

# FastTrack for Microsoft 365 Benefit

Article • 05/28/2025

## What is FastTrack for Microsoft 365?

FastTrack for Microsoft 365 is a service designed to help organizations seamlessly deploy Microsoft 365 solutions to help users work effectively and productively. FastTrack provides remote guidance to help organizations learn, prepare, and deploy Microsoft 365 services quickly and efficiently.

To effectively deploy Microsoft 365, Microsoft Viva, and security services, FastTrack uses step-by-step deployment guides. These guides simplify the deployment process and help organizations use Microsoft 365 services as quickly as possible.

FastTrack works with a network of certified partners who provide expertise in deploying Microsoft 365 solutions. These partners help organizations navigate the deployment process, customize the approach to meet your specific needs, and provide further support to ensure successful adoption to drive effective utilization of your services. These services are determined on a case-by-case basis according to your specific requirements.

With FastTrack, organizations can use the full power of Microsoft 365, including Microsoft Teams, Microsoft Viva, and Microsoft 365 security services. By following the deployment guides and working with certified partners, organizations can quickly and easily deploy Microsoft 365 and help their users collaborate.

FastTrack offers assistance in the following languages: English, French, German, Italian, Japanese, Korean, Portuguese (Brazil), Spanish, Traditional Chinese, and Simplified Chinese (resources speak Mandarin only).

### Note

Since FastTrack guidance is tailored to you and your environment, your experience might be impacted if you choose to deploy outside of this guidance.

## How to use this service description

The FastTrack service description is designed to help business stakeholders and IT teams understand the FastTrack benefit and answer key questions, including: What purchases are eligible? How to get help? What can I expect of FastTrack? What obligations do I have? How does the engagement work? What about data migration?

To facilitate these questions, the service description is broken into four sections:

- [Eligibility](#) – Understand if your purchase is eligible for FastTrack assistance and identify the Microsoft 365 services covered by FastTrack Specialists.
- [Process and Expectations](#) – Learn how to engage FastTrack for assistance, get an overview of how that assistance is provided, receive tips for a successful experience, and understand key responsibilities of both FastTrack and your company.
- [Products and Capabilities](#) – Gain information on the specific guidance FastTrack provides for each Microsoft 365 product or capability and our expectations for your source environment before the start of work.
- [Data Migration](#) – Understand the type of data FastTrack migrates into your Microsoft 365 environment and specifics around the process and limitations.

# Eligibility

Article • 04/30/2025

FastTrack assistance is available for customer tenants with 150 or more licenses from one of the eligible plans from the following Microsoft product families: Microsoft 365, Office 365, Microsoft Viva, Enterprise Mobility & Security, and Windows 10/11. These plans can be for an individual product (like Exchange Online) or a suite of products (Office 365 E3). Because Microsoft provides many purchasing options, the list of eligible plans is extensive and is found in [Eligible plans](#).

## Products and capabilities covered

FastTrack can provide you with remote, guided assistance for the following services that might be included with your purchased plan:

- Microsoft Entra
- Exchange Online
- Microsoft 365 Apps

### ⓘ Note

Office 365 ProPlus has been renamed to Microsoft 365 Apps. In some cases, you might find uses of the legacy name. For details of when this change takes effect, please see [Name change for Office 365 ProPlus](#).

### ⓘ Note

Multiple Microsoft Purview branding changes have been made, including:

- Microsoft Information Governance is now Microsoft Purview Data Lifecycle Management and Records Management.
- Microsoft Information Protection is now Microsoft Purview Information Protection.
- Microsoft eDiscovery is now Microsoft Purview eDiscovery.
- Microsoft Audit is now Microsoft Purview Audit.
- Microsoft Insider Risk Management is now Microsoft Purview Insider Risk Management and Communication Compliance.

- Microsoft 365 Copilot
- Microsoft Defender XDR
- Microsoft Defender for Cloud Apps

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Edge
- Microsoft Intune
- Microsoft Intune Suite (including all add-ons, Endpoint Privilege Management (EPM), Enterprise Application Management, Remote Help, Microsoft Tunnel for Mobile App Management (Tunnel for MAM), Advanced Analytics, management of specialty devices, and Firmware-Over-The-Air (FOTA) updates)
- Microsoft Purview Audit
- Microsoft Purview Data Lifecycle Management and Purview Records Management
- Microsoft Purview eDiscovery
- Microsoft Purview Information Protection
- Microsoft Purview Insider Risk Management and Communication Compliance
- Microsoft Sentinel
- Microsoft Teams (including Teams Core enablement, Teams Meetings and events, Teams Phone, Teams Rooms, and Teams Premium)
- Microsoft Viva
- Microsoft OneDrive
- Microsoft SharePoint
- Windows 10/11
- Windows 365

## Eligible plans

You must purchase at least 150 licenses per tenant from one of the following plans to be eligible for FastTrack. The list is based on product family to help facilitate you finding the specific plans purchased by your company: Microsoft 365, Office 365, Enterprise Mobility & Security, and Windows 10/11.

## Microsoft 365 plans

### Microsoft 365 Enterprise

- Microsoft 365 E3\*
- Microsoft 365 E5\*
- Microsoft 365 E5 Security\*
- Microsoft 365 E5 Compliance\*
- Microsoft 365 E5 Purview eDiscovery & Purview Audit\*
- Microsoft 365 E5 Purview Information Protection & Purview Data Lifecycle Management \*

- Microsoft 365 E5 Purview Insider Risk Management\*
- Microsoft 365 F1\*
- Microsoft 365 F3\*
- Microsoft 365 F5 Security\*
- Microsoft 365 F5 Compliance\*
- Microsoft 365 F5 Security & Compliance\*
- Microsoft 365 US Government G3\*\*
- Microsoft 365 US Government G5\*\*
- Microsoft 365 Apps for Enterprise\*
- Microsoft 365 Apps for Enterprise (device)\*

## Microsoft 365 Business

- Microsoft 365 Business Basic\*
- Microsoft 365 Business Standard\*
- Microsoft 365 Business Premium\*
- Microsoft 365 Apps for Business\*

## Microsoft 365 Education

- Microsoft 365 A3\*
- Microsoft 365 A5\*
- Microsoft 365 A5 Security\*
- Microsoft 365 A5 Compliance\*
- Microsoft 365 A5 Purview eDiscovery & Purview Audit\*
- Microsoft 365 A5 Purview Information Protection & Purview Data Lifecycle Management\*
- Microsoft 365 A5 Purview Insider Risk Management\*
- Microsoft 365 Apps for Education (device)\*

## Microsoft 365 Copilot

- Microsoft 365 Copilot

### Note

In addition to 150 eligible paid licenses required for FastTrack services, you need at least one Microsoft 365 Copilot license to qualify for FastTrack assistance with your Microsoft 365 Copilot deployment.

# Office 365 plans

## Office 365 Enterprise

- Office 365 Enterprise E1
- Office 365 Enterprise E3
- Office 365 Enterprise E4
- Office 365 Enterprise E5
- Office 365 Enterprise F3
- Office 365 US Government G1\*\*
- Office 365 US Government G3\*\*
- Office 365 US Government G4\*\*
- Office 365 US Government G5\*\*
- Office 365 US Government F3\*\*

## Office 365 Education\*\*

- Office 365 A3
- Office 365 A5

## Exchange Online

- Exchange Online Plan 1
- Exchange Online Plan 2
- Exchange Online Kiosk
- Exchange Online Protection
- Microsoft Defender for Office 365

## Microsoft Teams

- Teams Phone
- Calling Plan
- Audio Conferencing
- Teams Rooms\*\*\*\*
- Teams Phone for India
- Teams Premium

## Microsoft Viva

- Viva Suite

- Viva Workplace Analytics and Employee Feedback (including Viva Insights Premium, Viva Pulse, and Viva Glint)
- Viva Employee Communications and Communities (including Viva Amplify, Viva Connections Premium, Viva Engage Premium, and Answers in Viva)
- Viva Learning
- Viva Insights
- Viva Goals
- Viva Connections
- Viva Engage
- Viva Glint

**ⓘ Note**

Viva Goals will be retired on December 31, 2025.

150 paid Microsoft 365 licenses are required for FastTrack assistance on Viva Connections, Viva Engage, Viva Insights, and Viva Learning seeded features. In addition to 150 eligible paid licenses, you need at least 150 paid Microsoft Viva add-on licenses to qualify for FastTrack assistance for deployment of premium Viva features.

## OneDrive

- OneDrive for business with Office Online
- OneDrive for business Plan 1
- OneDrive for business Plan 2

## SharePoint

- SharePoint Plan 1
- SharePoint Plan 2

\*Available only for FastTrack-eligible cloud services and features described in this benefit description.

\*\*For more information about US Government assistance, see [Office 365 US Government - Service Descriptions | Microsoft Learn](#).

\*\*\*\* Minimum license requirement for Teams Rooms assistance is 150 Microsoft Teams licenses. There are no minimum required Teams Rooms licenses.

# Enterprise Mobility + Security plans

## Enterprise Mobility + Security

- Enterprise Mobility + Security (EMS) E3\*\*\*
- Enterprise Mobility + Security (EMS) E5\*\*\*

## Microsoft Entra

- Microsoft Entra ID P1
- Microsoft Entra ID P2
- Microsoft Entra ID Governance
- Microsoft Entra Suite
- Microsoft Entra Private Access
- Microsoft Entra Internet Access

### Note

In addition to 150 eligible Microsoft Entra ID P1 or P2 paid licenses required for FastTrack services, you need at least one of the following to qualify for FastTrack assistance with Microsoft Entra Global Secure Access deployments: 25 Microsoft Entra Suite paid licenses, 25 Microsoft Entra Internet Access paid licenses, or 25 Microsoft Entra Private Access paid licenses.

## Microsoft Purview Information Protection

- Microsoft Purview Information Protection

## Microsoft Intune

- Microsoft Intune

## Microsoft Intune and Configuration Manager

- Microsoft Intune and Configuration Manager

## Microsoft Intune for Education

- Microsoft Intune for Education



## Microsoft Intune Suite

- Microsoft Intune Suite
- Endpoint Privilege Management
- Enterprise Application Management
- Advanced Analytics
- Remote Help
- Microsoft Tunnel for Mobile Application Management
- Microsoft Cloud PKI
- Microsoft Intune Plan 2 features
  - Firmware-Over-The-Air updates
  - Specialized devices management

### Note

In addition to 150 eligible Microsoft Intune paid licenses required for FastTrack services, you need at least one Intune Suite or Intune Suite add-on license (purchased or trial) to qualify for FastTrack assistance with Intune Suite and its add-ons deployment.

\*\*\*Available for cloud services that are eligible for FastTrack benefits. Cloud services not eligible are routed to a FastTrack Specialist or partner referral.

## Windows 10/11 plans

### Windows Enterprise

- Windows 10/11 E3
- Windows 10/11 E5
- Windows 10 Enterprise with Software Assurance

### Windows Education

- Windows 10/11 A3
- Windows 10/11 A5

### Note

There's no minimum licensing requirement for commercial independent software vendors (ISVs) building Windows 10/11 apps. All app requests must be targeting a Windows 10/11

or Microsoft 365 Apps version that is currently within the mainstream servicing window.

## Windows 365


- Windows 365 Enterprise
- Windows 365 Frontline
- Windows 365 Government

### Note

In addition to 150 eligible paid licenses required for FastTrack services, you need at least one Windows 365 license (purchased or trial) to qualify for FastTrack assistance with your Windows 365 deployment.

