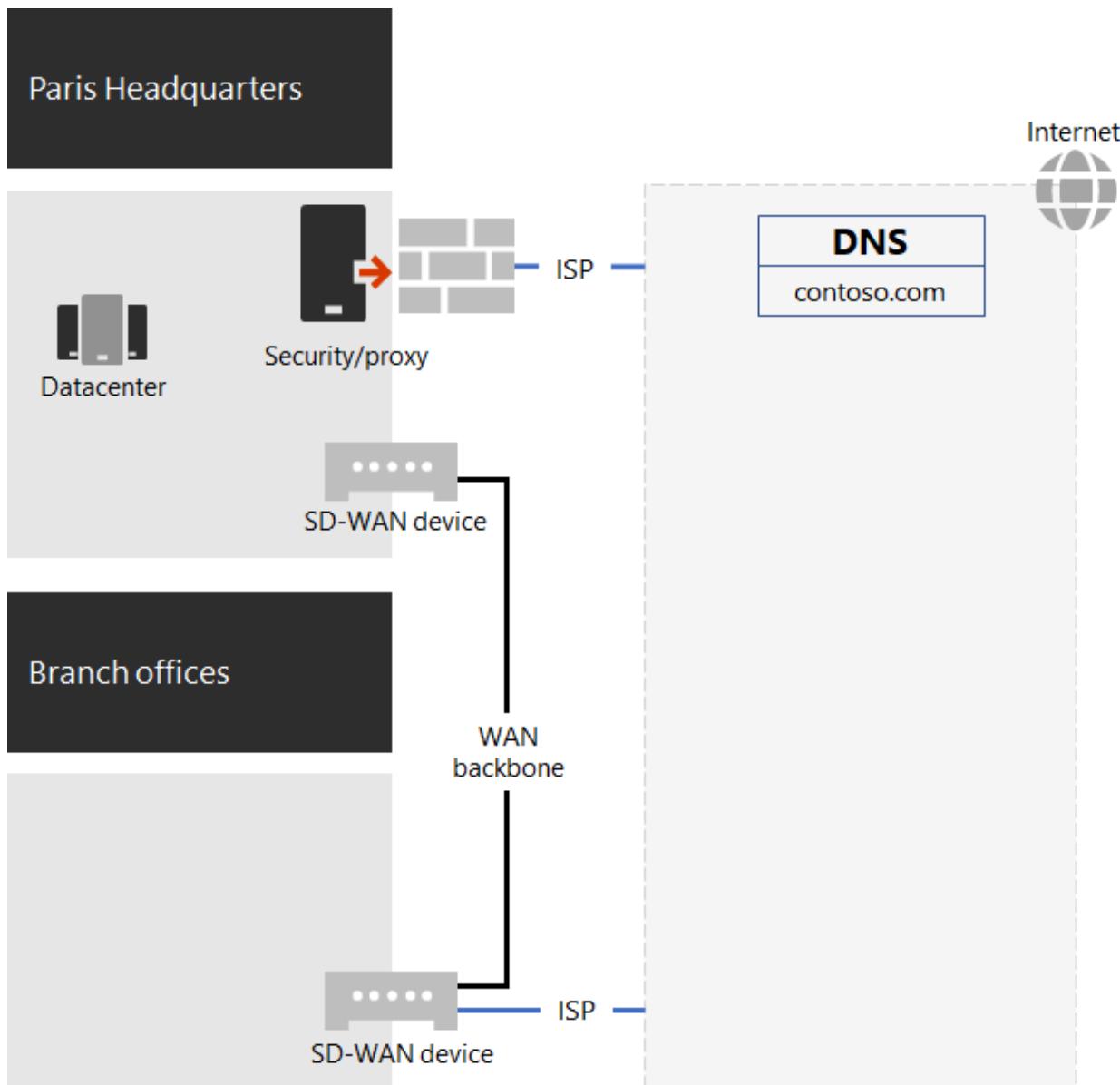


Figure 1: The Contoso network

## Use of SD-WAN for optimal network connectivity to Microsoft

Contoso followed [Microsoft 365 network connectivity principles](#) to:

- Identify and differentiate Microsoft 365 network traffic
- Egress network connections locally
- Avoid network hairpins
- Bypass duplicate network security devices

There are three categories of network traffic for Microsoft 365: *Optimize*, *Allow*, and *Default*. Optimize and Allow traffic is trusted network traffic that's encrypted and secured at the endpoints and is destined for the Microsoft 365 network.

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.
- Deploy SD-WAN devices at each office 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. Another connects to a local ISP circuit. The SD-WAN device routes Optimize and Allow category network traffic over the ISP link.

## The Contoso line-of-business app infrastructure

Contoso architected its line-of-business application and server intranet 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 datacenters contain centralized application servers that serve the entire organization.

Figure 2 shows the percentage of network traffic capacity used when accessing servers across the Contoso intranet.

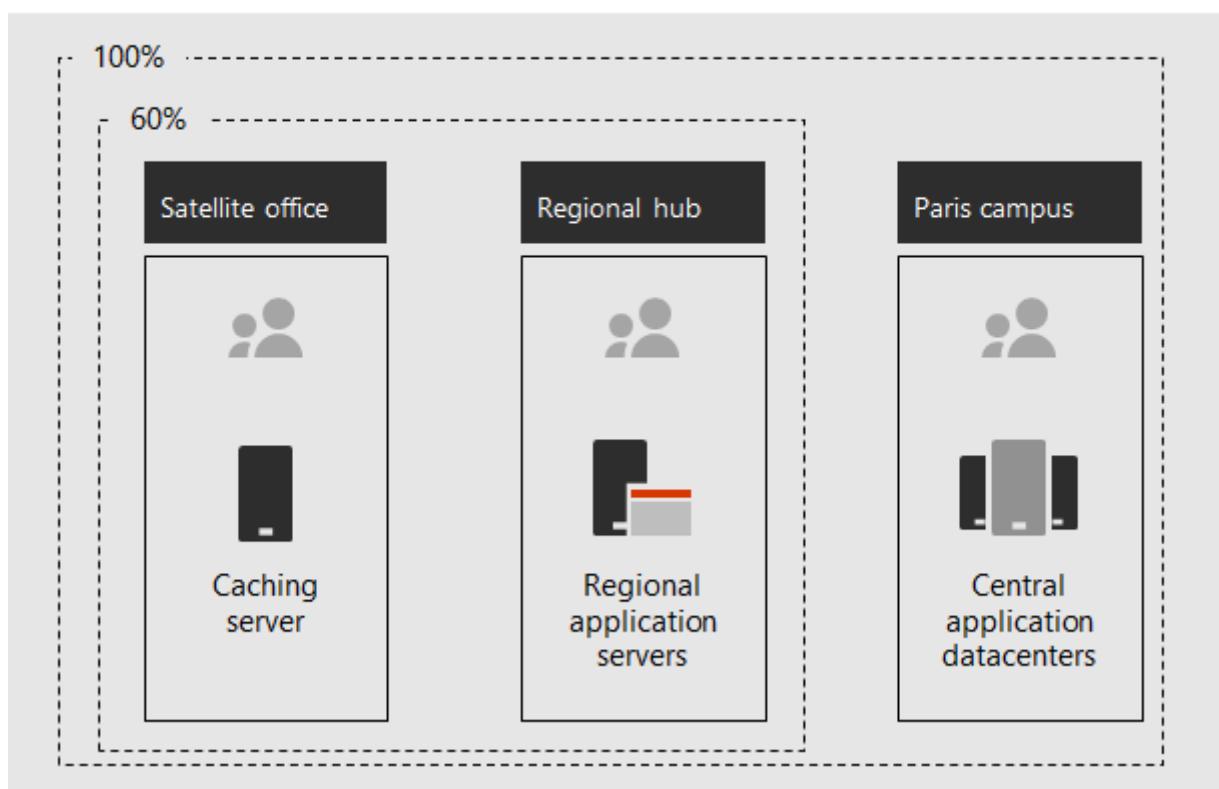


Figure 2: The Contoso infrastructure for internal applications

For the satellite or regional hub offices, 60 percent of the resources needed by employees can be served by satellite and regional hub office servers. The additional 40 percent of resource requests must go over the WAN link to the Paris campus.

## Network analysis and preparation for Microsoft 365 for enterprise

Successful adoption of Microsoft 365 for enterprise services by Contoso users depends on highly available and performant connectivity to the internet or directly to Microsoft cloud services. Contoso took these steps to plan and implement optimized connectivity to Microsoft 365 for enterprise cloud services:

1. Create a company WAN network diagram to aid with planning

To start their network planning, Contoso created a diagram showing their office locations, existing network connectivity, 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. Create a plan for Microsoft 365 for enterprise network connectivity

Contoso used the [Microsoft 365 network connectivity principles](#) and sample reference network architectures to identify SD-WAN as their preferred topology for Microsoft 365 connectivity.

## 3. Analyze internet-connection utilization and MPLS-WAN bandwidth at each office, and increase bandwidth as needed

Each office's current usage was analyzed, and circuits were increased so that predicted Microsoft 365 cloud-based traffic would operate with an average of 20-percent unused capacity.

## 4. Optimize 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 were configured into the SD-WAN devices for routing over the ISP circuit.

## 5. Configure internal DNS

DNS is required to be functional and to be looked up locally for Microsoft 365 traffic.

## 6. Validate network endpoint and port connectivity

Contoso ran Microsoft network connectivity test tools to validate connectivity for Microsoft 365 for enterprise cloud services.

## 7. Optimize employee computers for network connectivity

Individual computers were checked to ensure that the latest operating system updates were installed and that endpoint security monitoring was active on all clients.

# Next step

Learn how Contoso is [leveraging its on-premises Active Directory Domain Services in the cloud](#) for employees and federating authentication for customers and business partners.