## Ineligible plans

Plans not eligible for FastTrack services include (but aren't limited to):

 Expand table

Plan	Details
Exchange Online Archiving	FastTrack guidance for this plan is available when obtained through an eligible plan, like Enterprise E3 and E5.
Office 365 operated by 21Vianet	For more information on the FastTrack Benefit for Office 365 operated by 21Vianet, contact <a href="#">21Vianet support</a> .
Microsoft Office 365 Dedicated and ITAR/Federal Plans	
No-cost plans (like Office 365 A1 or the student use benefit plan)	

# Process and Expectations

06/06/2025

In this article, we explain how to engage FastTrack for assistance, what to expect from the process, and provide tips for a successful experience. FastTrack provides guidance about moving to and using Microsoft 365. You'll receive documented guidance and best practices on planning a successful rollout.

## Engaging FastTrack


### ⓘ Note

If you're currently working with a FastTrack Ready partner, you can contact them directly for any new FastTrack engagements. A FastTrack Request for Assistance (RFA) isn't required.


FastTrack assistance can be requested in the following ways:

- Through the Microsoft 365 admin center – Your tenant admin signs into the admin center and then requests assistance there.
- Through the Microsoft 365 Setup site – You sign in to request assistance for your organization. A Microsoft 365 tenant admin review is required after submission.

To request assistance directly through the Microsoft 365 admin center:

1. Sign in to the [admin center](#) .
2. Select **Advanced deployment guides & assistance** from the **Training, guides, & assistance** card on the landing page.
3. Select **FastTrack assistance**.
4. Select **Submit a new request**.
5. Complete the **FastTrack request for deployment assistance** form.

To request assistance directly through the Microsoft 365 Setup site:

1. Sign in to the [Microsoft 365 Setup site](#) .
2. Select **Submit a new request**.
3. Complete the **FastTrack request for deployment assistance** form.

### ⓘ Note

Your organization's Microsoft 365 tenant admin is notified and must review the submitted request for assistance (RFA) form within 30 days or the request expires.

**ⓘ Note**

For a list of FastTrack Ready approved partners, see [FastTrack Ready approved partners](#) <sup>↗</sup>.

To request assistance for FastTrack for Azure, submit a request with [FastTrack for Azure](#) <sup>↗</sup>.

To request assistance for App Assure, complete the [App Assure service request](#) <sup>↗</sup>. The following products are in scope for App Assure assistance:

- Azure Virtual Desktop
- Microsoft 365 Apps
- Microsoft Edge
- Windows 10/11
- Windows 365

## FastTrack expectations

### Customer success tips

Your preparation for FastTrack's assistance is vital to a smooth and successful process. Before engaging with FastTrack, be sure to establish:

- The desired start date for your FastTrack engagement.
- The planned deployment date for the services.
- The business reason (why you plan to launch the service to users).
- The success owners (who is responsible for the success of the project).

We also recommend you consider and identify the following personnel:

- Stakeholders – Recruit and empower executive sponsors and champions.
- Scenarios – Prioritize and define success criteria.
- Awareness – Implement a communication campaign and plan the launch event.
- Training – Educate end users and prepare helpdesk resources.

# Products and Capabilities


Article • 10/02/2024


## Overview

Every customer has a unique source environment. To ensure a successful onboarding experience, it's vital for customer expectations to be explained before we begin.

Based on each customer's current setup, a FastTrack Specialist works to create a remediation plan that brings the customer source environment up to the minimum requirements for successful onboarding. All supported Microsoft 365 products have different requirements. Review the requirements provided for each before beginning deployment.

## Getting started

FastTrack provides deployment guidance for Microsoft 365 products and services through various deployment channels. When a customer submits a [request for assistance](#) , that request is reviewed to determine the best method of assistance. These guidelines include:

- [Microsoft 365 advanced deployment guides](#) – Tailored guidance and resources for planning and deploying your tenant, apps, and services.
- [Partner assistance](#)  – Dedicated FastTrack Partners that assist with deployment of Microsoft 365.
- Internal resources – FastTrack Subject Matter Experts (SMEs) and Engineers that assist with deployment of Microsoft 365.

## Supported products and capabilities

FastTrack Specialists provide remote guidance first for core capabilities (common for all Microsoft Online Services) and then onboarding of each eligible service.

These guidelines include:

- [Microsoft Entra](#)
- [Microsoft Intune](#)
- [Microsoft Defender](#)
- [Microsoft Purview](#)
- [Microsoft Viva \(Employee Experiences\)](#)

- [Office 365](#)
- [Windows and Other Services](#)

## FastTrack core onboarding

FastTrack provides remote guidance for core onboarding, which involves service provisioning, tenant configuration, and identity integration. It also includes steps for providing a foundation for onboarding services like Exchange Online, SharePoint, and Microsoft Teams, including a [discussion on security, network connectivity, and compliance](#).

Onboarding for one or more eligible services can begin once core onboarding is finished.

## Network enablement

As part of the FastTrack benefit, we advise connecting to Microsoft 365 cloud services to ensure the highest levels of performance of Microsoft 365. Active Directory forests have the functional forest level set to Windows Server 2003 onward, with the following forest configuration:

- A single Active Directory forest.
- A single Active Directory account forest and resource forest (Exchange, Lync 2013, or Skype for Business) topologies.
- Multiple Active Directory account forests and resource forest (Exchange, Lync 2013, or Skype for Business) topologies.
- Multiple Active Directory account forests with one of the forests being a centralized Active Directory account forest that includes Exchange, Lync 2013, or Skype for Business.
- Multiple Active Directory account forests, each with its own Exchange organization.
- Tasks required for tenant configuration and integration with Microsoft Entra ID, if needed.

### Important

- For multi-forest Active Directory scenarios, if Lync 2013 or Skype for Business is deployed, it must be deployed in the same Active Directory forest as Exchange.
- When implementing multiple Active Directory forests with multiple Exchange organizations in an Exchange multi-hybrid configuration, shared user principal

name (UPN) namespaces between source forests aren't supported. Primary SMTP namespaces between Exchange organizations should also be separated. For more information, see [Hybrid deployments with multiple Active Directory forests](#) <sup>↗</sup>.

- Active Directory Federation Services (AD FS) deployment is out of scope. Contact a [Microsoft Partner](#) <sup>↗</sup> for assistance with this.

## Out of scope for all products and capabilities

- On-site support.
- Project management of the customer's remediation activities.
- Ongoing management, threat response, and remediation.
- Security information and event management (SIEM) or API integration.
- Troubleshooting issues encountered during engagement (including devices that fail to onboard).
- Ongoing management and threat response.
- Management of break/fix issues related to already deployed services.
- Custom scripting and coding.
- Design, architect, and third-party document review.
- Tenant to Tenant migration.

## Microsoft advanced deployment guides

Microsoft provides customers with technology and guidance to assist with deploying your Microsoft 365, Microsoft Viva, and security services. We encourage our IT pro customers to start their deployment journey with [these](#) <sup>↗</sup> offerings.

For all non-IT pro customers, see **\*\*Microsoft 365 Setup** <sup>↗</sup>.

## Further support

Microsoft-approved Partners can provide support with out-of-scope services, including:

- [FastTrack for Azure – Technical Enablement FAQ | Microsoft Azure](#) <sup>↗</sup>.
- [Break/Fix help](#) <sup>↗</sup>.
- [Microsoft Unified Overview | Microsoft Unified](#) <sup>↗</sup>.

## US Government assistance

For more information about Us Government assistance, see [Office 365 US Government - Service Descriptions | Microsoft Learn](#).

---

## Feedback

Was this page helpful?



Yes



No

[Provide product feedback](#) 



# Microsoft 365 Copilot

Article • 04/30/2025

## Microsoft 365 Copilot

Microsoft 365 Copilot is an AI-powered assistant that uses large language models (LLMs). It integrates with your data, with Microsoft Graph, and with Microsoft 365 Apps, like Word, Excel, PowerPoint, Outlook, Microsoft Teams, and more. Microsoft 365 Copilot provides real-time intelligent assistance, enabling users to enhance their creativity, productivity, and skills. FastTrack deployment assistance for Microsoft 365 Copilot helps customers with license assignment, adoption, extending Microsoft 365 Copilot, and measuring the impact and business value of Microsoft 365 Copilot.

FastTrack provides remote guidance and best practices for:

- Readiness, including:
  - Ensuring required products and features are enabled for an optimized experience.
  - Moving Microsoft 365 Apps to a supported update channel.
  - Configuring Copilot settings in the Microsoft 365 Admin Center.
  - Providing guidance on data governance with reporting, SharePoint Advanced Management, and Microsoft Purview.
  - Setting up [Microsoft 365 Copilot Chat](#) for non-Microsoft 365 Copilot licensed users.
- Adoption, including:
  - Reviewing Microsoft 365 Copilot license assignments.
  - Using the [Copilot Success Kit](#) [↗](#) to highlight the foundational components of successful adoption.
  - Providing guidance on available resources for training and skilling.
  - Reviewing Copilot Dashboard to understand usage and value.
  - Using [Microsoft Viva](#) apps to accelerate enablement.
- [Microsoft 365 Copilot extensibility](#).
- Measurement of adoption and impact, including:
  - Explaining the Copilot Control System, including IT admin controls and reporting capabilities to understand usage and business value.
  - Setting up [Microsoft 365 Copilot Analytics](#), including Copilot Dashboard and Copilot Reports in Viva Insights Analyst Workbench, specifically the Copilot business outcome report.

## Out of scope

- Providing project management and implementation.

- Creating and implementing an adoption and change management strategy or plan.
- Providing end-user training
- Providing data governance assessment.
- Providing custom scenarios or content (like communications or training materials).

## Microsoft 365 Copilot Chat

Microsoft 365 Copilot Chat is an AI-powered tool that enhances work efficiency by providing intelligent assistance within the Microsoft 365 ecosystem. It uses advanced machine learning to offer personalized recommendations, automate tasks, and analyze data. This tool integrates with various Microsoft 365 applications, helping users streamline workflows and boost productivity. Intuitive interface and real-time support make it an essential tool for modern workplaces.

FastTrack provides remote guidance for:

- Readiness and deployment, including:
  - Meeting technical prerequisites for Copilot Chat.
  - Managing user access and permissions for control and security.
  - Pinning Copilot Chat for easy access.
  - Setting up web grounding for secure use.
- Adoption and value, including:
  - Using the Copilot Chat and agent starter kit for key adoption steps.
  - Offering resources to train users on Copilot Chat.
  - Recommending strategies to maximize benefits and drive usage.
  - Reviewing usage scenarios and reports to monitor patterns.

## Out of scope

- Providing project management and implementation.
- Creating and implementing an adoption and change management strategy or plan.
- Providing end user training.
- Providing custom scenarios or content creation.
- Providing data governance assessment.
- Setting up consumption licensing, like Microsoft Copilot Studio pay-as-you-go.

## Microsoft 365 Copilot extensibility

Microsoft 365 Copilot extensibility empowers organizations to integrate AI capabilities directly into their workflows, driving productivity and innovation through tailored solutions.

Additionally, FastTrack offers advanced deployment guides to accelerate the successful implementation of Copilot extensibility.

FastTrack provides remote guidance for:

- Deploying Copilot agents.
- Configuring Microsoft Graph connectors.
- Setting up first-party Microsoft Graph connectors.
- Implementing data protection and management controls.
- Measuring and reporting on Copilot extensibility usage.
- Deploying declarative agents with Microsoft 365 Copilot Chat.
- Deploying SharePoint agents with Copilot chat.
- Setting up Copilot Control System for Copilot extensibility.

## Out of scope

- Providing project management and implementation.
- Creating and implementing an adoption and change management strategy or plan.
- Providing end user training.
- Creating custom agents.
- Providing data governance assessment.