# See also

[Networking roadmap for Microsoft 365](#)

[Microsoft 365 for enterprise overview](#)

[Test lab guides](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Identity for the Contoso Corporation

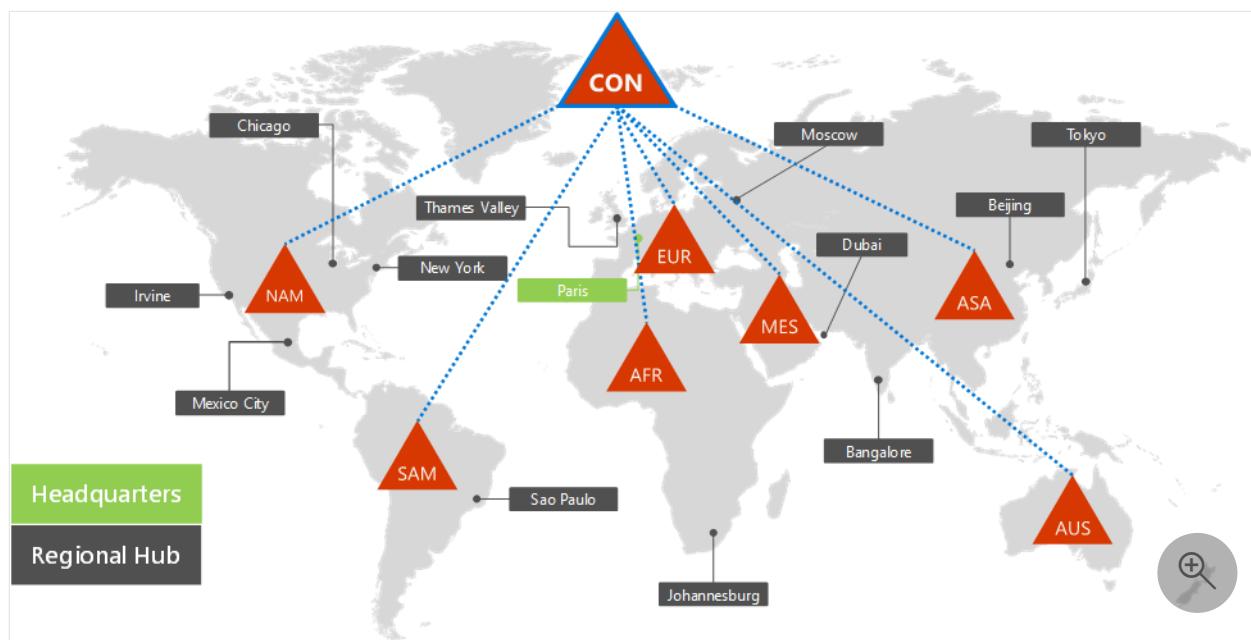
Article • 07/01/2024

Microsoft provides Identity as a Service (IDaaS) across its cloud offerings through Microsoft Entra ID. To adopt Microsoft 365 for enterprise, the Contoso IDaaS solution had to use their on-premises identity provider and include federated authentication with their existing trusted, third-party identity providers.

## The Contoso Active Directory Domain Services forest

Contoso uses a single Active Directory Domain Services (AD DS) forest for contoso.com with seven subdomains, one for each region of the world. The headquarters, regional hub offices, and satellite offices contain domain controllers for local authentication and authorization.

Here's the Contoso forest with regional domains for the different parts of the world that contain regional hubs.



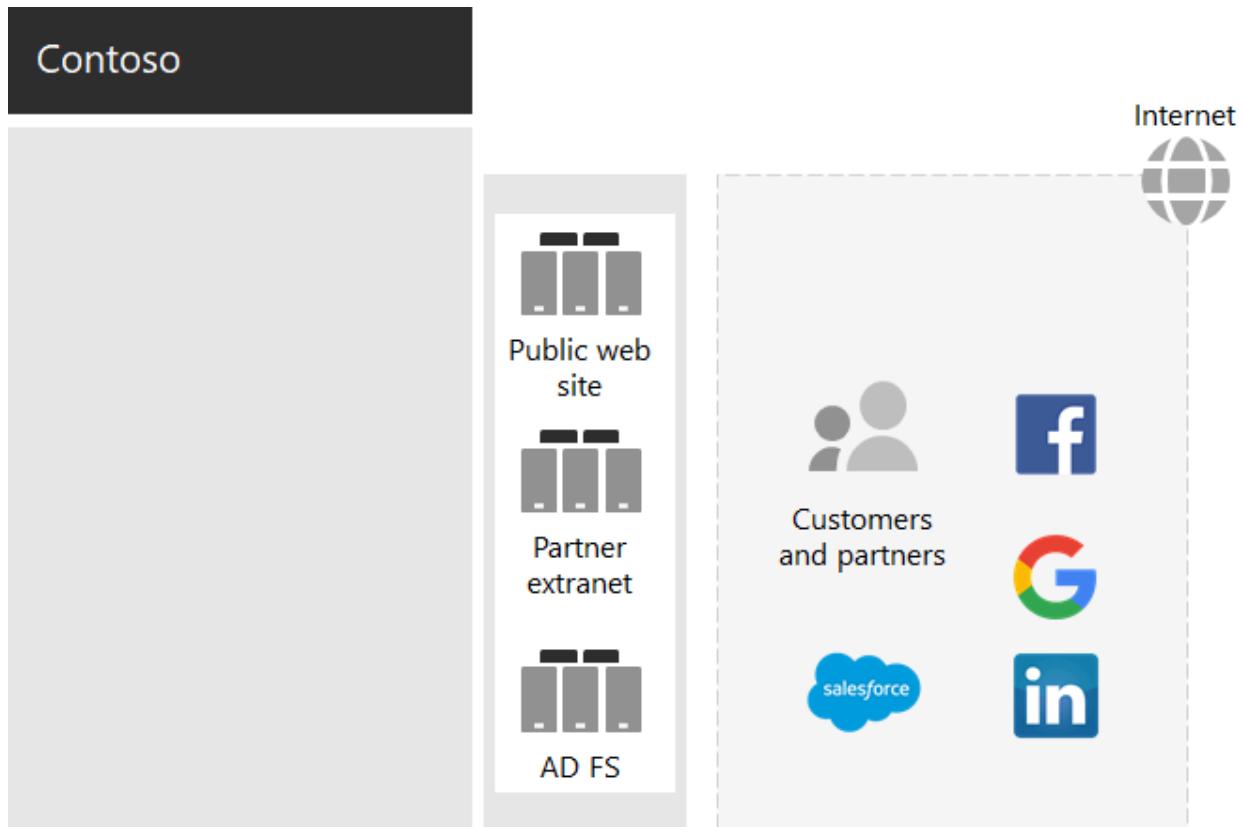
Contoso decided to use the accounts and groups in the contoso.com forest for authentication and authorization for its Microsoft 365 workloads and services.

## The Contoso federated authentication infrastructure

Contoso allows:

- Customers to use their Microsoft, Facebook, or Google Mail accounts to sign in to the company's public web site.
- Vendors and partners to use their LinkedIn, Salesforce, or Google Mail accounts to sign in to the company's partner extranet.

Here's 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.



AD FS servers in the DMZ facilitate authentication of customer credentials by their identity providers 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 authentication. Contoso identity architects are investigating the conversion of this infrastructure to Microsoft Entra [B2B](#) and [B2C](#) solutions.

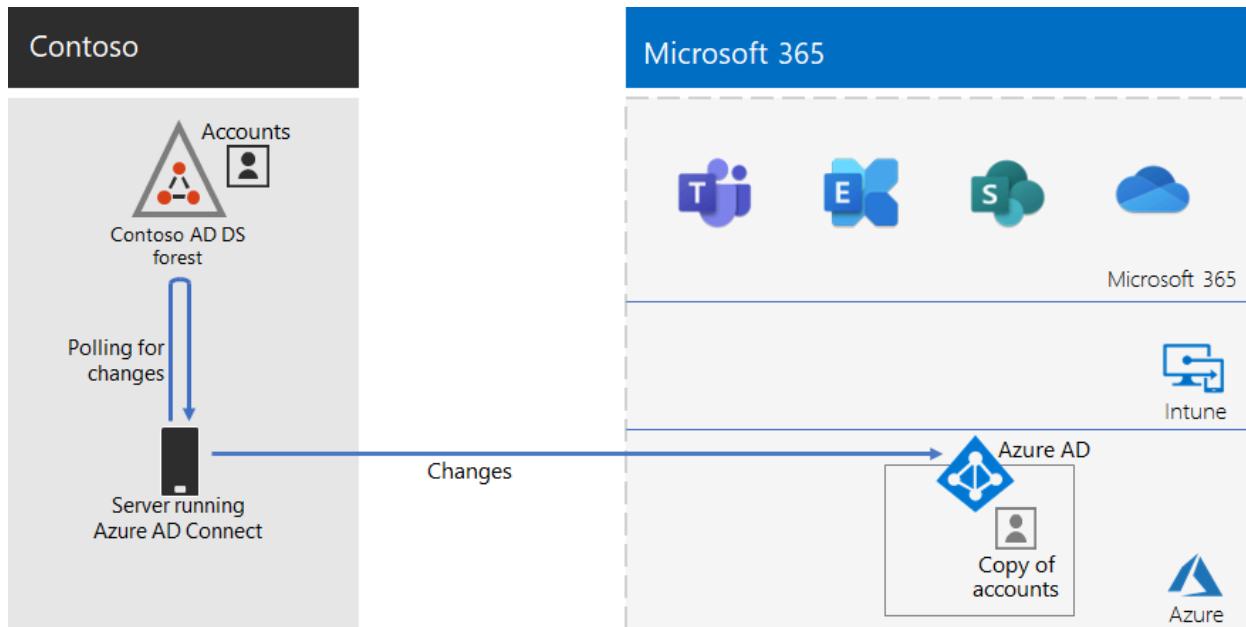
## Hybrid identity with password hash synchronization for cloud-based authentication

Contoso wanted to use its on-premises AD DS forest for authentication to Microsoft 365 cloud resources. It decided to use password hash synchronization (PHS).

PHS synchronizes the on-premises AD DS forest with the Microsoft Entra tenant of their Microsoft 365 for enterprise subscription, copying user and group accounts and a hashed version of user account passwords.

To do directory synchronization, Contoso deployed the Microsoft Entra Connect tool on a server in its Paris datacenter.

Here's the server running Microsoft Entra Connect polling the Contoso AD DS forest for changes and then synchronizing those changes with the Microsoft Entra tenant.