## Microsoft 365 Copilot Analytics

Microsoft 365 Copilot Analytics is designed to empower every IT and business leader to measure adoption and business impact of Copilot and agents — with Microsoft Copilot Dashboard and customizable reporting for deeper analysis against your key performance indicators (KPIs).

FastTrack provides remote guidance for:

- Assigning licenses and roles.
- Configuring personal insights features.
- Configuring Microsoft Copilot Dashboard.
- Configuring the Microsoft Viva Insights admin portal (Analyst Workbench).
- Uploading the organizational data file.
- Surveying data uploads for Copilot sentiment analysis in the Microsoft Copilot Dashboard
- Surveying business data uploads for the Copilot business outcome report.
- Enabling the Microsoft Power BI templates in the Viva Insights portal.
- Creating queries in the Viva Insights portal.
- Enabling, installing, and pinning the Viva Insights Teams app.

## Out of scope

- Interpreting or analyzing data in Viva Insights reports or query results.
- Developing custom reports.
- Third-party integrations.
- Project management (including defining success criteria).
- Adoption and change management activities.

## Microsoft advanced deployment guides

Microsoft provides customers with technology and guidance to assist with deploying your Microsoft 365, Microsoft Viva, and security services. We encourage our customers to start their deployment journey with [these](#) offerings.

For non-IT admins, see [All Microsoft 365 guides](#).

### Note

For comprehensive deployment and adoption support of Copilot for Microsoft 365, customers can engage the [Microsoft partner network](#).

# Microsoft Defender

Article • 05/28/2025

## Zero Trust

FastTrack provides comprehensive guidance on implementing Zero Trust security principles. The Zero Trust model assumes breach and verifies each request as though it originates from an uncontrolled network. This approach ensures robust security across your networks, applications, and environment. FastTrack accomplishes this by focusing on identity, devices, applications, data, infrastructure, and networks. With FastTrack, you can confidently advance your Zero Trust security journey and protect your digital assets effectively.

With Microsoft Defender, you can implement Zero Trust principles by providing extended detection and response (XDR) capabilities. This includes automatically collecting, correlating, and analyzing signal, threat, and alert data from across your Microsoft 365 environment, including endpoints, email, applications, and identities. By integrating with Microsoft Sentinel, you can create a comprehensive XDR and security information and event management (SIEM) solution that enhances your organization's security posture.

## Microsoft Defender XDR

Microsoft Defender XDR is a unified pre- and post-breach enterprise defense suite. Defender XDR natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and apps to provide integrated protection against sophisticated attacks.

FastTrack provides remote guidance for:

- Providing an overview of the Microsoft Defender portal.
  - Providing an overview of cross-product incidents, including focusing on what's critical by ensuring the full attack scope, impacted assets, and automated remediation actions that are grouped together.
  - Demonstrating how Microsoft Defender XDR can orchestrate the investigation of assets, users, devices, and mailboxes that become compromised through automated self-healing.
  - Explaining and providing examples of how customers can proactively hunt for intrusion attempts and breach activity affecting your email, data, devices, and accounts across multiple data sets.
  - Showing customers how they can review and improve their security posture holistically using Microsoft Secure Score.
- Provide education and configuration guidance on Unified Security Operations Platform.
  - Connecting of a Microsoft Sentinel workspace.

- Review of the following capabilities within the Defender portal.
  - Search.
  - Threat management.
  - Content management.
  - Configuration.
- Provide education and configuration guidance on Defender XDR Attack Disruption capabilities.

## Out of scope

- Deployment guidance or education on:
  - How to remediate or interpret the various alert types and monitored activities.
  - How to investigate a user, computer, lateral movement path, or entity.
  - Custom threat hunting.
- Security information and event management (SIEM) or API integration.
- Preview features.

## Microsoft Defender for Cloud Apps

Microsoft Defender for Cloud Apps is a multi-purpose software-as-a-service (SaaS) security solution. It combines SaaS security posture management, data loss prevention, app-to-app protection, and integrated threat protection to ensure holistic coverage for your apps. By adopting a SaaS security approach, you can easily identify misconfigurations. This improves your overall app posture, implements policies to protect sensitive data, and protects app-to-app scenarios to ensure that only apps have the acceptable permissions to access other app data. When you natively integrate into Microsoft Defender XDR, organizations like yours benefit from using the signal from SaaS to actively hunt in their environments and combat incidents across their apps, devices, identities, and email.

FastTrack provides remote guidance for:

- Configuring the portal, including:
  - Importing user groups.
  - Managing admin access and settings.
  - Scoping your deployment to select certain user groups to monitor or exclude from monitoring.
  - How to set up IP ranges and tags.
  - Personalizing the end-user experience with your logo and custom messaging.
- Integrating first-party services including:
  - Microsoft Defender for Endpoint.
  - Microsoft Defender for Identity.

- Microsoft Entra ID Protection.
- Microsoft Purview Information Protection.
- Setting up cloud discovery using:
  - Microsoft Defender for Endpoints.
  - Zscaler.
  - iboss.
- Creating app tags and categories.
- Customizing app risk scores based on your organization's priorities.
- Sanctioning and unsanctioning apps.
- Reviewing the Defender for Cloud Apps and Cloud Discovery dashboards.
- Enabling app governance.
  - Guide the customer through the overview page and create up to five (5) app governance policies.
- Connecting featured apps using app connectors.
- Protecting apps with Conditional Access App Control in the Conditional Access within Microsoft Entra ID and Defender for Cloud Apps portals.
- Deploying Conditional Access App Control for featured apps.
- Reviewing SaaS Security Posture Management (SSPM) capabilities in Secure Score recommendations for available apps.
- Using the activity and file logs.
- Managing OAuth apps.
- Reviewing and configuring policy templates.
- Providing configuration assistance with the top SaaS use cases (including the creation or updating of up to six (6) policies).
- Understanding incident correlation in the Microsoft Defender portal.
- Creating a Cloud Discovery snapshot report.

## Out of scope

- Discussions comparing Defender for Cloud Apps to other Cloud Access Security Broker (CASB) or SaaS security offerings.
- Configuring Defender for Cloud Apps to meet specific compliance or regulatory requirements.
- Deploying the service to a nonproduction test environment.
- Deploying Cloud App Discovery as a proof of concept.
- Setting up the infrastructure, installation, or deployment of automatic log uploads for continuous reports using Docker or a log collector.
- Supporting custom log parsers, including:
  - Unsupported formats.
  - Normalizing their logs.

- Providing guidance on how to download their logs.
- Blocking app usage using block scripts.
- Adding custom apps to Cloud Discovery.
- Connecting custom apps with Conditional Access App Control.
- Onboarding and deploying Conditional Access App Control for any app.
- Integrating with non-Microsoft identity providers (IdPs) and data loss prevention (DLP) providers.
- Training or guidance covering advanced hunting.
- Automated investigation and remediation including Microsoft Power Automate playbooks.
- SIEM or API integration (including Microsoft Sentinel).

## Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is a platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

FastTrack provides remote guidance for:

- Assessing the OS version and device management approach (including Microsoft Intune, Microsoft Endpoint Configuration Manager, Group Policy, and non-Microsoft configurations) as well as the status of your endpoint security software.
- Onboarding Microsoft Defender for Endpoint P1 and P2 using:
  - Local script.
  - Group Policy.
  - Intune.
  - Configuration Manager.
  - Defender for Endpoint security settings management.
- Providing recommended configuration guidance for Microsoft traffic to travel through proxies and firewalls, restricting network traffic for devices that aren't able to connect directly to the internet.
- Enabling the Defender for Endpoint service by explaining how to deploy an endpoint detection and response (EDR) agent profile using one of the supported management methods.
- Deployment guidance, configuration assistance, and education on:
  - Vulnerability management core features.
  - Attack surface reduction capabilities, including:
    - Attack surface reduction rules.
    - Controlled folder access.
    - Device control for removable media devices.
    - Network protection.



- Next-generation protection.
- Endpoint detection and response.
- Automated investigation and remediation.
- Secure score for devices.
- Microsoft Defender SmartScreen configuration using Intune.
- Device discovery.<sup>1</sup>
- Reviewing simulations and tutorials (like practice scenarios, fake malware, and automated investigations).
- Overview of reporting and threat analytics features.
- Integrating Microsoft Defender for Office 365, Microsoft Defender for Identity, and Defender for Cloud Apps with Defender for Endpoint.
- Conduct walkthroughs of the Microsoft Defender portal.
- Onboarding and configuration of the following operating systems:<sup>4</sup>
  - Windows 10/11, including Windows 365 Cloud PCs.
  - Windows Server 2012 R2.<sup>2</sup>
  - Windows Server 2016.<sup>2</sup>
  - Windows Server 2019.<sup>2</sup>
  - Windows Server 2022.<sup>2</sup>
  - Windows Server 2019 Core Edition.<sup>2</sup>
  - Supported macOS versions.
  - Supported Linux server distributions.
  - Android.<sup>3</sup>
  - iOS.<sup>3</sup>

<sup>1</sup> Only some aspects of device discovery are supported. For more information, see the following **Out of scope** section.

<sup>2</sup> Windows Server 2012 R2 and 2016 support is limited to onboarding and configuration of the unified agent.

<sup>3</sup> For more information, see the following **Out of scope** section for mobile threat defense details.

<sup>4</sup> For more information about integrating Defender for Endpoint with Microsoft Defender for Servers, see [Microsoft Defender for Cloud](#).

## Out of scope

- Onboarding and enablement guidance for preview features.
- Troubleshooting issues encountered during engagement (including devices that fail to onboard). FastTrack directs customers to Microsoft Support for assistance.
- Supporting Microsoft Defender for Business.

- Onboarding or configuration for the following Defender for Endpoint agents:
  - Windows Server 2008 R2.
  - Windows 7.
  - Windows 8.
  - Any operating system or device type not supported by Defender for Endpoint.
  - Linux distributions not supported by Defender for Endpoint.
  - Linux instances using customized kernels.
  - Windows Subsystem for Linux (WSL).
  - Virtual Desktop Infrastructure (VDI) (persistent or non-persistent), including Azure Virtual Desktop and non-Microsoft VDI solutions.
- Server onboarding and configuration.
  - Configuring a proxy server for offline communications.
  - Configuring Configuration Manager deployment packages on down-level Configuration Manager instances and versions.
  - Servers not managed by Configuration Manager or Defender for Endpoint security settings management.
- Linux server onboarding and configuration.
  - Prescriptive assistance with any non-Microsoft systems management tools or products (including development of configuration files associated with them), including:
    - Chef
    - Puppet.
    - Ansible.
    - Saltstack.
  - FastTrack refers customers to applicable technical guidance whenever possible.
- macOS onboarding and configuration.
  - JAMF-based deployment.
  - Other mobile device management (MDM) product-based deployment.
  - Manual deployment.
- Mobile threat defense onboarding and configuration (Android and iOS).
  - Unmanaged bring your own devices (BYOD) or devices managed by other enterprise mobility management systems.
  - Set up app protection policies (like mobile app management (MAM)).
  - Android devices.
  - Admin-enrolled devices.
  - Assistance with coexistence of multiple VPN profiles.
  - Onboarding devices to Intune. For more information on onboarding assistance, see [Microsoft Intune](#).
- Configuration of the following attack surface reduction capabilities:
  - Hardware-based application and browser isolation (including Application Guard).
  - Application control, including AppLocker and Windows Defender Application Control.
  - The following device control functions:

- Device installation restrictions.
- Data protection.
- Storage.
- Windows Portable Devices (WPD) removable storage access.
- Connectivity.
- Bluetooth.
- Direct Memory Access (DMA) guard.
- Exploit protection.
- Network and endpoint firewalls.
- Configuration or management of account protection features like:
  - Credential Guard.
  - Local user group membership.
- Configuration or management of BitLocker.

#### ⓘ Note

For information on BitLocker assistance with Windows 11, see [Windows 11](#).

- Configuration or management of network device discovery.
- Configuration or management of the following device discovery capabilities:
  - Onboarding of unmanaged devices not in scope for FastTrack (like Linux).
  - Configuring or remediating internet-of-things (IoT) devices including vulnerability assessments of IoT devices through Defender for IoT.
  - Integration with non-Microsoft tooling.
  - Exclusions for device discovery.
  - Preliminary networking assistance.
  - Troubleshooting network issues.
- Attack simulations (including penetration testing).
- Enrollment or configuration of Microsoft Threat Experts.
- Configuration or training guidance for API or SIEM connections.
- Training or guidance covering advanced hunting.
- Training or guidance covering the use of or creation of Kusto queries.
- Training or guidance covering Defender SmartScreen configuration using Group Policy Objects (GPOs), Windows Security, or Microsoft Edge.
- Defender Vulnerability Management Add-on.
- Defender Vulnerability Management Standalone.

Contact a [Microsoft Partner](#)  for assistance with these services.

## Microsoft Defender for Identity

Microsoft Defender for Identity is a cloud-based security solution. It uses your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

FastTrack provides remote guidance for:

- Running the sizing tool for resource capacity planning.
- Creating your instance of Defender for Identity.
- Configuring Windows event collection across Active Directory Domain Services (AD DS), Active Directory Federation Services (AD FS), and Active Directory Certificate Services (AD CS).
- Managing admin access with role groups.
- Downloading, deploying, and configuring the sensor on your Active Directory domain controllers for both single and multiple forest environments.
- Creating and configuring directory service accounts or managed action accounts in Active Directory including group managed service accounts (gMSA).
- Downloading, deploying, and configuring the sensor on your AD FS servers.
- Portal configuration, including:
  - Tagging sensitive accounts, devices, or groups.
  - Email notifications for health issues and security alerts.
  - Alert exclusions.
  - Scheduled reports.
- Providing deployment guidance, configuration assistance, and education on:
  - Identity Security Posture Assessment reports within Microsoft Secure Score.
  - User Investigation Priority Score and User Investigation ranking reports.
  - Inactive user reports.
  - Remediation options on a compromised account.
- Facilitating the migration from Advanced Threat Analytics (ATA) to Defender for Identity (if applicable).

## Out of scope

- Deploying Defender for Identity as a proof of concept.
- Deploying or performing the following Defender for Identity sensor activities:
  - Manual capacity planning.
  - Deploying the standalone sensor.
  - Deploying the unified sensor (in preview).
  - Deploying the sensor using a Network Interface Card (NIC) Teaming adaptor.
  - Deploying the sensor through a non-Microsoft tool.
  - Connecting to the Defender for Identity cloud service through a web proxy connection.
- Creating and configuring permissions for the AD FS database.

- Creation and management of honeytokens accounts or devices.
- Enabling Network Name Resolution (NNR).
- Enabling and configuration of the Deleted Objects container.
- Deployment guidance or education on:
  - Remediating or interpreting various alert types and monitored activities.
  - Investigating a user, computer, lateral movement path, or entity.
  - Threat or advanced hunting.
  - Incident response.
- Providing a security alert lab tutorial for Defender for Identity.
- Providing notification when Defender for Identity detects suspicious activities by sending security alerts to your syslog server through a nominated sensor.
- Configuring Defender for Identity to perform queries using security account manager remote (SAMR) protocol to identify local admins on specific machines.
- Configuring VPN solutions to add information from the VPN connection to a user's profile page.
- SIEM or API integration (including Microsoft Sentinel).

## Source environment expectations

- Aligned with Defender for Identity prerequisites.
- Active Directory, AD FS, and AD CS deployed.
- The Active Directory domain controllers you intend to install Defender for Identity sensors on have internet connectivity to the Defender for Identity cloud service.
  - Your firewall and proxy must be open to communicate with the Defender for Identity cloud service (\*.atp.azure.com port 443 must be open).
- Domain controllers running on one of the following servers:
  - Windows Server 2016.
  - Windows Server 2019 with KB4487044 (OS Build 17763.316 or later).
  - Windows Server 2022.
- Microsoft .NET Framework 4.7 or later.
- A minimum of six (6) GB of disk space is required and 10 GB is recommended.
- Two (2) cores and six (6) GB of RAM installed on the domain controller.

## Microsoft Defender for Office 365

Microsoft Defender for Office 365 safeguards your organization against malicious threats posed by email messages, links (URLs), attachments, and collaboration tools like Microsoft Teams, SharePoint, and Outlook. With real-time views of threats and tools like Threat Explorer, you can hunt and stay ahead of potential threats. Use attack simulation training to run realistic

attack scenarios in your organization. These simulated attacks can help you identify and find vulnerable users before a real attack impacts your bottom line.

FastTrack provides remote guidance for:

- Reviewing the Configuration analyzer and/or Defender for Office 365 Recommended Configuration Analyzer (ORCA).
- Setting up evaluation mode.
- Enabling preset policies, Safe Links (including Safe Documents), Safe Attachments, anti-malware, anti-phishing, anti-spam, anti-spoofing, impersonation, and quarantine policies.
- Providing an overview of priority accounts and user tags.
- Defining spam and bulk user experiences.
- Enabling Teams protection.
- Configuring user-reported message settings.
- Using Attack simulation training and configuring an advanced delivery policy
- Providing an overview of the Tenant Allow/Block List (TABL), submissions, email entity page, reporting, campaigns, threat explorer, and threat analytics.
- Providing an overview of spoof intelligence, impersonation protection, and mailbox intelligence.
- Providing an overview of zero-hour auto purge (ZAP) automated investigation and response (AIR).
- Understanding incident correlation in the Microsoft Defender portal.
- Understanding the impact of features that modify messages and external tags.
- Transitioning from a non-Microsoft provider following the Microsoft best practice guidance except for creating an inventory of your current settings.
- Providing an overview of mail flow analysis.

## Out of scope

- Discussions comparing Defender for Office 365 to other security offerings.
- Deploying Defender for Office 365 as a proof of concept.
- Training or guidance covering advanced hunting.
- Integration with Microsoft Power Automate playbooks.
- SIEM or API integration (other than Microsoft Sentinel).

## Source environment expectations

In addition to [FastTrack core onboarding](#), [Exchange Online](#) must also be configured.

## Microsoft Defender for Cloud

Microsoft Defender for Cloud is a cloud-native application protection platform (CNAPP) that's made up of security measures and practices designed to protect cloud-based applications from various cyber threats and vulnerabilities.

When you enable Defender for Cloud, you automatically gain access to Microsoft Defender XDR. FastTrack enhances the integration between Defender XDR and Defender for Cloud by assisting in improving your security posture with Defender for Cloud Foundational CSPM (cloud security posture management), a free new feature. FastTrack also helps you extend your protection of cloud workloads by deploying Microsoft Defender for Servers on Windows devices that run in Microsoft Azure and on-premises. Defender for Servers integrates with Microsoft Defender for Endpoint to provide endpoint detection and response (EDR) and other threat protection features.

FastTrack provides remote guidance for:

- Providing an overview of Defender for Cloud, including:
  - Scoping pre-deployment best practices.
    - Ensuring the basic environment setup and knowledge is in place.
    - Defining and implementing a management group hierarchy in the Azure environment.
  - Validating roles and permissions.
    - Creating a central team responsible for tracking and enforcing security in the Azure environment.
    - Assigning the necessary role-based access control (RBAC) permissions for the central security team.
  - Providing policy management.
    - Assigning and customizing the Defender for Cloud default policy.
    - Choosing standards for the compliance dashboard.
    - Ensuring resources are secure by default using Azure policy.
  - Onboarding Defender for Cloud features for Azure.
    - Enabling all Microsoft Defender plans.
    - Configuring security contact and email settings.
    - Deploying required agents
  - Exporting Defender for Cloud data to Microsoft Sentinel.
- Deploying Foundational CSPM, including:
  - Windows and Linux servers running in Azure and on-premises.
  - Security recommendations.
  - Asset inventory.
  - Microsoft Secure Score.
  - Data visualization and reporting.
  - Data exporting.
  - Workflow automation.

- Remediation tools.
- Microsoft cloud security benchmark (MCSB).
- Deploying Defender for Servers P1 features, including:
  - Configuring Windows and Linux servers running in Azure and on-premises.
  - Provisioning Defender for Servers.
  - Onboarding to Azure Arc.
  - Provisioning and integrating Defender for Endpoint.
  - Configuring unified view.
  - Configuring OS-level, agent-based threat detection.

## Out of scope

- Detailed pricing information. Contact your account team for more information.
- Deploying features on Windows or Linux servers that run in Amazon Web Services (AWS) and Google Cloud Platform (GCP).
- Onboarding Defender for Cloud, including:
  - Management.
    - Reviewing additional Defender for Cloud data ingested into Microsoft Sentinel following Defender for Servers P2 enablement.
    - Preparing and deploying Logic Apps.
    - Deploying workflow automation.
    - Exporting data for additional reporting.
    - Exporting Defender for Cloud data to other security information and event management (SIEM) or information technology service management (ITSM) solutions.
    - Setting alert suppression rules.
  - Policy management.
    - Ensuring resources are secure through Azure Blueprints (Preview) which will be deprecated July 11, 2026.
    - Assigning custom policies.
- Deploying Defender for Cloud Foundational CSPM, including:
  - Deploying agentless scanning capability.
  - Managing governance.
  - Deploying the risk-based Recommendation dashboard.
  - Reviewing attack path analysis.
  - Deploying Azure DevOps security capabilities.
  - Deploying the data aware security posture.
- Deploying Defender for Server P2 features, including:
  - Configuring Windows servers running in Azure and on-premises.



- Deploying agentless scanning for both Defender for Cloud Foundational CSPM and Defender for Servers.
- Enabling File Integrity Monitoring (FIM) through the Defender for Endpoint sensor.
- Customizing and optimizing FIM.
- Configuring just-in-time virtual machine access.
- Managing Azure Update Manager remediation for Azure Arc devices.
- Managing free data ingestion using Azure Monitor Agent (AMA) to ingest logs.
- Deploying the Microsoft Defender Vulnerability Management add-on.
- Configuring security policy and regulatory compliance.
- Managing docker host hardening.
- Deploying a network map.
- Deploying any of the following Microsoft Defender workloads:
  - Microsoft Defender for Storage.
  - Microsoft Defender for Resource Manager.
  - Microsoft Defender for Key Vault.
  - Microsoft Defender for App Service.
  - Microsoft Defender for APIs.
  - Microsoft Defender for Containers.
  - Microsoft Defender External Attack Surface Management (Defender EASM).
  - Microsoft Defender for Databases.
  - Microsoft Defender for Azure SQL databases.
  - Microsoft Defender for SQL servers on devices.
  - Microsoft Defender for open-source relational databases (including Postgre SQL, MySQL, and MariaDB).
  - Microsoft Defender for Azure Cosmos DB
- Deploying any of the following deprecated Microsoft Defender workloads:
  - Microsoft Defender for DNS.
  - Microsoft Defender for Kubernetes.
  - Microsoft Defender for Container Registries.

## Copilot in Defender

FastTrack provides remote guidance for:

- Onboarding assistance, including:
  - Provisioning Security Compute Units (SCUs).
  - Configuring default environments.
- Walkthroughs for Copilot for Defender embedded experiences, including:
  - Incident summaries, guided responses, and incident reports.
  - Identity and device summaries.
  - File and script analyzer guidance.