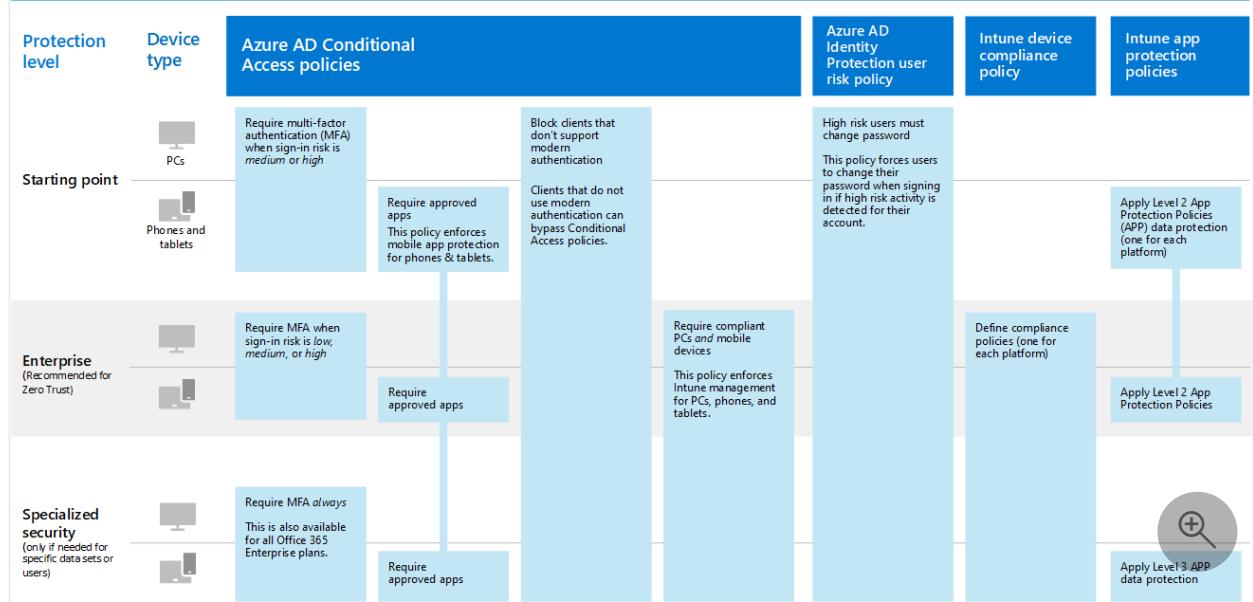
## Conditional Access policies for Zero Trust identity and device access

Contoso created a set of Microsoft Entra ID and Intune [Conditional Access policies](#) for three protection levels:

- *Starting point* protections apply to all user accounts.
- *Enterprise* protections apply to senior leadership and executive staff.
- *Specialized security* protections apply to specific users in the finance, legal, and research departments who have access to highly regulated data.

Here's the resulting set of Contoso identity and device Conditional Access policies.

## Zero Trust identity and device access policies for Contoso



## Next step

Learn how Contoso uses its Microsoft Endpoint Configuration Manager infrastructure to [deploy and keep current Windows 10 Enterprise](#) across its organization.

## See also

[Deploy identity for Microsoft 365](#)

[Microsoft 365 for enterprise overview](#)

## Feedback

Was this page helpful?

Yes

No

[Provide product feedback](#)

# Windows 10 Enterprise deployment for Contoso

Article • 02/17/2023

Prior to the wide rollout of Microsoft 365 for 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 advanced 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 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

Shows you the state of your devices with respect to the Windows updates so that you can ensure that they are on the most current updates as appropriate.

- Device Health

Identifies devices that crash frequently, and therefore might need to be rebuilt or replaced and device drivers that are causing device crashes, with suggestions of alternative versions of those drivers that might reduce the number of crashes. Provides notification of Windows Information Protection misconfigurations that send prompts to end users.

Contoso has an existing 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

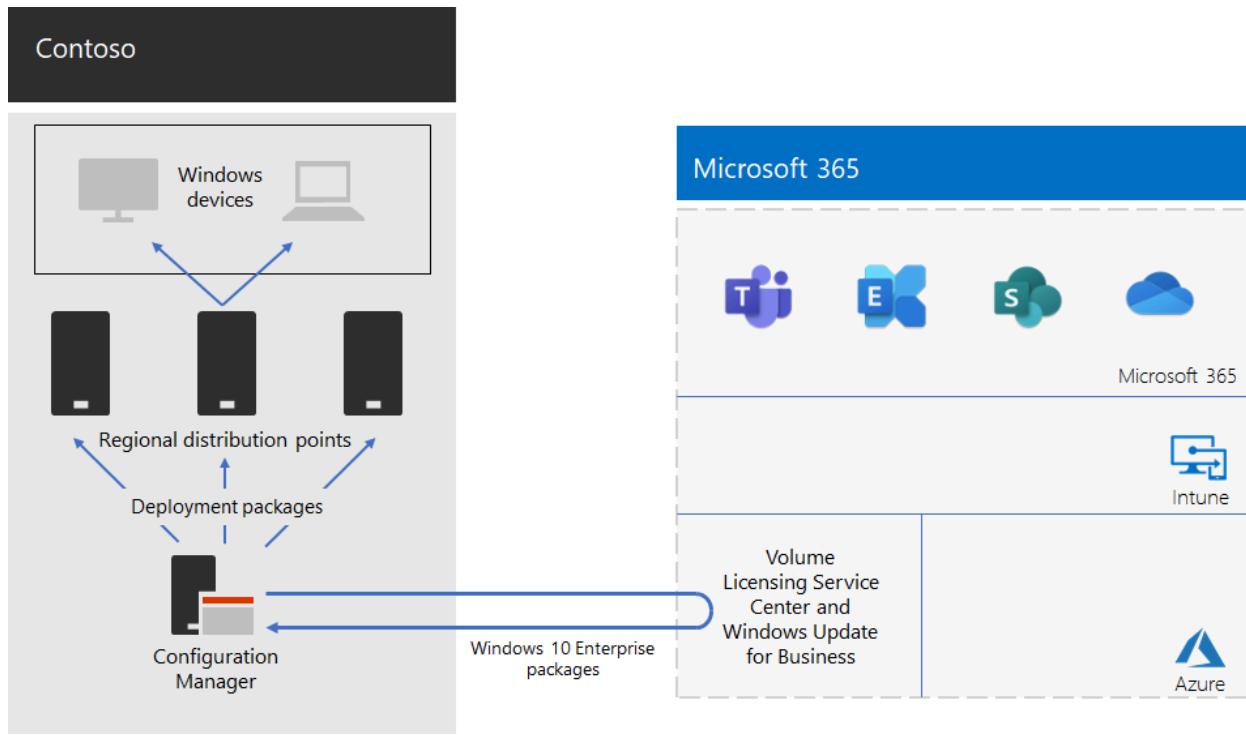
Contoso used the Upgrade Readiness in Windows Analytics to determine the set of installed apps and their compatibility with Windows 10 Enterprise.

## 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 groups.
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 group.
6. Ran the Configuration Manager deployment task sequences to deploy the selected Windows package to the broad deployment group.
7. Monitored PCs and devices in the broad deployment group using the Device Health and Update Compliance solutions to address issues.

Here is Contoso's in-place upgrade and ongoing updates deployment architecture.



This infrastructure consists of:

- 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 regional hub 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 group membership.

## Next step

Learn how Contoso is leveraging its Configuration Manager infrastructure to [deploy and keep current Microsoft 365 Apps for enterprise](#) across its organization.

## See also

[Windows 10 Enterprise](#)

[Microsoft 365 for enterprise overview](#)

[Test lab guides](#)

# Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Microsoft 365 Apps for enterprise deployment for Contoso

Article • 02/17/2023

Contoso upgraded their PCs to Windows 10 Enterprise and Microsoft 365 Apps for enterprise to enable more effective collaboration, better security, and a more modern desktop experience. After they assessed their infrastructure and business needs, Contoso identified these key requirements for the deployment:

- All PCs should run Microsoft 365 Apps for enterprise.
- Deployment should use existing management tools and infrastructure when possible.
- Deployment must support multiple languages and existing architectures on users' devices.
- PCs should stay up-to-date and secure with minimal IT administrative costs and minimal impact to users.

## Deployment tools

Based on their requirements, Contoso chose to deploy Windows 10 Enterprise and Microsoft 365 Apps for enterprise through 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.
- A 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 for Office Add-ins and VBA](#), a free tool from Microsoft, to assess compatibility issues with their Office macros and add-ins.

# Managing deployment and updates

Microsoft 365 Apps for enterprise has a new release model: Office as a service. The service model makes it easy to stay up to date with new features. But it often requires IT departments to change how they deploy and test new releases. To minimize compatibility issues and to ensure their computers stay up to date, Contoso deployed Windows and Office in two stages:

- First, they deployed Microsoft 365 Apps for enterprise to a small set of representative devices across the organization. This pilot group was used to test apps, add-ins, and hardware with Microsoft 365 Apps for enterprise.
- Four months later, after addressing all critical issues with apps, add-ins, and hardware in the pilot group, Contoso deployed Microsoft 365 Apps for enterprise to the rest of the devices in the organization (the broad group).

Instead of managing updates to Office by using Configuration Manager, Contoso enabled automatic updates from the cloud. Cloud-based updates reduce administrative overhead while ensuring that devices stay up to date.

Contoso followed the same two-stage approach for feature updates as 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 Enterprise Channel (Preview) for updates to the pilot group
- Semi-Annual Enterprise Channel for updates to the broad group

Because the Semi-Annual Enterprise Channel (Preview) releases a version of Microsoft 365 Apps for enterprise four months earlier than the Semi-Annual Enterprise Channel, Contoso has time to validate the updates without having to manage them.

## Deployment process

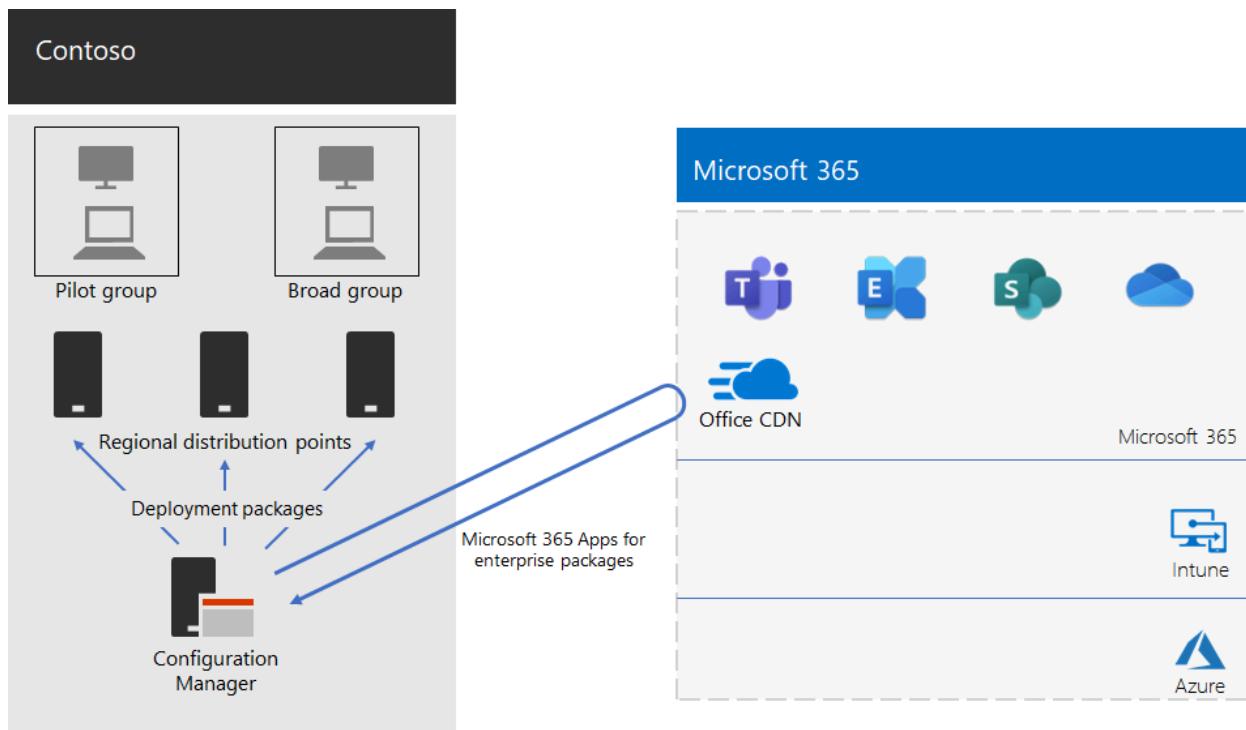
To complete the deployment of Office, Contoso implemented the following process, which includes best practice recommendations from Microsoft:

1. Before deployment, Contoso used the Readiness Toolkit for Office Add-in and VBA to test their apps and Office Add-ins to assess their compatibility with Microsoft 365 Apps for enterprise.
2. In Configuration Manager, they enabled peer cache on their client devices, which helps with limited network capacity when deploying to client devices in remote locations.

3. Contoso 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 for additional testing of apps, add-ins, and hardware with Windows 10 Enterprise and Microsoft 365 Apps for enterprise.
4. They created deployment packages for Office by using the Office Client Management dashboard and the Office 365 Installer wizard, which are both part of the Configuration Manager console. They built two Microsoft 365 Apps for enterprise packages, one for the pilot group on the Semi-Annual Enterprise Channel (Preview) and one for the broad group on the Semi-Annual Enterprise Channel.
5. Each Office package included English, French, and German Language packs. If a device required a language that wasn't included in the Office package, that language pack 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 Microsoft 365 Apps for enterprise.
7. In Configuration Manager, they deployed the Windows and Office packages to distribution points across their network. Then they ran the Configuration Manager deployment task sequences to deploy the pilot Microsoft 365 Apps for enterprise package to the pilot group.
8. After they addressed compatibility issues with the pilot group, Contoso ran the task sequences to deploy the Microsoft 365 Apps for enterprise 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 in the initial deployment.

Here is the Contoso Microsoft 365 Apps for enterprise installation and ongoing updates deployment architecture.



## Next step

Learn how Contoso is [using Microsoft Intune](#) in Microsoft 365 for enterprise to manage its devices and the apps that they run across the organization.

## See also

[Microsoft 365 Apps for enterprise](#)

[Microsoft 365 for enterprise overview](#)

[Test lab guides](#)

---

## Feedback

Was this page helpful?

Yes

No

[Provide product feedback ↗](#)

# Mobile device management for Contoso

Article • 08/01/2024

Microsoft 365 for enterprise includes Intune and a set of Azure services that support mobile device and application management and security.

Contoso has many mobile-enabled employees. Some have offices in Contoso locations, and some 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

Contoso identified the following Intune use cases of mobile device management for Microsoft 365 for enterprise:

- 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 doesn't use Intune to:

- Allow employees to securely access Microsoft 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 on-premises Microsoft Exchange servers.

## Deploy

This is how Contoso set up their mobile device management infrastructure:

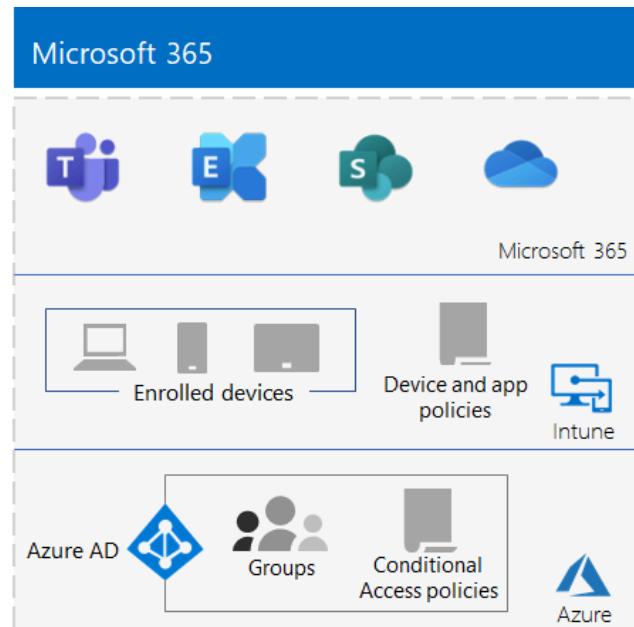
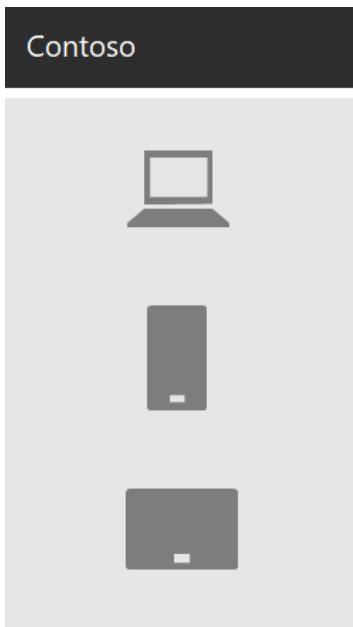
- Set Intune as the Mobile Device Management (MDM) authority, and use Intune on Azure to administer content and manage the devices
- Created Microsoft Entra groups for devices for enrollment and Intune settings and device-based Conditional Access policies

For more information, see [Contoso Conditional Access policies](#).

- Enabled the Apple device platform to support employees with iPads, iMacs, and iPhones, and corporate-owned iPhones
- 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 aren't enrolled, implemented a set of Mobile Application Management (MAM) policies to require authentication for access to Microsoft 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.

Contoso enrolled deployed PCs and company-owned smartphones and tablets by adding them to the appropriate Intune device groups. They also established a BYOD program for employees to enroll their personal devices. Enrolled devices receive Intune policies, which result in managed and secured devices and their applications. Devices that aren't enrolled have Mobile Application Management (MAM) policies that specify allowed applications.

Here is the Contoso mobile device management deployment architecture.



## Next step

Learn how Contoso uses the [information protection capabilities](#) of Microsoft 365 for enterprise to classify, identify, and protect crucial digital assets across its organization.

## See also

[Device management for Microsoft 365](#)

[Microsoft 365 for enterprise overview](#)

[Test lab guides](#)

---

## Feedback

Was this page helpful?

Yes

No

[Provide product feedback ↗](#)

# Information protection for the Contoso Corporation

Article • 12/22/2022

Contoso is serious about their information security. Leakage or destruction of intellectual property that describes their product designs and proprietary manufacturing techniques would place them at a competitive disadvantage.

Before moving their sensitive digital assets to the cloud, Contoso made sure that their on-premises information classification and protection requirements were supported by the cloud-based services of Microsoft 365 for enterprise.

## Contoso data security classification

Contoso performed an analysis of their data and determined the following classification levels.

[ ] Expand table

Level 1: Baseline	Level 2: Sensitive	Level 3: Highly regulated
Data is encrypted and available only to authenticated users.	Level 1 plus strong authentication and data loss protection.	Level 2 plus the highest levels of encryption, authentication, and auditing.
Provided for all data stored on-premises and in cloud-based storage and workloads. Data is encrypted while it resides in the service and in transit between the service and client devices.	Strong authentication includes Microsoft Entra multifactor authentication (MFA) with SMS validation. Microsoft Purview Data Loss Prevention ensures that sensitive or critical information doesn't travel outside the Microsoft cloud.	The highest levels of encryption for data at rest and in the cloud, compliant with regional regulations, combined with MFA with smart cards and granular auditing and alerting.
Examples of Level 1 data are normal business communications (email) and files for administrative, sales, and support workers.	Examples of Level 2 data are financial and legal information and research and development data for new products.	Examples of Level 3 data are customer and partner personal information, product engineering specifications, and proprietary manufacturing techniques.

# Contoso information policies

The following table lists the Contoso information policies.

[Expand table](#)

Value	Access	Data retention	Information protection
Low business value (Level 1: Baseline)	Allow access to all.	6 months	Use encryption.
Medium business value (Level 2: Sensitive)	Allow access to Contoso employees, subcontractors, and partners.  Use MFA, Transport Layer Security (TLS), and Mobile Application Management (MAM).	2 years	Use hash values for data integrity.
High business value (Level 3: 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.

## The Contoso path to information protection with Microsoft 365 for enterprise

Contoso followed these steps to prepare Microsoft 365 for enterprise for their information-protection requirements:

### 1. Identify 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 asset.

### 2. Determine 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. Create sensitivity labels and their settings for the different levels of information

Contoso created sensitivity labels for their data levels, with their highly regulated label that includes encryption, permissions, and watermarks.

4. Move data from on-premises SharePoint sites and file shares to their new SharePoint sites

The files migrated to the new SharePoint sites inherited the default retention labels assigned to the site.

5. Train employees how to use sensitivity labels for new documents, how to interact with Contoso IT when creating new SharePoint sites, and to always store digital assets on SharePoint sites

Changing bad worker information-storage habits is often considered the hardest part of the information protection transition for the cloud. Contoso IT and management needed to get employees to always label and store their digital assets in the cloud, refrain from using on-premises file shares, and not use third-party cloud storage services or USB drives.

## Conditional Access policies for information protection

As part of their rollout of Exchange Online and SharePoint, Contoso configured the following set of Conditional Access policies and applied them to the appropriate groups:

- Managed and unmanaged application access on devices policies
- Exchange Online access policies
- SharePoint access policies

Here's resulting set of Contoso policies for information protection.

Protection level	Device type	Azure AD conditional access policies				Intune device compliance policy	Intune app protection policies	SharePoint device access policies
Baseline	PC	Require compliant PCs	Block clients that don't support modern authentication	Block ActiveSync clients	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.)	Define compliance policies (One policy for each platform)	Define app protection policies (iOS and Android)	Access control policy: allow browser-only access to specific SharePoint sites from unmanaged devices
	Phone/Tablet	Require approved apps (Enforces mobile app protection for phones and tablets)	(Clients that do not use modern authentication can bypass conditional access rules, so it's important to block these)					
Sensitive	PC	Require compliant PCs and mobile devices (Enforces Intune management for PCs and phone/tablets)					Access control policy: block access to specific SharePoint sites from unmanaged devices	Access control policy: allow browser-only access to specific SharePoint sites from unmanaged devices
	Phone/Tablet							
Highly regulated	PC							
	Phone/Tablet							

### Note

Contoso also configured additional Conditional Access policies for identity and sign-in. See [Identity for the Contoso Corporation](#).

These policies ensure that:

- Apps that are allowed and the actions they can take with the organization's data are defined by app protection policies.
- PCs and mobile devices must be compliant.
- Exchange Online uses Office 365 message encryption (OME) for Exchange Online.
- SharePoint uses app-enforced restrictions.
- SharePoint uses access control policies for browser-only access and to block access for unmanaged devices.

## Mapping Microsoft 365 for enterprise features to Contoso data levels

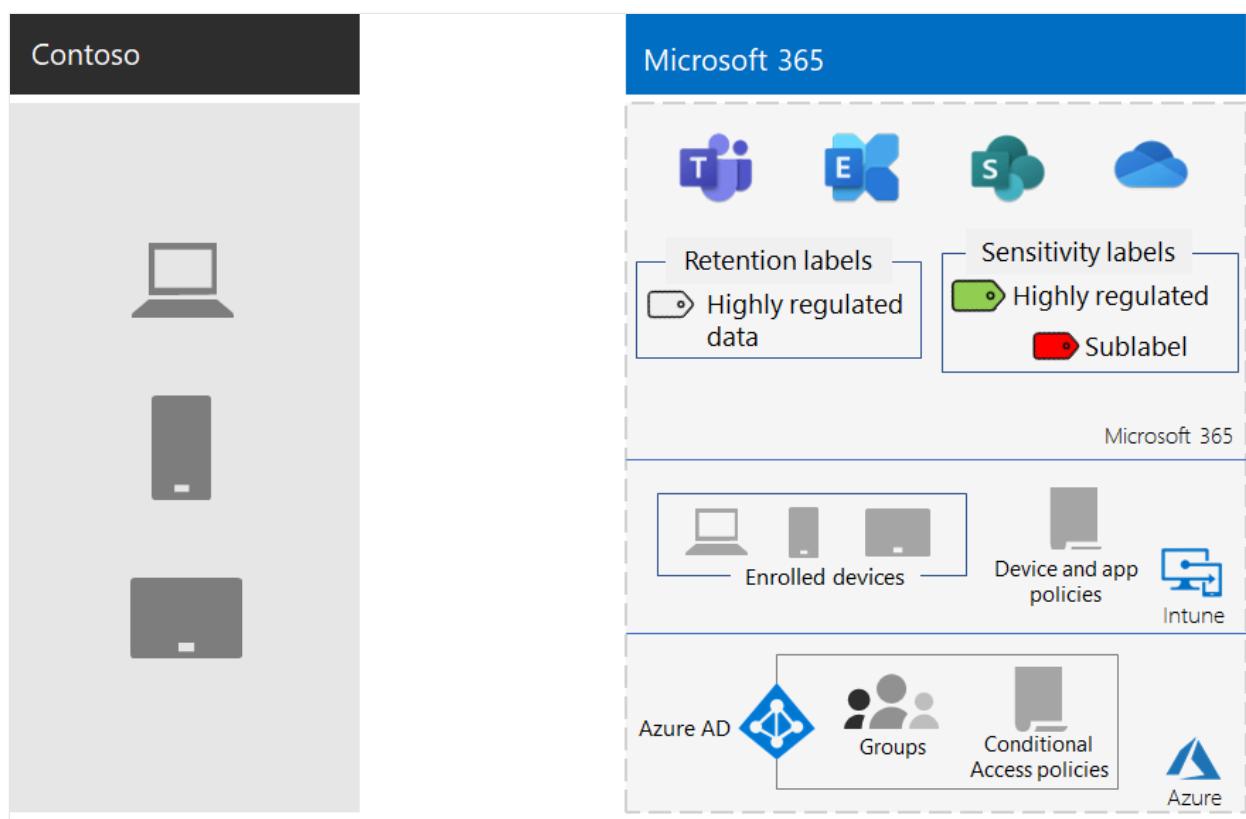
The following table maps Contoso data levels to information protection features in Microsoft 365 for enterprise.

[\[ \] Expand table](#)

Level	Microsoft 365 cloud services	Windows 10 and Microsoft 365 Apps for enterprise	Security and compliance
Level 1: Baseline	SharePoint and Exchange Online Conditional Access policies Permissions on SharePoint sites	Sensitivity labels BitLocker Windows Information Protection	Device Conditional Access policies and Mobile Application Management policies
Level 2: Sensitive	Level 1 plus: Sensitivity labels Microsoft 365 retention labels on SharePoint sites Data Loss Prevention for SharePoint and Exchange Online Isolated SharePoint sites	Level 1 plus: Sensitivity labels on digital assets	Level 1

<b>Level</b>	<b>Microsoft 365 cloud services</b>	<b>Windows 10 and Microsoft 365 Apps for enterprise</b>	<b>Security and compliance</b>
Level 3: Highly regulated	Level 2 plus: Bring your own key (BYOK) encryption and protection for trade secret information Azure Key Vault for line-of-business applications that interact with Microsoft 365 services	Level 2	Level 1

Here's the resulting Contoso information-protection configuration.



## Next step

Learn how Contoso uses the [security features across Microsoft 365 for enterprise](#) for identity and access management, threat protection, information protection, and security management.

## See also

[Microsoft Defender for Office 365](#)

## Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

# Summary of Microsoft 365 for enterprise security for the Contoso Corporation

Article • 07/30/2024

To get approval to deploy Microsoft 365 for enterprise, the Contoso IT security department conducted a thorough security review. They identified the following 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.
- Protect PCs and email 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 additional encryption and permissions.
- IT security staff can monitor the current security posture from central dashboards and get notified of security events for quick response and mitigation.

## The Contoso path to Microsoft 365 security readiness

Contoso followed these steps to prepare their security for their deployment of Microsoft 365 for enterprise:

### 1. Limit administrator accounts for the cloud

Contoso did an extensive review of its existing Active Directory Domain Services (AD DS) administrator accounts and set up series of dedicated cloud administrator accounts and groups.

### 2. Classify data into three security levels

Contoso did a careful review and determined the three levels, which were used to identify the Microsoft 365 for enterprise features to protect the most valuable data.

### 3. Determine access, retention, and information protection policies for data levels

Based on the data levels, Contoso determined detailed requirements to qualify future IT workloads that are moved to the cloud.

To follow security best practices and Microsoft 365 for enterprise deployment requirements, Contoso security administrators and its IT department deployed many security features and capabilities, as described in the following sections.

## Identity and 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 strong passwords. The accounts are protected by Microsoft Entra multifactor authentication (MFA) and Microsoft Entra Privileged Identity Management (PIM). *PIM is only available with Microsoft 365 E5.*

Signing in with a **Microsoft Entra DC admin**, or **Global admin** account is only done for specific administrative tasks. The passwords are only known to designated staff and can only be used within a time period that's configured in Microsoft Entra PIM.

Contoso security administrators assigned lesser admin roles to accounts that are appropriate to that IT worker's job function.

For more information, see [About Microsoft 365 admin roles](#).

- MFA for all user accounts

MFA adds an additional layer of protection to the sign-in process. It requires users to acknowledge a phone call, text message, or app notification on their smart phone after correctly entering their password. With MFA, Microsoft Entra user accounts are protected against unauthorized sign-in, even if an account password is compromised.

- To protect against compromise of the Microsoft 365 subscription, Contoso requires MFA on all **Microsoft Entra DC admin**, or **Global admin** 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 managers and executives.

- Safer device and application access with Conditional Access policies

Contoso is using [Conditional Access policies](#) for identity, devices, Exchange Online, and SharePoint. 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 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 Conditional Access policies include additional protection for sensitive and highly regulated sites.

- Windows Hello for Business

Contoso deployed [Windows Hello for Business](#) to eventually eliminate the need for passwords through 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 enabled [Windows Defender Credential Guard](#) through AD DS group policy.

## Threat protection

- Protection from malware with Microsoft Defender Antivirus

Contoso is using [Microsoft 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 Microsoft Defender for Office 365

Contoso is using Exchange Online Protection and [Defender for Office 365](#) to protect against unknown malware, viruses, and malicious URLs transmitted through emails.

Contoso also enabled mailbox audit logging to identify who logs in to user mailboxes, sends messages, and does other activities performed by the mailbox owner, a delegated user, or an administrator.

- Attack monitoring and prevention with Office 365 threat investigation and response

Contoso uses [Office 365 threat investigation and response](#) to protect 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 labels

Contoso determined three levels of data protection and deployed [Microsoft 365 sensitivity labels](#) that users apply to digital assets. For its trade secrets and other intellectual property, Contoso uses sensitivity sublabels for highly regulated data. This process encrypts content and restricts access to specific user accounts and groups.

- Prevent intranet data leaks with Data Loss Prevention

Contoso configured [Microsoft Purview Data Loss Prevention](#) policies for Exchange Online, SharePoint, 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 Defender for Cloud Apps

Contoso is using [Microsoft Defender for Cloud Apps](#) to map their cloud environment, monitor its usage, and detect security events and incidents. *Microsoft Defender for Cloud Apps is only available with Microsoft 365 E5.*

- Device management with Microsoft Intune

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 Microsoft Defender for Cloud

Contoso uses the [Microsoft Defender for Cloud](#) to present 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 deployed the [Windows Security app](#) to its PCs and devices running Windows 10 Enterprise so that users can see their security posture at a glance and take action.

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

# Microsoft 365 solution and architecture center

This solution and architecture center brings together the technical guidance you need to understand, plan, and implement integrated Microsoft 365 solutions for enterprise resource planning and secure and compliant modern collaboration.