- Natural language to Keyword Query Language (KQL) overview and demonstration.
- Defender Threat Intelligence (Defender TI) prompting.

## Out of scope

- Detailed pricing information. Contact your account team for more information.
- Threat hunting and incident responses.
- Providing walkthroughs of Security Copilot standalone experiences.

## Microsoft advanced deployment guides

Microsoft provides customers with technology and guidance to assist with deploying your Microsoft 365, Microsoft Viva, and security services. We encourage our customers to start their deployment journey with [these](#) offerings.

For non-IT admins, see [Microsoft 365 Setup](#).

# Microsoft Entra

Article • 04/30/2025

## Zero Trust

FastTrack provides comprehensive guidance on implementing Zero Trust security principles. The Zero Trust model assumes breach and verifies each request as though it originates from an uncontrolled network. This approach ensures robust security across your networks, applications, and environment. FastTrack accomplishes this by focusing on identity, devices, applications, data, infrastructure, and networks. With FastTrack, you can confidently advance your Zero Trust security journey and protect your digital assets effectively.

With Microsoft Entra, you can implement Zero Trust principles by ensuring strong authentication and access policies. This includes enforcing least privileged access with granular permissions and controls, managing access to secure resources, and minimizing the blast radius of potential attacks. By integrating with Microsoft Entra ID, you can create secure Zero Trust solutions that protect your organization's identity and access management.

## Identity integration

FastTrack provides remote guidance for:

- Preparing on-premises Active Directory Identities for synchronization to Microsoft Entra ID including installing and configuring Microsoft Entra Connect (single or multi-forest) and licensing (including group-based licensing).
- Creating cloud identities including bulk import and licensing including using group-based licensing.
- Choosing and enabling the correct authentication method in Microsoft Entra Connect for your cloud journey, password hash sync, pass-through authentication, or Active Directory Federation Services (AD FS).
- Choosing and enabling one or more of the following phishing-resistant passwordless authentication methods:
  - Passkeys (Fast Identity Online (FIDO2)):
    - FIDO2 security keys.
    - Microsoft Authenticator app passkeys.
    - Windows Hello for Business cloud Kerberos trust.
  - Microsoft Entra certificate-based authentication (CBA).
- Providing planning documentation for Windows Hello for Business hybrid key or certificate trust.

- Migrating authentication from AD FS to Microsoft Entra ID using password hash sync or Pass-through Authentication.
- Migrating preintegrated software-as-a-service (SaaS) apps (Microsoft Entra app gallery) from AD FS to Microsoft Entra ID for single sign-on (SSO).
- Enabling SaaS app integrations with SSO from the Microsoft Entra app gallery.
- Enabling automatic user provisioning for preintegrated SaaS apps as listed in the app integration tutorial list (limited to Microsoft Entra app gallery and outbound provisioning only).
- Enabling security defaults to secure your Identities for nonpremium Microsoft Entra customers.
- Configuring Microsoft Entra join.
- Configuring Microsoft Entra hybrid join.

## Out of scope

- Setting up or configuring the following:
  - Public key infrastructure (PKI) certificate authorities.
  - Network Device Enrollment Service (NDES) deployments.
  - Wireless networks.
  - Network devices.
  - VPNs.
  - Virtual local areas.

## Microsoft Entra ID P1

FastTrack provides remote guidance to enable secure access to apps and to protect identities from security threats.

This guidance includes:

- Multifactor authentication (MFA) (cloud only).
- Self-service password reset (SSPR).
- Conditional Access.
- Self-service group management.
- Dynamic group membership.
- Business-to-business (B2B) collaboration between Microsoft Entra tenants.
- Setup of a multitenant organization in Microsoft 365 admin center.
- B2B direct connect.
- Cross-tenant synchronization.
- Cross-tenant access.
- Password protection.

- Application Proxy for on-premises web apps.
- Connect Health.
- Company branding.
- Managing collections in My Apps.
- Role-based access control (RBAC) for built-in administrative roles.
- Administrative units.
- Built-in monitoring and reporting capabilities.
- Terms of use.

## Microsoft Entra ID P2 (included in Microsoft 365 E5)

FastTrack provides remote guidance to enable secure access to apps and to protect identities from security threats.

This guidance includes:

- Identity Protection.
- Risk-based Conditional Access.
- Privileged Identity Management (PIM).
- Basic entitlement management.
- Access reviews.

## Microsoft Entra ID Governance

FastTrack provides remote guidance for:

- Deploying Privileged Identity Management (PIM) (also included in Microsoft Entra ID P2).
- Deploying entitlement management.
- Configuring access reviews.
- Configuring automatic user provisioning to on-premises Active Directory or Microsoft Entra ID for Workday HCM or SAP SuccessFactors through tutorial assistance.
- Configuring attribute writeback from Microsoft Entra ID to Workday HCM or SAP SuccessFactors through tutorial assistance.
- Deploying lifecycle workflow built-in tasks and templates including use of custom security attributes to scope a workflow.

## Out of scope

- Any API related configuration or customization.

- Any configuration inside of Workday HCM or SAP SuccessFactors portals.
- Configuring advanced attribute mappings.
- Custom expression mapping for provisioning or writeback.
- Data remediation for manual human resource (HR) data.
- Lifecycle workflow custom task extensions and APIs.
- Azure Logic Apps customization or integration.

## **Microsoft Entra Global Secure Access**

### **Global Secure Access configuration**

FastTrack provides remote guidance for:

- Activating Global Secure Access in the tenant.
- Enabling traffic forwarding profiles for Microsoft Entra Internet Access, Microsoft Entra Private Access, and Microsoft traffic.
- Enabling source IP restoration.
- Installing the Global Secure Access client on Windows 10/11, macOS, iOS, and Android clients.

### **Microsoft Entra Internet Access for Microsoft Services (included in Microsoft Entra ID P1)**

FastTrack provides remote guidance for:

- Enabling Global Secure Access signaling for Conditional Access.
- Enabling universal tenant restrictions including blocking access for all external identities and applications.
- Configuring compliant network access.
- Configuring applicable Conditional Access policies.

### **Microsoft Entra Internet Access**

FastTrack provides remote guidance for:

- Creating and applying web filtering policies.
- Applying web filtering policies to security profiles.
- Creating Conditional Access policies that apply to Microsoft Entra Internet Access.

### **Microsoft Entra Private Access**

FastTrack provides remote guidance for:

- Installing and configuring connectors.
- Publishing applications.
- Creating Conditional Access policies that apply to Microsoft Entra Private Access.

## Out of scope

- Network device, virtual local area network (VLAN) configuration, and internal network routing for Microsoft Entra Internet Access and Microsoft Entra Private Access.
- Remote network connectivity.
- Third-party security information and event management (SIEM) integration.

## Source environment expectations

The on-premises Active Directory and its environment are prepared for Microsoft Entra, including remediation of identified issues that prevent integration with Microsoft Entra ID and other in-scope features.

## Copilot in Entra

FastTrack provides remote guidance for:

- Onboarding assistance, including:
  - Provisioning Security Compute Units (SCUs).
  - Configuring default environments.
- Walkthroughs for Copilot in Entra embedded experiences, including:
  - Using Copilot in Entra to protect identities and secure access with AI-driven risk detection and mitigation.
  - Using Copilot in Entra to troubleshoot access failure during critical access attempts.
  - Demonstrating assistance in incident investigation and troubleshooting with Microsoft Entra skills in Security Copilot.
  - Demonstrating assistance in lifecycle workflows to assist with employee onboarding scenarios.
  - Demonstrating assistance to investigate and remediate risky applications registered with Microsoft Entra.

## Out of scope

- Detailed pricing information. Contact your account team for more information.
- Providing walkthroughs of standalone experiences.

# Microsoft advanced deployment guides

Microsoft provides customers with technology and guidance to assist with deploying your Microsoft 365, Microsoft Viva, and security services. We encourage our customers to start their deployment journey with [these](#) offerings.

For non-IT admins, see [Microsoft 365 Setup](#).



# Microsoft Intune

Article • 10/30/2024

## Zero Trust

FastTrack provides comprehensive guidance on implementing Zero Trust security principles. The Zero Trust model assumes breach and verifies each request as though it originates from an uncontrolled network. This approach ensures robust security across your networks, applications, and environment. FastTrack accomplishes this by focusing on identity, devices, applications, data, infrastructure, and networks. With FastTrack, you can confidently advance your Zero Trust security journey and protect your digital assets effectively.

With Microsoft Intune, you can implement Zero Trust principles by securely provisioning, configuring, and updating all endpoint devices. This includes enforcing security policies through the cloud, covering endpoint security, device configuration, app protection, and compliance. This approach helps prevent data leaks to untrusted apps or services and ensures prompt responses to security compromises.

## Microsoft Intune

Microsoft Intune is a cloud-based endpoint management solution. It manages user access to organizational resources and simplifies app and device management across your devices, including mobile devices, desktop computers, and virtual endpoints. You can protect access and data on organization-owned and users' personal devices.

Intune has compliance and reporting features that support the Zero Trust security model.

FastTrack provides remote guidance for:

- Licensing your end users.
- Configuring identities used by Intune by using either on-premises Active Directory or cloud identities (Microsoft Entra ID).
- Adding users to your Intune subscription, defining IT admin roles, and creating user and device groups.
- Configuring your mobile device management (MDM) authority, based on management needs, including setting Intune as your MDM authority when Intune is the only MDM solution.
- Providing MDM guidance for:

- Configuring tests groups to be used to validate MDM management policies.
- Configuring MDM management policies and services including:
  - App deployment for each supported platform through web links or deep links.
  - Conditional Access policies.
  - Deployment of email, wireless networks, VPN profiles for existing certificate authority, wireless network, or VPN infrastructure in the organization.
  - Connecting to the Intune Data Warehouse.
  - Integrating Intune with:
    - Team Viewer for remote assistance (a Team Viewer subscription is required).
    - Mobile Threat Defense (MTD) partner solutions (an MTD subscription is required).
    - A telecom expense management solution (a telecom expense management solution subscription is required).
  - Enrolling devices of each supported platform to Intune.
  - Configuring endpoint security policies including Windows Local Administrator Password Solution (LAPS) using Intune.
- Providing app protection guidance on:
  - Configuring app protection policies for each supported platform.
  - Configuring Conditional Access policies for managed apps.
  - Targeting the appropriate user groups with the previously mentioned MAM policies.
  - Using managed-apps usage reports.
- Providing migration guidance from legacy PC management to Intune MDM.

## Out of scope

- Setting up or configuring certificate authorities, wireless networks, VPN infrastructures, or Apple MDM push certificates for Intune.
- Setting up or upgrading either the Configuration Manager site server or client to the minimum requirements needed to support cloud-attach.
- Integrating Intune with Microsoft Defender for Endpoint and creating device compliance policies based on its Windows 10 risk level assessment. FastTrack doesn't assist with purchasing, licensing, or activation.

Contact a [Microsoft Partner](#) for assistance with any out-of-scope services.

## Copilot in Intune

FastTrack provides remote guidance for:

- Onboarding assistance, including:
  - Provisioning Security Compute Units (SCUs).
  - Configuring default environments.
- Walkthroughs for Copilot in Intune embedded experiences, including:
  - Using Copilot in Intune to troubleshoot device issues and assist with root cause assessment
  - Using Copilot in Intune for policy management to summarize existing settings, overall security impact, and providing guidance on best practices.
  - Using Copilot in Intune for running device queries and creating Kusto Query Language (KQL).