## Foundational solution guides

### QUICKSTART

[Set up your infrastructure for hybrid work](#)

[Set up secure collaboration with Microsoft 365](#)

[Deploy ransomware protection](#)

[Manage data privacy and data protection](#)

[Microsoft 365 for smaller businesses and campaigns](#)

## Architecture illustrations and design principles

### ARCHITECTURE

[Microsoft cloud architecture models](#)

[Microsoft 365 productivity illustrations](#)

[Design principles](#)

[Infographics for your users](#)

[Architecture icons and templates](#)

## Administration and migration solution guides

### HOW-TO GUIDE

[Tenant management](#)

[Remove a former employee](#)

## Meetings and communications solution guides

### DEPLOY

[Plan and deploy a Teams Voice solution](#)

### OVERVIEW

[Organizational communication](#)

## Teamwork and collaboration solution guides

### DEPLOY

[Manage contracts for your business](#)

### OVERVIEW

[Intelligent intranet](#)

[Collaboration governance](#)

[File collaboration](#)

[OneDrive guide for enterprises](#)

## Compliance solution guides

### DEPLOY

[Insider risk solutions](#)

[Auditing solutions](#)

[eDiscovery \(Premium\)](#)

### REFERENCE

[ISO - Recommended action plan](#)

[NIST - Recommended action plan](#)

[CCPA - Recommended action plan](#)

[GDPR - Recommended action plan](#)

## Security solution guides

### DEPLOY

[Top tasks for security teams to support working from home](#)

[Microsoft 365 security for Business Decision Makers \(BDMs\)](#)

[Identity and device access configurations](#)

[Deploy Microsoft Defender for Endpoint](#)

[Evaluate Microsoft Defender XDR](#)

[Security recommendations for priority accounts](#)

[Evaluate Microsoft Defender XDR](#)

### HOW-TO GUIDE

[Switch from a non-Microsoft endpoint protection solution to Microsoft Defender for Endpoint](#)

[Address false positives/negatives in Microsoft Defender for Endpoint](#)

## Workload resources

### REFERENCE

[Contoso case studies](#)

### TUTORIAL

[Test lab guides](#)

## Industry-specific guidance

### OVERVIEW

[Security and compliance for financial services](#)

[Security and compliance for energy and utility services](#)

[Microsoft 365 for frontline workers](#)

[Microsoft 365 for Healthcare](#)

[Microsoft 365 for Retail](#)

[Teams for Education](#)

[Teams for Government](#)

[Support remote government workers using Teams](#)

# Enterprise business continuity management customer and cloud partner responsibilities

Article • 06/24/2024

Getting Microsoft 365 cloud services to your users is a partnership between your organization and Microsoft. Microsoft provides the services and you're responsible for connecting your client endpoints, managing identity and access and how those services are used. There are shared responsibilities, such as the identity and directory infrastructure as well. This article covers some of the critical items you need to be mindful of to keep your business functioning during a service incident and it helps set expectations as to what Microsoft does during a service incident.

## Transparency during service incidents

As a trusted partner, Microsoft builds highly resilient cloud services and follows structured procedures to resolve service incidents when they happen. When a service incident occurs, Microsoft recognizes that **timely, targeted, and highly available** communications are critical for customers.

### Timely

Microsoft notifies Microsoft 365 administrators by updating the tenant-specific Service Health Dashboard (SHD) in the Microsoft 365 Admin Portal. Service incident updates are normally provided on an hourly cadence. If a different cadence is needed, we'll inform you of the change in the SHD communication postings.

### Targeted

In most cases, when our monitoring systems detect an issue, we can identify the affected customer base, from a single customer up to region or beyond and direct the necessary communications to those customers. This helps you know what you need to know for your business and not be distracted by noise notifications that don't impact you. For example, if a specific mailbox database is impacted, we're able to identify exactly which customers have users on the affected infrastructure and scope our communications to them. If the scope of impact of the incident is unclear, we expand

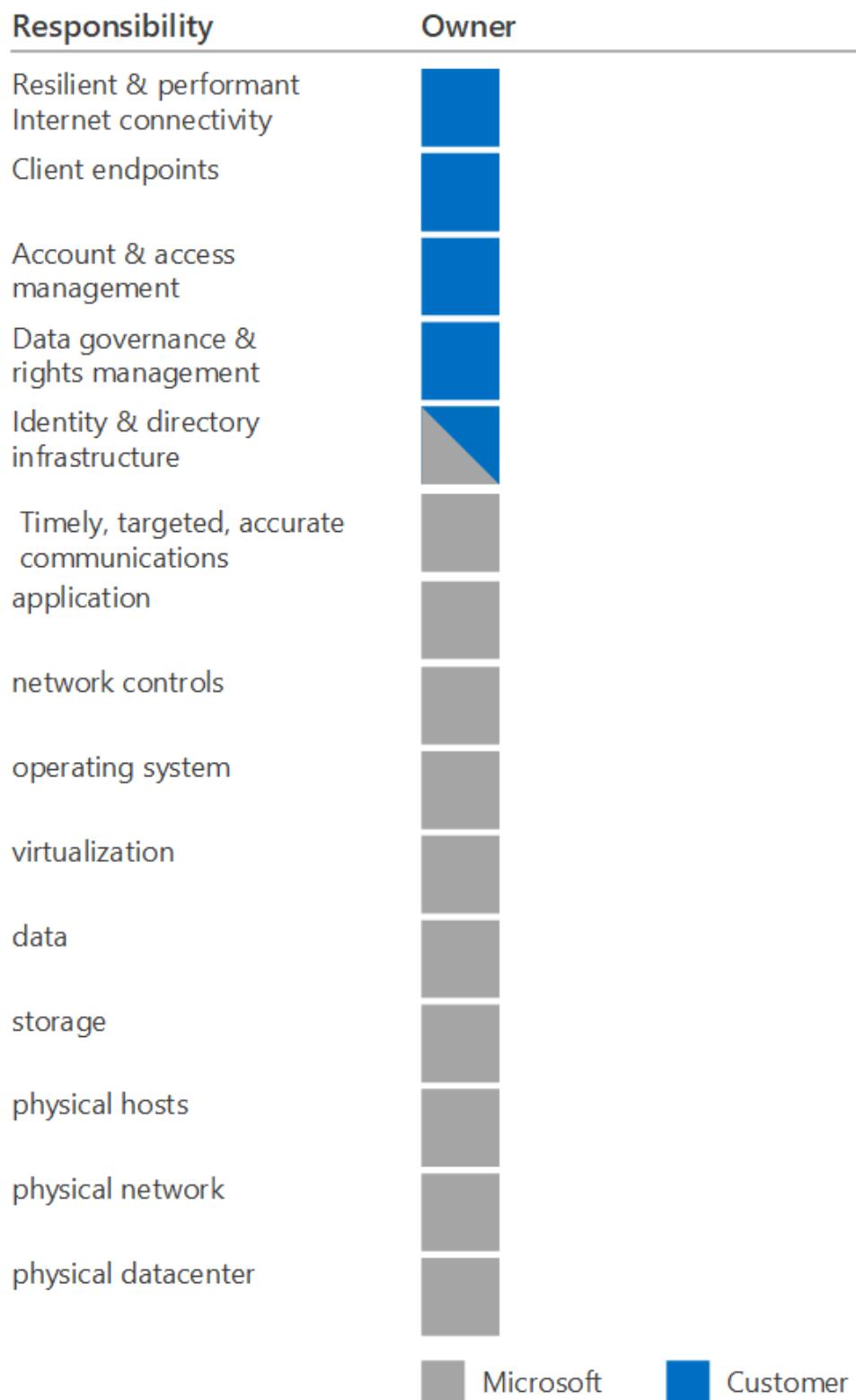
our communications out to the widest group of customers who are potentially impacted.

## Highly available

Microsoft maintains multiple channels for service status communications that customers can use.

- In the event the Admin center or the Service Health Dashboard within the Admin center are unavailable, you can monitor the service status using our [backup site](#).
- We maintain a Twitter account [@MSFT365Status](#) where we'll respond to reports of impact and post updates on SHD impacting events.
- The Admin App for Microsoft 365 tenant administrators gives you the ability to connect with your organization's Microsoft 365 service status on the go. Tenant administrators have the ability to view service health information and maintenance status updates from their mobile devices. For more information, visit the [Admin App FAQ](#).
- The [Microsoft 365 Service Communications API](#) enables you to access service communications so you can more easily monitor your environment. You can connect to the API, receive real-time service health data, and publish the information on an internal dashboard to inform enterprise users of incidents. Distributing the information internally can decrease your helpdesk traffic during an outage.
- For major incidents, Microsoft publishes Post Incident Reviews (PIR) to the SHD within the Admin center. PIRs contain key incident information to help you understand the nature of the outage. It generally contains the following sections:
  - User impact
  - Scope of impact
  - Incident start-end date and time
  - Root cause
  - Actions taken
  - Next steps
- Ancillary communications are available in the Microsoft 365 Message Center, such as notices of upcoming changes, new features, or planned maintenance.
- For more information, see the [Service Health and Continuity guide](#) to learn more about the different communication channels and how to monitor service health.

Providing access to Microsoft 365 online services is a partnership between your organization and Microsoft. The following chart summarizes the balance of responsibility for both Microsoft and the customer during a service incident and during regular operations.



# Your environment - service continuity

When thinking about your continuity plan, be mindful of events that may impact your organization and its overall ability to communicate. At a high level, there are three factors that could impact your business.

## People

Consider events that would cause impact to your workforce like a natural disaster or a pandemic. This is often overlooked, due to the unlikely nature of a broad-scale impact if your workforce is widely distributed. But, if a large percentage of the workforce were offline, would your business continue to operate? How do you mitigate that?

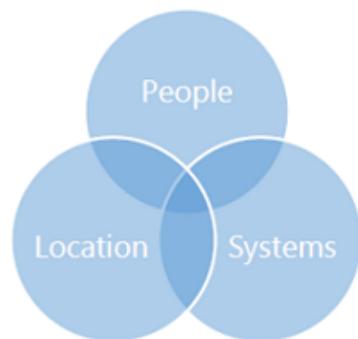
## Location

Many organizations require employees to be in specific physical or network locations in order to connect to enterprise systems and cloud services.

Microsoft publishes [network connectivity principles](#) that guide enterprises through best practices for setting up network connectivity to cloud resources. Examples of optimization include implementation of split tunnel VPNs to allow connections directly from a user's network rather than over a VPN tunnel. While these connectivity principles are important for maintaining low-latency connections, service resiliency requires alternative methods of connecting to corporate resources for general collaboration.

## Systems

Many collaboration solutions are dependent on systems, such as the company-wide area network (WAN). When those systems aren't available, how would your organization respond? This graphic represents issues that may impact more than one area. The accompanying table provides examples to consider



	LAN failure	Pandemic	Severe weather event	Security Breach
Systems	Yes	Yes	?	Yes
People	No	Yes	Yes	No
Location	No	Yes	Yes	No

Your continuity plans should consider each of these areas. For example: If you require users to be on the corporate network and there's a snowstorm, how do those users gain

access to key resources? If the snow prevents travel into the office and service engineers are required to connect to the corporate network, is there a policy mandating they have their corporate laptops in their possession at home?

---

## Feedback

Was this page helpful?



# Built-in service resiliency in Microsoft 365

Article • 06/24/2024

Microsoft recognizes the need to provide solutions that function consistently and remain highly available in a way that our customers can rely on them. When any given service is unavailable, it's called downtime. The definition of downtime varies for each Microsoft 365 service, but they commonly focus on any period of time when users are unable to use the essential functionality of the service. For example, here's the definition of downtime for SharePoint taken from the Microsoft 365 service level agreement:

**"SharePoint Downtime:** Any period of time when users are unable to read or write any portion of a SharePoint site collection for which they have appropriate permissions."

You can find the downtime definitions for each service in the [Service Level Agreements](#).

To minimize downtime, either planned or unexpected, Microsoft 365 services are designed and operated to be highly available and resilient to failure by focusing on four areas:

## Active/Active design

In Microsoft 365, we're driving towards having all services architected and operated in an active/active design that increases resiliency. This design means that there are always multiple instances of a service running that can respond to user requests and that they're hosted in geographically dispersed datacenters. All user traffic comes in through the Microsoft Front Door service and is automatically routed to the optimally located instance of the service and around any service failures to prevent or reduce impact to our customers.

## Reduce incident scope

The scope of a service incident is measured by how severe it is, how long it lasts and how many customers are impacted. We strive to limit the scope of all incidents by:

- having multiple instances of each service partitioned off from each other
- deploying updates in a controlled, graduated fashion using rings of validation so that any issues that might arise from the update can be detected and mitigated early in the deployment process. This design allows for regression of the update if

needed and first occurs in a small group inside Microsoft (inner ring) before it's deployed for larger groups like all 140,000 Microsoft employees (ring 2), then for early adopter rings (ring 3) and ultimately for all customers globally (ring 4).

- driving improvements in monitoring through automation. Microsoft 365 is a large service, and the SLA target uptime is high. At the very beginning of a service incident, if humans had to be involved in detection and response, we couldn't respond fast enough to meet SLAs. Automation is the key to fast and effective service incident detection and response. The sooner we know about something, the faster it can be fixed.

Along with the active/active capabilities built into Microsoft 365 service architecture, these efforts mitigate the severity, duration, and number of impacted customers during a service incident.

## Fault isolation

Just as the services are designed and operated in an active/active fashion and are partitioned off from each other to prevent a failure in one from affecting another, the code base of the service is developed using similar partitioning principles called fault isolation. Fault isolation measures are incremental protections made within the code base itself. These measures help prevent an issue in one area from cascading into other areas of operation.

Fault isolation measures are applied at multiple stages of the development and delivery of a service, including code development, service deployment, load balancing, and database replication.

The Microsoft Security Development Lifecycle (SDL) further promotes resiliency and consists of a set of practices that support security and compliance requirements. SDL guides our developers in building resilient, secure, compliant services. Key elements of SDL include code reviews, threat modeling, penetration testing, and standardized incident response processes across the Microsoft cloud.

Microsoft 365 services are highly interconnected, but the systems and technology behind them are engineered in a way that limits the impact of one service incident from spilling over to other services. For example, an issue affecting Exchange won't impact core functionality in Teams, or an issue with search functionality in SharePoint won't affect users' ability to upload or download files.

## Continuous service improvement

When we experience an incident, we take it seriously. After all, our redundant cloud architecture and rigorous internal processes aim to keep our services accessible. During an incident, our monitoring rapidly detects the affected services and, if your tenant is affected, you'll be notified through various channels. Simultaneously, engineers follow well-defined processes to triage the issue and take the necessary steps to restore normal operation as quickly as possible. Once the service is functioning normally again, we hold post incident reviews as part of the cycle of continuous service improvement. During the post incident review, we identify the root causes of the incident and what was required to fix the issues. Then we take what was learned from the situation and apply it to the design and operations of all of our suite of offerings. With this knowledge, we can prevent the same root cause from impacting other services and additional customers.

---

## Feedback

Was this page helpful?

 Yes

 No

# Developing your business continuity plan

Article • 03/02/2023

This article provides guidance on developing a business continuity plan that takes Microsoft 365 dependencies into account. Here we recommend methods for analyzing your business functions and identifying the ones that depend on Microsoft 365 services. You'll perform this analysis with the anticipation that there will be service failures and that you have to prepare for those possibilities.

Broadly speaking, business continuity planning involves four aspects, assessment, planning, capability validation, and communication and coordination.

## Assessment

First you must identify the business functions in your org and the services and processes that support them. This includes completing a business impact analysis, where each business function is ranked according to how critical it is and you identify the processes and services that each one depends on. Here's a sample table you can refer to help you get started with your own assessment.

### Sample Business Impact Assessment (BIA)

This is a BIA document for `name of the service, system, process, or function`

[\[\] Expand table](#)

BIA fields	Description
BIA type	<code>is it a business process or technology, service or system?</code>
BIA name	<code>name of the service/system/function/process</code>
Service description	<code>give a full description of the service, process, or function</code>
Enterprise function	<code>some examples: customer services; legal; marketing; risk management, security, sales, information technology, production, manufacturing</code>
Fiscal year	<code>the current fiscal year, re-evaluate these on a regular basis</code>

BIA fields	Description
Criticality	develop your own classifications, but here are some examples: mission critical, important, deferrable
Business unit	name of the business unit that owns this business function
Process (service, feature)	the name of the process, service, or feature
Business group senior leader	the name and contact information of the senior leader of the business group that owns this business process
Does the technology have an established <b>internal</b> Service Level Agreement (SLA) or Operational Level Agreement (OLA)?	please explain in as much detail as possible
Does the technology have an established <b>external</b> SLA or OLA?	please explain in as much detail as possible
Does the technology have a known executive mandate driving a specific process SLA? If yes, explain in detail.	details here
Will the loss or compromise of the data associated with this service trigger a major event? If yes, explain in detail.	details here
Does the service have a workaround or alternative in place for some or all of its key functions and features? If yes, explain in detail.	details here
Does the service process, store, or transmit customer data, such as personally identifiable information (PII)? If yes, explain in detail.	details here
BIA status	develop your own status classification, here are some examples: planned, started, in-progress, complete, on-hold, expired
Completion date	the date this BIA was completed
BIA facilitator	name of the person or group who is responsible for developing and maintaining this BIA
BIA approval	name of the person or group who is the executive sponsor of this BIA and who has responsibility for

BIA fields	Description
	approving it.
Contributors	optional list of the people who helped develop this BIA and their contact information
BIA approval location	indicate where the executive approval is located, or attach proof to this document

## Planning

Next, you look across business processes to see where any cascading dependency relationships exist. Based on the outcome, you prioritize and form resiliency strategies, and standard operating procedures supporting your strategies.

You can use [Microsoft Service Map](#) to help you in with this mapping. Microsoft Service Map automatically discovers application components on Windows and Linux systems and maps all TCP dependencies, identifies connections, and remote third-party systems that the app depends on. It also maps dependencies to areas of your network that are traditionally dark, such as Active Directory.

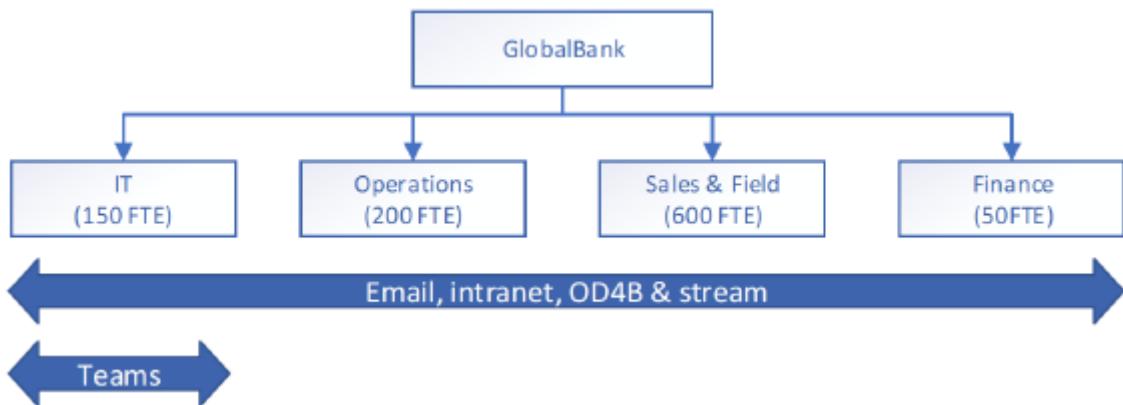
Here's a sample Dependency Analysis (DA) you can start from. In your DA, you'll identify and examine the process dependencies. Make sure you include people, suppliers, customers, partnerships, and facilities. The data from this analysis will be used to identify gaps between the recovery requirements of a process and the recovery capabilities of supporting dependencies.

[\[+\] Expand table](#)

Field	Description
Process type	
Facilitator	
Completed by	
Completed date	
Contributors	

## Capability validation

Once you have inventoried your business processes and mapped out relationships to other process and technologies, you need to build validation scenarios for all the processes. Basically, figure out how you're going to validate your business process continuity plans. You'll probably find that some are more important than others and you'll want to prioritize those. Don't forget that regularly training for employees on incident response and continuity measures is important once the plan is established. Post incident reviews should be used to enhance your resiliency strategies by incorporating learnings from each validation or test.



## Incident coordination and communication

During a service incident, normal communications channels may be impacted or degraded, so you should prearrange alternatives to help your organization stay connected during an incident. It's critical that the communication channels be established, vetted for security and compliance, and users trained on their use prior to a disruption. Failing from a known state to another known state is far preferable to users coming up with ad-hoc, unknown solutions in the middle of a crisis.

At Microsoft, each service team has established internal alternative communication channels to help us coordinate when our normal communications channels aren't available. These include backup telephony and audio-conferencing solutions, Viva Engage groups, Teams groups, internal Service Health Dashboards, and internal Incident Management software.

During your BIA and DA, you'll be mapping critical processes and the technologies or services they depend on. Pay special attention to communication during this phase of planning and think of alternatives. Here are some examples.