## Out of scope

- Detailed pricing information. Contact your account team for more information.
- Providing walkthroughs of standalone experiences.

## Certificate delivery

FastTrack provides remote guidance for:

- Simple Certificate Enrollment Protocol (SCEP) and the Network Device Enrollment Service (NDES).
  - Configuring enterprise Certificate Authority-related items.
  - Creating and issuing a SCEP certificate template.
  - Installing and configuring NDES.
  - Installing and configuring the Microsoft Intune Connector for SCEP.
  - Installing and configuring Microsoft Entra application proxy and Microsoft Entra application connectors.
  - Creating and assigning a trusted certificate device configuration profile in Microsoft Endpoint Manager.
  - Creating and assigning a SCEP certificate device configuration profile on Microsoft Endpoint Manager.
- Public-Key Cryptography Standards (PKCS) and PFX (PKCS#12) certificates.
  - Configuring enterprise Certificate Authority-related items.
  - Creating and issuing a PKCS certificate template.
  - Installing and configuring a PFX certificate connector.
  - Creating and assigning a trusted certificate device configuration profile in Microsoft Endpoint Manager.

- Creating and assigning a PKCS certificate device configuration profile in Microsoft Endpoint Manager.

## Out of scope

- Assistance with public key infrastructure (PKI) certificates or enterprise Certificate Authority.
  - Supporting advanced scenarios, including:
    - Placing the NDES server in the customer's DMZ.
    - Configuring or using a Web Application Proxy server to publish the NDES URL externally to the corporate network. We recommend and provide guidance for using the Microsoft Entra application proxy to accomplish configuration.
    - Using imported PKCS certificates.
    - Configuring Intune certification deployment using a hardware security module (HSM).

## Cloud-attach

FastTrack provides remote guidance to customers to cloud-attach existing Configuration Manager environments with Intune.

This includes:

- Licensing end users.
- Configuring identities to be used by Intune by using on-premises Active Directory and cloud identities.
- Adding users to your Intune subscription, defining IT admin roles, and creating user and device groups.
- Providing guidance setting up Microsoft Entra hybrid join.
- Providing guidance on setting up Microsoft Entra ID for MDM autoenrollment.
- Providing guidance on how to set up cloud management gateway when used as a solution for co-management of remote internet-based device management.
- Configuring supported workloads to switch to Intune.
- Installing the Configuration Manager client on Intune-enrolled devices.

## Deploy Outlook mobile for iOS and Android securely

FastTrack provides remote guidance to customers to deploy Outlook mobile for iOS and Android securely to ensure users have all required apps installed.

This includes:

- Downloading Outlook for iOS and Android, Microsoft Authenticator, and Intune Company Portal apps through the Apple App Store or Google Play Store.
- Setting up:
  - The Outlook for iOS and Android, Microsoft Authenticator, and Intune Company Portal apps deployment with Intune.
  - App protection policies.
  - Conditional Access policies.
  - App configuration policies.

## Endpoint analytics

FastTrack provides remote guidance to customers to enable Endpoint analytics.

This includes:

- Confirming the licenses for your endpoints and users.
- Confirming your organizational environments meet the prerequisites for Endpoint analytics features.
- Configuring endpoints with correct policies to enable Endpoint analytics features.
- Setting organizational baselines to track progress.
- Providing guidance on using Remediation within Endpoint analytics, including:
  - Using Microsoft-authored remediation scripts.

## Out of scope

- Creating custom remediation scripts.

Contact a [Microsoft Partner](#)  for assistance with any out-of-scope services.

## Source environment expectations

- IT admins must have existing certificate authority, wireless network, and VPN infrastructures enabled in their production environments in order to deploy wireless network and VPN profiles with Intune.
- The customer environment should have an existing healthy PKI before enabling PKCS and SCEP certificate delivery with Intune.
- Endpoint devices must be managed by Intune.

- IT admins are responsible for registering the devices to the organization by either having the hardware vendor upload the hardware IDs for uploading it themselves into the Windows Autopilot service.

## Microsoft Intune Suite

Microsoft Intune Suite provides mission-critical advanced endpoint management and security capabilities for Intune.

### Endpoint Privilege Management

Endpoint Privilege Management (EPM) supports your zero-trust journey by helping your organization achieve a broad user base running with least privilege while allowing users to still run tasks allowed by your organization and remain productive.

FastTrack provides remote guidance to customers to enable EPM.

This includes:

- Providing an overview of EPM, prerequisites, and endpoints.
- Providing guidance on enabling EPM and elevation setting policies and default responses for elevation requests.
- Providing guidance for creating elevation rules policies to manage the identification of specific files and how elevation requests for those files are handled.
- Creating reusable settings groups to manage the certificates already in place.
- Providing guidance for policy conflict handling.
- Providing support-approved file elevations.
- Providing role-based access control (RBAC) permissions for elevation requests.
- Creating policies for support-approved file elevations.
- Managing pending elevation requests.
- Providing EPM reports.

### Out of scope

- Managing pending approvals using automation.

Contact a [Microsoft Partner](#) for assistance with any out-of-scope services.

For more information, see [Use Endpoint Privilege Management with Microsoft Intune](#).

## Enterprise Application Management

Enterprise Application Management provides an Enterprise App Catalog of Win32 apps that are easily accessible in Intune. You can add these apps to your tenant by selecting them from the Enterprise App Catalog. When you add an Enterprise App Catalog app to your Intune tenant, default installation, requirements, and detection settings are automatically provided. In addition, Intune hosts Enterprise App Catalog apps in Microsoft storage.

FastTrack provides remote guidance to customers to enable Enterprise Application Management.

This includes:

- Providing an overview of and prerequisites for Enterprise Application Management.
- Configuring prepackaged and pre-configured apps that are self-updating.
- Adding the Windows Catalog app to Intune.
- Enabling app information monitoring.
- Enabling app installation status reports.

## Out of scope

- Automation using Microsoft Graph API.

Contact a [Microsoft Partner](#) for assistance with any out-of-scope services.

For more information, see [Microsoft Intune Enterprise Application Management](#).

## Advanced Analytics

Advanced Analytics is a set of analytics-driven capabilities that help IT admins understand, anticipate, and improve the end-user experience.

FastTrack provides remote guidance to customers to enable Advanced Analytics.

This includes:

- Providing an overview of and prerequisites for Advanced Analytics.
- Enabling anomaly detection in Endpoint analytics to monitor the health of devices for user experience and productivity regressions following configuration changes.
- Providing an enhanced device timeline of events on a specific device to assist with troubleshooting device issues.
- Configuring device scopes in Endpoint analytics, including custom device scopes to slice Endpoint analytics reports to a subset of devices.

- Configuring device queries in Intune, including near-real time access to data about device state.
- Enabling battery health reports.

## Source environment expectations

- The customer uses Intune for device management.

For more information, see [What is Microsoft Intune Advanced Analytics?](#).

## Remote Help

Remote Help is a cloud-based solution for secure help desk connections with role-based access controls (RBAC).

FastTrack provides remote guidance to customers to enable Remote Help.

This includes:

- Providing an overview of and prerequisites for Remote Help.
- Clarifying the prerequisites for Remote Help on Windows, Android, and macOS.
- Configuring Remote Help for the customer's tenant.
- Configuring RBAC to set the level of access a helper is allowed.
- Configuring Remote Help on Windows enrolled and unenrolled devices, including:
  - Clarifying network considerations.
  - Installing and updating the Remote Help Win32 App.
  - Enabling log files
- Configuring Remote Help to work with Conditional Access.
- Configuring the ServiceNow connector.
- Configuring Remote Help on macOS enrolled and unenrolled devices, including:
  - Clarifying network considerations.
  - Installing the Remote Help app,
  - Configuring native app OS permissions.
  - Installing and updating the Remote Help native macOS app.
- Configuring Remote Help on Android devices, including:
  - Clarifying the rerequisites.
  - Deploying the Remote Help app.
  - Providing guidance on granting permissions for Zebra and Samsung devices.
  - Using Remote Help on Android devices.

## Out of scope



- ServiceNow integration and troubleshooting.
- Configuring original equipment manufacturer (OEM) Android devices.

Contact a [Microsoft Partner](#) for assistance with any out-of-scope services.

For more information, see [Use Remote Help with Microsoft Intune](#).

## Microsoft Tunnel for Mobile Application Management

When you use the Microsoft Tunnel VPN Gateway, you can extend Microsoft Tunnel support by adding Tunnel for Mobile Application Management (MAM). Tunnel for MAM extends the Microsoft Tunnel VPN Gateway to support devices that run Android or iOS and that aren't enrolled with Intune.

FastTrack provides remote guidance to customers to enable Tunnel for MAM.

This includes:

- Providing an overview of and prerequisites for Tunnel for MAM.
- Configuring Microsoft Tunnel VPN for unenrolled Android devices.
- Configuring policies to support Tunnel for MAM.
- Configuring line-of-business (LOB) apps.
- Configuring Microsoft Tunnel VPN for unenrolled iOS and iPad devices.
- Reviewing the required SDK for iOS.
- Configuring policies for Tunnel for MAM for iOS.
- Configuring LOB apps in Microsoft Entra admin center
- Configuring Xcode LOB apps integration.
- Monitoring Microsoft Tunnel.

### Out of scope

- Core Microsoft Tunnel Gateway setup.

Contact a [Microsoft Partner](#) for assistance with any out-of-scope services.

For more information, see [Microsoft Tunnel for Mobile Application Management](#).

## Microsoft Cloud PKI

Microsoft Cloud PKI is a cloud-based service that simplifies and automates certificate lifecycle management for Intune-managed devices. It provides a dedicated public key infrastructure (PKI) for your organization and handles the certificate issuance, renewal, and revocation for all Intune-supported platforms.

FastTrack provides remote guidance to customers to enable Microsoft Cloud PKI.

This includes:

- Providing an overview of and prerequisites for Microsoft Cloud PKI.
- Configuring RBAC-created custom roles with Microsoft Cloud PKI permissions.
- Creating a two-tier PKI hierarchy with both root and issuing certification authority (CA) in the cloud.
- Configuring bring your own CA (BYOCA) to anchor an Intune-issuing CA to a private CA through Active Directory Certificate Services or a non-Microsoft certificate service.
- Creating trusted certificate profiles.
- Creating Simple Certificate Enrollment Protocol (SCEP) certificate profiles.
- Monitoring the issuing CA and reviewing issued certificates.
- Providing a SCEP certificate profile report
- Enabling Microsoft Cloud PKI audit logs.

## Out of scope

- Explaining cryptographic concepts.
- Setting up or configuring on-premises CAs.
- Configuring CAs for web service enrollment.
- Deploying certificates on relying parties (like VPN, Wi-Fi, apps, or servers).
- Configuring your Network Policy Server (NPS) or Remote Authentication Dial-In User Service (RADIUS).

Contact a [Microsoft Partner](#)  for assistance with any out-of-scope services.

For more information, see [Overview of Microsoft Cloud PKI for Microsoft Intune](#).

## Firmware Over-the-Air updates and specialty device management

Firmware Over-the-Air (FOTA) updates allow for remote updating of device firmware using a wireless connection rather than requiring the devices to be physically connected to a computer or network.

Specialty device management with Intune provides a range of management, configuration, and protection capabilities for specialized devices, like AR and VR headsets, large smart-screen devices, and select conference room meeting devices.

FastTrack provides remote guidance to customers to enable FOTA updates and specialty device management.

This includes:

- Setting up Intune enrollment for Android devices on the Android Open Source Project (AOSP) platform for corporate-owned user-less and user-associated devices (including RealWear devices).
- Enabling Android FOTA updates.
- Enabling Samsung Enterprise FOTA (E-FOTA) update management.
- Enabling Zebra LifeGuard Over-the-Air (LG OTA) integration.
- Configuring Meta Work Accounts for automatic user provisioning with Microsoft Entra ID.
- Configuring automatic user provisioning for Meta Quest for Business Work Accounts with Microsoft Entra ID.
- Monitoring provisioning logs.
- Setting up the Meta Quest Device Manager.
- Configuring Intune integration with Meta Quest Device Manager.

## Out of scope

- Meta Quest for Business troubleshooting.
- OEM configuration and integration troubleshooting.

Contact a [Microsoft Partner](#) for assistance with any out-of-scope services.

For more information, see [Mobile Firmware-over-the-air update](#).

## Microsoft advanced deployment guides

Microsoft provides customers with technology and guidance to assist with deploying your Microsoft 365, Microsoft Viva, and security services. We encourage our customers to start their deployment journey with [these](#) offerings.

For non-IT admins, see [Microsoft 365 Setup](#).

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

# Microsoft Purview

06/02/2025

## Zero Trust

FastTrack provides comprehensive guidance on implementing Zero Trust security principles. The Zero Trust model assumes breach and verifies each request as though it originates from an uncontrolled network. This approach ensures robust security across your networks, applications, and environment. FastTrack accomplishes this by focusing on identity, devices, applications, data, infrastructure, and networks. With FastTrack, you can confidently advance your Zero Trust security journey and protect your digital assets effectively.

With Microsoft Purview, you can implement Zero Trust principles by identifying and protecting your data using a Zero Trust approach. This includes classifying and labeling sensitive data, applying encryption, and enforcing data loss prevention policies. By doing so, you can ensure that your data is secure, compliant, and only accessible to authorized users.

## Microsoft Purview Compliance Manager

Microsoft Purview Compliance Manager is a solution that helps you automatically assess and manage compliance across your multicloud environment.

FastTrack provides remote guidance for the following items:

- Reviewing role types.
- Adding and configuring assessments.
- Assessing compliance by implementing improvement actions and determining how this impacts your compliance score.
- Reviewing built-in control mapping and assessing controls.
- Generating a report within an assessment.

## Out of scope

- Custom scripting and coding.
- Connectors.
- Compliance with industry and regional regulations and requirements.
- Hands-on implementation of recommended improvement actions for assessments in Compliance Manager.

## Source environment expectations

Aside from the FastTrack core onboarding, there are no minimum system requirements.

## Microsoft Purview Information Protection

Microsoft Purview Information Protection helps you discover, classify, protect, and govern sensitive information wherever it lives or travels.

FastTrack provides remote guidance for:

- Activating and configuring your tenant.
- Data classification.
- Sensitive information types.
- Creating sensitivity labels.
- Applying sensitivity labels.
- Default sensitivity labels for SharePoint document libraries.
- Installing and configuring the Microsoft Purview Data Loss Prevention (DLP) migration assistant for Symantec and Forcepoint.
- Understanding migration report output from the Microsoft Purview DLP migration assistant.
- Fine-tuning migrated policies in the Microsoft Purview compliance portal.
- Discovering and labeling files at rest using the Microsoft Purview Information Protection scanner.
- Monitoring emails in transit using Exchange Online mail flow rules.
- Using migration guidance from the Azure Information Protection add-in to provide built-in labeling for Office apps.
- Enabling the sensitivity label requirement for Microsoft Power BI in the compliance portal.
- Creating and setting up labels and policies.
- Applying information protection to documents.

FastTrack also provides guidance if you want to apply protection using Microsoft Azure Rights Management Services (Azure RMS), Office 365 Message Encryption (OME), and DLP.

The following remote guidance is available only for E5 Premium customers:

- Trainable classifiers.
- Exact Data Match (EDM) custom sensitive information types.
- Knowing your data with content explorer and activity explorer.
- Automatically publishing labels using policies.
- Creating Endpoint DLP policies for Windows 10 and later devices.
- Creating Endpoint DLP policies for macOS devices.

- Creating DLP policies for Microsoft Teams chats and channels.
- Automatically classifying and labeling information in Office apps (like Word, PowerPoint, Excel, and Outlook) running on Windows and using the Microsoft Purview Information Protection client.
- Extending sensitivity labels to Outlook appointments, invites, and Teams online meetings.

## Out of scope

- Customer Key.
- Custom regular expressions (RegEx) development for sensitive information types.
- Creation or modification of keyword dictionaries.
- Interacting with customer data or specific guidelines for configuration of EDM-sensitive information types.
- Custom scripting and coding.
- Azure Purview.
- Configuring Enterprise State Roaming.
- SharePoint data governance and administration.

## Source environment expectations

- For more information, see [FastTrack core onboarding](#).
- SharePoint data access governance for data access planning:
  - [SharePoint data access governance](#).
  - [SharePoint advanced management overview](#).
  - [Restricted access control policy for SharePoint sites](#).
  - [Restricted access control policy for OneDrive](#).

## Customer responsibilities

- A list of file share locations to be scanned.
- An approved classification taxonomy.
- Understanding of any regulatory restriction or requirements regarding key management.
- A service account created for your on-premises Active Directory synchronized with Microsoft Entra ID.
- All prerequisites for the Microsoft Purview Information Protection scanner are in place. For more information, see [Prerequisites for installing and deploying the Microsoft Purview Information Protection unified labeling scanner](#).
- Ensure user devices are running a supported operating system and have the necessary prerequisites installed. For more information, see [Admin Guide: Install the Microsoft](#)

[Purview Information Protection unified labeling client for users](#) and [What is the Microsoft Purview Information Protection app for iOS or Android?](#).

- Installation and configuration of the Azure RMS connector and servers including the Active Directory RMS (AD RMS) connector for hybrid support.
- Setup and configuration of Bring Your Own Key (BYOK), Double Key Encryption (DKE) (unified labeling client only), or Hold Your Own Key (HYOK) (classic client only) should you require one of these options for your deployment.

## Microsoft Purview Data Lifecycle Management and Purview Records Management

Microsoft Purview Data Lifecycle and Purview Records Management helps you to govern your Microsoft 365 data for compliance or regulatory requirements.

FastTrack provides remote guidance for:

- Creating and applying retention policies.
- Creating and publishing retention labels.
- The following remote guidance is available only for E5 Premium customers: Creating and applying event-based retention labels.
- Creating and applying adaptive policy scopes.
- Reviewing file plan creation.
- Reviewing dispositions.
- Policy lookups.

### Out of scope

- Development of a records management file plan.
- Data connectors.
- Azure Purview data governance.
- Creating and managing Power Automate flows.
- Custom scripting and coding.
- Design, architect, and third-party document review.
- Importing Outlook Data Files (PSTs) to Office 365.
- Development of information architecture in SharePoint.
- SharePoint data governance and administration.

### Source environment expectations

- For more information, see [FastTrack core onboarding](#).

- SharePoint data access governance for data access planning:
  - [SharePoint data access governance](#).
  - [SharePoint advanced management overview](#).
  - [Restricted access control policy for SharePoint sites](#).
  - [Restricted access control policy for OneDrive](#).

# Microsoft Purview Insider Risk Management

## Purview Insider Risk Management

Microsoft Purview Insider Risk Management correlates various signals to identify potential malicious or inadvertent insider risks, like IP theft, data leakage, and security violations.

FastTrack provides remote guidance for:

- Creating policies and reviewing settings.
- Accessing reports and alerts.
- Creating cases.
- Enabling and configuring forensic evidence.

### Out of scope

- Creating and managing Power Automate flows.
- Data connectors (beyond the HR connector).
- Information barriers.
- Privileged access management.

## Purview Communication Compliance

Microsoft Purview Communication Compliance provides the tools to help organizations detect regulatory compliance and business conduct violations like sensitive or confidential information, harassing or threatening language, and sharing of adult content.

FastTrack provides remote guidance for the following items:

- Creating policies and reviewing settings.
- Accessing reports and alerts.
- Creating notice templates.

### Out of scope



- Creating and managing Power Automate flows.
- Information barriers.

## Source environment expectations

For more information, see [FastTrack core onboarding](#).

# Microsoft Purview eDiscovery & Audit

## Purview eDiscovery (Premium)

Microsoft Purview eDiscovery (Premium) can help your organization respond to legal matters or internal investigations by discovering data where it lives. You can manage eDiscovery workflows by identifying persons of interest and their data sources, apply holds to preserve data, and then manage the legal hold communication process.

FastTrack provides remote guidance for:

- Creating a new case.
- Putting custodians on hold.
- Managing custodians.
- Performing searches.
- Adding search results to a review set.
- Running analytics on a review set.
- Reviewing and tagging documents.
- Exporting data from the review set.
- Importing non-Office 365 data.

## Out of scope

- Purview eDiscovery API.
- Data connectors.
- Compliance boundaries and security filters.
- Design, architect, and third-party document review.

## Purview Audit (Premium)

Microsoft Purview Audit (Premium) helps organizations conduct forensic and compliance investigations. This is done by increasing audit log retention required to conduct an

investigation, providing access to intelligent insights that help determine scope of compromise, and faster access to the Office 365 Management Activity API.

FastTrack provides remote guidance for:

- Enabling advanced auditing.
- Performing a search audit log UI and basic audit PowerShell commands.

## Out of scope

- Custom scripting and coding.

## Source environment expectations

For more information, see [FastTrack core onboarding](#).

# Copilot in Purview

FastTrack provides remote guidance for:


- Onboarding assistance, including:
  - Provisioning Security Compute Units (SCUs).
  - Configuring default environments.
- Walkthroughs for Copilot for Purview embedded experiences, including:
  - Data loss prevention (DLP):
    - Using alert summaries (full alert summaries within the solution).
    - Using Security Copilot-powered DLP policy insights.
    - Using advanced hunting.
      - Expanding prompts available in DLP beyond the alert summary, like data and user-specific investigation.
  - Using activity explorer.
    - Security Copilot prompts in activity explorer provide responses about activity data and generate filters.
  - Insider risk management:
    - Using alert summaries (full alert summaries within the solution).
    - Using advanced hunting.
      - Expanding prompts available in insider risk management beyond the alert summary, like user-specific investigation.
  - Compliance:
    - Reviewing eDiscovery evidence summaries.
    - Using eDiscovery natural language search.

- Using eDiscovery case summaries.
- Using communication compliance contextual summaries.

## Out of scope

- Detailed pricing information. Contact your account team for more information.
- Providing walkthroughs of standalone experiences.

## Microsoft advanced deployment guides

Microsoft provides customers with technology and guidance to assist with deploying your Microsoft 365, Microsoft Viva, and security services. We encourage our customers to start their deployment journey with [these](#)  offerings.

For non-IT admins, see [Microsoft Purview setup guides](#).

# Microsoft Sentinel

06/03/2025

## Zero Trust

FastTrack provides comprehensive guidance on implementing Zero Trust security principles. The Zero Trust model assumes breach and verifies each request as though it originates from an uncontrolled network. This approach ensures robust security across your networks, applications, and environment. FastTrack accomplishes this by focusing on identity, devices, applications, data, infrastructure, and networks. With FastTrack, you can confidently advance your Zero Trust security journey and protect your digital assets effectively.

With Microsoft Sentinel, you can implement Zero Trust principles through a comprehensive approach to security that focuses on explicit verification, using least privileged access, and assuming breach. Microsoft Sentinel's advanced threat detection, incident management, and automated response features help identify and mitigate threats quickly, ensuring that any potential breaches are contained and addressed promptly.