- If email is your primary method of keeping your users and stakeholders informed, and your email service is degraded or unavailable, you can use another service such as Microsoft Teams, Viva Engage, or another 3rd-party service as a backup. The key is to establish these beforehand and train your users on where to go. A

Viva Engage thread isn't going to be useful if no one knows it exists or if no one has it bookmarked.

- If your internal Incident Management processes rely on voice communications to coordinate your responses, establish an alternative telephony solution for use during a crisis. This solution doesn't need to have full parity with your primary service but should provide the minimum level of collaboration to coordinate your Business Continuity and Incident Management teams. Additionally, asking users to publish their mobile phone numbers in your Global Address List can provide an additional layer of backup communication in extreme cases.
- You may want to create a custom service health dashboard, or other such site, which can provide status updates during an incident. Training users where to go for information beforehand will help reduce unnecessary calls to help desk and instill confidence in your user base that the situation is being handled quickly and efficiently. Use the O365 Service Communications API to tie this information into Microsoft 365 for an even greater level of visibility.
- It's critical that the location of your Business Continuity Plans and Standard Operating Procedures is well known. We recommend maintaining online and offline copies of critical documentation, such as with SharePoint or OneDrive configured for automatic sync to local devices. For Service/Network Operations Centers and other similar teams that are critical for recovery, you may also want to keep hard copies available to be used in case event of an emergency.

## Know your external points of integration

Regardless of business model, every company has points of integration with their customers, partners, and vendors. The business value supply chain is built on integration with external entities. Improving business continuity for service disruptions requires consideration and protection of each point of integration.

As you analyze your supply chain, external communications should be considered in the same way internal communications are analyzed. Do your customers rely on your Exchange Online servers as the only method of contacting you? Have you established and made your suppliers aware of alternative communication methods, in the event uptime is impacted? Here's a sample table that suggests how to organize your thinking.

[ ] Expand table

External entity name	Impacting incident scenario	Microsoft 365 services integrated	Alternatives
Vendor name	Mail flow	Exchange Online is the only means of communication	Set up external Microsoft Teams channels or a third-party

External entity name	Impacting incident scenario	Microsoft 365 services integrated	Alternatives
		with Contoso	collaboration software
service supplier name	Chat	Microsoft Teams	Third-party instant messaging
partner name	Voice	Microsoft Teams	Mobile or public pstn
supplier name	File sharing	Externally shared SharePoint sites and OneDrive	Third-party file sharing

---

## Feedback

Was this page helpful?

 Yes

 No

# Service incident mitigation strategies

Article • 06/24/2024

Here are some strategies and scenarios that show how to mitigate the impact of a Microsoft 365 service incident on your business process.

## Service incident scenarios and potential mitigations

 Expand table

Microsoft 365 dependency	potential mitigations
Incident Management system relies on Exchange to engage On-Call Engineers and Incident Managers.	Ensure that your Incident Management system supports multichannel communications, such as parallel email, phone call, and SMS notification, and call tree hierarchies in case the primary on-call doesn't engage, the system automatically engages the backup. Also include backup contact methods in every notification, so that backup communication methods are embedded for easy reference. Alternative communication methods, such as Viva Engage, can be used for emergency collaboration if the incident management service is unavailable.
Microsoft Teams is used for storing files accessed via the client.	Teams stores files uploaded to the client in a SharePoint document library. Files are still accessible via SharePoint. Train users on file locations in SharePoint.
Microsoft Teams conference calling is relied upon for general communication and incident management triage.	Establish a backup conferencing solution with a 3rd-party provider.
VoIP phones are used as a secondary method of communication.	Implement non-VoIP phones capable of PSTN calling, especially for network and service operations centers during incidents. Add employee mobile phone numbers to the company directory for enabling critical personnel to be contacted over the cellular network.
OneDrive for Business is relied upon for file storage and user productivity. <a href="#">Files On-Demand</a> is configured to free up space on local user drives.	OneDrive sync supplies group policies allowing admins to require specific content to be synced locally or free up space when desired. To mitigate the risk of document inaccessibility, configure this policy to sync critical documents locally. Train users to manually apply the 'always keep on this device' setting for key documents.

<b>Microsoft 365 dependency</b>	<b>potential mitigations</b>
Communication of business disruptions to customers and suppliers rely on Exchange.	Public third-party social networks can be used as an alternative means of mass communication.
Hybrid on-premises architecture, such as ADFS or Pass Through Authentication, fails causing disruption to user's ability to authenticate to cloud services.	Configure <a href="#">Password Hash Sync</a> , in conjunction with your hybrid authentication services, as a secondary cloud-based authentication mechanism to avoid sign-in disruption during the outage. <a href="#">Refer to Create a Resilient Access Control Management Strategy with Microsoft Entra ID</a> for further information on building resilient authentication and access control architectures.

## Leveraging mobile app access

As mobile use has proliferated, there are new means to stay connected and Microsoft 365 mobile applications can be a key part of your resiliency strategy. Because they connect to cloud services over the cellular provider network, they aren't dependent on your organizations network infrastructure.

Let's use Outlook as an example. Users can Connect to their Exchange mailboxes over different network protocols (https or MAPI) depending on the email app being used. If there's a service incident that involves one of the protocols, say MAPI for instance which the desktop client uses, then your users can still get to their mailbox through the Outlook Mobile app or Outlook on the Web.

If you decide to allow users to connect to Microsoft 365 services via their mobile devices you can use Microsoft Intune to securely configure and manage those devices. Once the user accounts and devices are enrolled in your mobile management solution ensure that the apps have been downloaded and configured.

## Feedback

Was this page helpful?

Yes

No

# Microsoft 365 documentation navigation guide

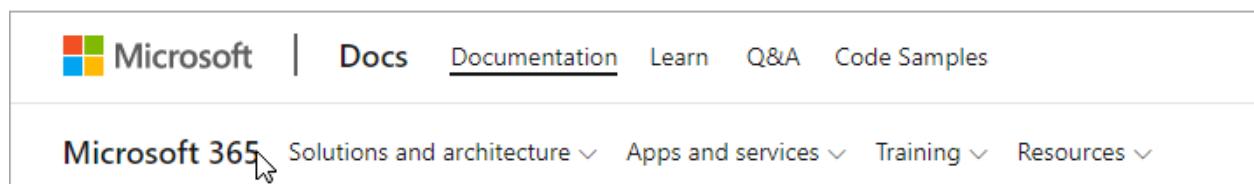
Article • 09/27/2022

This topic provides some tips and tricks for navigating the Microsoft 365 technical documentation space.

## Hub page

The Microsoft 365 hub page can be found at <https://aka.ms/microsoft365docs> and is the entry point for finding relevant Microsoft 365 content.

You can always navigate back to this page by selecting **Microsoft 365** from the header at the top of every page within the Microsoft 365 technical documentation set:



## TOC search

On Microsoft Learn, you can search the content in the table of contents by using the filter search box at the top:

A screenshot of the Microsoft Learn TOC search interface. At the top, there is a breadcrumb navigation: "Microsoft 365 / Solution and architecture illustrations /". Below this is a "Version" dropdown set to "Microsoft 365". Underneath the dropdown is a "Filter by title" input field with a dropdown arrow. When the arrow is clicked, a list of items appears: "Microsoft 365 solution and architecture center", "Solution and architecture illustrations", and "Microsoft 365 productivity illustrations".

## Version filter

The Microsoft 365 technical documentation provides content for additional products, including Office 365 Germany and Office 365 operated by 21 Vianet (China). Features can vary between these versions, and as such, sometimes the content itself can vary.

You can use the version filter to ensure that you are seeing content for the appropriate version of Microsoft 365:



## Breadcrumbs

Breadcrumbs can be found below the header and above the table of contents, and indicate where the current article is located in the table of contents. Not only does this help set the context to what type of content you're reading, but it also allows you to navigate back up the table of contents tree:



## Article section navigation

The right-hand navigation pane allows you to quickly navigate to sections within an article, as well as identify your location within the article.

Is this page helpful?

 Yes  No

## In this article

[Step 1: Set up multi-factor authentication and conditional access policies](#)

[Step 2: Configure Microsoft Defender for Identity](#)

[Step 3: Turn on Microsoft 365 Defender](#)

[Step 4: Configure Microsoft Defender for Office 365](#)

[Step 5: Configure Microsoft Defender for Endpoint](#)

[Step 6: Configure Microsoft Cloud App Security](#)

[Step 7: Monitor status and take actions](#)

[Step 8: Train users](#)

## Submit feedback

If you find something wrong within an article, you can submit feedback to the SQL Content team for that article by scrolling down to the bottom of the page and selecting [Content feedback](#).

### Feedback

Submit and view feedback for

[This product](#) 

[This page](#) 

## Contribute to Microsoft 365 documentation

Did you know that you could edit the content on Microsoft Learn yourself? If you do so, not only will our documentation improve, but you'll also be credited as a contributor to the page. To get started, see:

- Microsoft Docs contributor guide

## Next steps

- Get started with the [Microsoft 365 technical documentation](#).

# Microsoft 365 admin center help

Explore resources for working in the Microsoft 365 admin center.



WHAT'S NEW  
[What's new in the Microsoft 365 admin...](#)



HOW - TO ...  
[Stay on top of Microsoft 365 changes](#)



HOW - TO ...  
[Set up multifactor authentication](#)

## Get started

Set up your subscription and email, add users, and install apps.



### [Small business help & learning](#)

Explore all the Microsoft 365 help resources a small business needs.



### [YouTube - Microsoft 365 help for small businesses](#)

Learn how to set up and manage Microsoft 365 for your business with short videos.



### [Get started](#)

Sign up and set up Microsoft 365.



### [Install apps](#)

Install Microsoft 365 apps.



### [Migrate data](#)

Move your data from another service to Microsoft 365.

## Manage

Manage your subscription, services, and users, secure your business, and get help troubleshooting.

## [Overview of the Microsoft 365 admin center](#)

Learn about admin roles, how to stay on top of changes, and how to customize your subscription.

## [Users and groups](#)

Manage passwords, add and remove users, set up and manage groups, manage guest access, and assign user licenses.

## [Email and calendars](#)

Manage email settings, distribution groups, and security settings, and set up shared mailboxes.

## [Domains](#)

Learn about domains, set up and manage domains, and update DNS records.

## [Your data and service](#)

Monitor the status of your service, back up data, install add-ins, and upgrade to the latest apps.

## [Subscriptions and billing](#)

Manage bills, subscriptions, and product licenses, update payment methods, and purchase additional services and storage.

## [Work with customers](#)

Share documents and use Teams to collaborate and meet.

## [Troubleshoot](#)

Access resources to help you troubleshoot and fix problems with your Microsoft 365 products or services.