## Microsoft Sentinel

Microsoft Sentinel is a scalable, cloud-native solution that provides security information and event management (SIEM) and security orchestration, automation, and response (SOAR). It delivers intelligent security analytics and threat intelligence across your enterprise. With Microsoft Sentinel, you get a single solution for attack detection, threat visibility, proactive hunting, and threat response.

Microsoft Sentinel provides a view across your enterprise, including:

- Reducing the impact of sophisticated attacks.
- Minimizing alert fatigue by prioritizing critical alerts.
- Shortening incident resolution times.

FastTrack provides remote guidance for:

- Providing an overview of the prerequisites for Microsoft Sentinel deployment.
- Providing conceptual workspace architecture best practices and considerations, including multi-tenancy scenarios.\*
- Helping prioritize data connectors to optimize Microsoft Sentinel configuration, including:
  - Explaining data transformation and collection customization to assist with optimization.\*
- Planning roles and permissions.

- Conducting cost expectation analysis based on planned configuration.\*
- Enabling the Microsoft Sentinel service.
- Discussing and configuring data retention.
- Configuring data connectors, including:
  - Setting up Microsoft data connectors.
  - Demonstrating how to configure non-Microsoft data connectors.\*
  - Exploring ingestion cost expectations.\*
- Configuring analytics rules, including:
  - Built-in analytics rules.
  - A query starter pack.
  - More rules for Zero Trust and insider threats.
  - User entity behavior analytics rules.
  - Apache Log4J enhancements.
- Providing an overview of the following items:
  - Security operations center (SOC) optimization.
  - Workbooks.
  - Watchlists.
  - User and entity behavior analytics (UEBA).
  - Logic app playbooks.
  - Incident response capabilities\*, simulations, and tutorials (like practice scenarios, fake malware, and automated investigations).

\*Supported with limitations.

## Out of scope

- Attack simulations (including penetration testing).
- Diagnosis of threats and threat hunting.
- Creation and configuration of Log Analytics workspaces.
- Troubleshooting issues encountered during engagement (including networking issues).
- Configuration of non-Microsoft or custom connectors.
- Configuration of data transformation.
- Migration from Microsoft Monitoring Agent (MMA) to Azure Monitor Agent (AMA).
- Complete conversations around non-Microsoft SIEM and SOAR solutions.
- Assisting with non-Microsoft SIEM and SOAR configuration.
- Migrations from non-Microsoft SIEM and SOAR solutions.
- Advanced SIEM Information Model (ASIM) parsers.
- Jupyter Notebooks.
- Azure Synapse and Azure Data Lake solutions.
- Preview features.
- Common Event Format (CEF)- and Syslog-filtered ingestion through AMA.

# Microsoft advanced deployment guides

Microsoft provides customers with technology and guidance to assist with deploying your Microsoft 365, Microsoft Viva, and security services. We encourage our customers to start their deployment journey with [these](#) offerings.

For non-IT admins, see [Microsoft 365 Setup](#).

## Employee Experience featuring Microsoft Viva

The FastTrack Viva team is set to drive AI transformation (Microsoft 365 Copilot) for customers through Microsoft Viva. We focus on utilizing both included capabilities (with Copilot licenses) and premium capabilities (with Viva Premium licenses) to enhance the value of Microsoft 365 Copilot for customers. Central to the deployment strategy are key features like the Microsoft Copilot Dashboard, Microsoft Copilot Academy, and the Microsoft 365 Copilot adoption community. This provides customers with the necessary tools and insights to effectively implement and utilize Microsoft 365 Copilot within their organizations.

### Source environment expectations

Microsoft Viva is built on top of the Microsoft 365 suite you currently use. Core deployments should include Office 365, Teams, modern SharePoint, and Viva Engage. Other scenario configuration details are listed for each respective service in the following Microsoft Viva sections.

The products covered here include:

- [Viva Connections](#)
- [Viva Engage](#)
- [Viva Insights](#)
- [Viva Learning](#)
- [Viva Goals](#)
- [Viva Glint](#)
- [Viva Amplify](#)
- [Viva Pulse](#)

#### ⓘ Note

Viva Goals will be retired on December 31, 2025.

## Viva Connections

Viva Connections encourages meaningful connections while fostering a culture of inclusion and aligning the entire organization around your vision, mission, and strategic priorities.

FastTrack provides remote guidance for:

- Assigning licenses and roles.
- Creating Viva Connections experiences.
- Setting up the default experience.
- Enabling Viva Connections dashboard and resources.
- Creating out-of-box adaptive cards for the dashboard.
- Setting audience targeting and Viva Connections access permissions.
- Enabling, installing, and pinning the Viva Connections Teams app.

## Out of scope

- Creation and integration of custom, third-party, or partner adaptive cards for the dashboard.
- SharePoint site architecture, configuration, branding, design, and web parts.
- SharePoint data, site, or third-party migration.
- On-premises SharePoint Server management or configuration.
- Project management (including defining success criteria).
- Adoption and change management activities.

## Viva Engage

Viva Engage delivers high-value experiences including community building, leadership engagement, knowledge sharing, and self-expression.

FastTrack provides remote guidance for:

- Assigning licenses and roles.
- Enabling native mode.
- Configuring Viva Engage admin settings.
- Enabling and configuring seeded and premium features of Viva Engage.
- Creating and managing Viva Engage communities.
- Setting up a Microsoft 365 Copilot adoption community.
- Enabling, installing, and pinning the Viva Engage Teams app.

## Out of scope

- Viva Engage APIs.
- Managing external networks.
- Setting up an external app or device for live events.
- Data migration.



- Integrating third-party apps.
- Project management (including defining success criteria).
- Adoption and change management activities.

## Viva Insights (including Copilot Analytics)

Viva Insights helps individuals, managers, and business leaders gain personalized insights and actionable recommendations.

FastTrack provides remote guidance for:

- Assigning licenses and roles.
- [Configuring personal insights features](#).
- Configuring Microsoft Copilot Dashboard.
- Configuring the Viva Insights admin portal (Analyst Workbench).
- Uploading the organizational data file.
- Surveying data uploads for Copilot sentiment analysis in the Microsoft Copilot Dashboard
- Surveying business data uploads for the Copilot business outcome report.
- [Enabling the Microsoft Power BI templates](#) in the Viva Insights portal.
- Creating of queries in Viva Insights portal.
- Enabling, installing, and pinning the Viva Insights Teams app.

## Out of scope

- Interpreting or analyzing data in Viva Insights reports or query results.
- Developing custom reports.
- Third-party integrations.
- Project management (including defining success criteria).
- Adoption and change management activities.

## Viva Learning

Viva Learning enables employees to discover, share, and track learning from various content sources. It enables business leaders to drive a culture of learning through empowered time management and coaching.

FastTrack provides remote guidance for:

- Assigning licenses and roles.
- Configuring Viva Learning admin settings.
- Enabling SharePoint integration.

- Configuring Viva Learning settings for supported learning management systems (LMSs).
- Enabling, installing, and pinning the Viva Learning Teams app.

## Out of scope

- Enabling single sign-in (SSO) for third-party providers.
- Enabling learning record sync for third-party providers.
- Enabling permissions sync for third-party providers.
- Integrating third-party provider using Viva Learning APIs.
- Project management (including defining success criteria).
- Adoption and change management activities.

## Viva Goals

### ⓘ Note

Viva Goals will be retired on December 31, 2025.

Viva Goals immerses everyone in the company's purpose and top priorities with a goal alignment solution that creates a culture of engaged employees achieving results.

FastTrack provides remote guidance for:

- Assigning licenses and roles.
- Configuring organization creation rules.
- Configuring admin settings.
- Enabling Viva Goals integrations.
- Enabling, installing, and pinning the Viva Goals Teams app.

## Out of scope

- Creating custom solutions for specific business needs.
- Development or writing custom code.
- Data migrations from third-party sources to Viva.
- Analyzing or interpreting data generated by the Viva apps.
- Writing and entering customer-specific objectives and key results (OKRs).
- Creation of adoption and change management deliverables.
- Conducting project management for deployment.
- Training of end users.

# Viva Glint

Viva Glint helps organizations capture valuable employee feedback and translate insights to actions, helping managers and teams to measure and improve their employee experience.

FastTrack provides remote guidance for:

- Assigning licenses to users.
- Reviewing required network connectivity.
- Setting up allowlists.
- Provisioning your Viva Glint tenant.
- Assigning company admin roles.
- Configuring Secure File Transfer Protocol (SFTP).
- Setting up user attribute structures.
- Uploading employee data and attributes.
- Reviewing Viva Glint General Settings.
- Setting up app features and settings.
- Reviewing survey access methods.
- Setting up survey distribution lists.

## Out of scope

- LinkedIn and third-party Viva Glint migrations.
- Survey program design.
- Executive consultation on survey insights.
- Viva Glint leader training.
- Viva Glint reports and dashboards.
- Deployment and launch support.
- Guidance on platform optimization, administration, and maintenance.
- Import of historical response data.

# Viva Amplify

Viva Amplify empowers leaders and communicators to elevate their message and energize their people by meeting employees where they are.

FastTrack provides remote guidance for:

- Assigning licenses and roles.
- Configuring Viva Amplify admin settings.
- Managing who can create campaigns.
- Managing organizational data.

## Out of scope

- User trainings.
- Adoption activities.

## Viva Pulse

Viva Pulse empowers leaders and managers to understand their team's experience and needs in the moment. Viva Pulse enables team leads to send brief surveys using research-backed templates to get a snapshot of team sentiment and act on feedback. Additionally, Viva Pulse reporting enables analysis of results and trends so leads can pinpoint what's working well and which areas to focus on over time.

FastTrack provides remote guidance for:

- Assigning licenses and roles.
- Reviewing Viva Pulse email notification settings.
- Reviewing in-app Viva Pulse admin settings.
- Providing admin management of survey template and question libraries
- Providing integration with Microsoft Copilot Dashboard.
- Allowing, installing, and pinning Viva Pulse using the Microsoft Teams app.

## Out of scope

- Survey question design.
- Training for users or managers.
- Project management (including defining success criteria).
- Adoption and change management activities.

## Microsoft advanced deployment guides

Microsoft provides customers with technology and guidance to assist with deploying your Microsoft 365, Microsoft Viva, and security services. We encourage our customers to start their deployment journey with [these](#) offerings.

For non-IT admins, see [Deploy employee experience with Microsoft Viva](#).

# Office 365

06/05/2025

## Exchange Online

For Exchange Online, FastTrack guides you through the process to get your organization ready to use email. The exact steps depend on the source environment and email migration plans.

FastTrack provides remote guidance for:

- Pointing your mail exchange (MX) records to Office 365.
- Setting up the data loss prevention (DLP) and Office 365 Message Encryption (OME) features for all mail-enabled domains validated in Office 365 as part of your subscription service.
- Configuring firewall ports and setting up DNS (Domain Name System), including the required Autodiscover, sender policy framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting, and Conformance (DMARC) and MX records (as needed).
- Setting up email flow between the source messaging environment and Exchange Online/Office 365 (as needed).
- Planning and preparing for mail migration from the source messaging environment to Office 365.
- Configuring mailbox clients (Outlook for Windows, Outlook on the web, and Outlook for iOS and Android).
- Setting up Exchange Online Protection features for all mail-enabled domains validated in Office 365.

### Note

The Mailbox Replication service (MRS) attempts to migrate Information Rights Managed (IRM) emails from your on-premises mailbox to the corresponding Exchange Online mailbox. Ability to read the protected content post-migration depends on the customer mapping and copying Active Directory Rights Managed Services (AD RMS) templates to the Azure Rights Management Service (Azure RMS).

## Data migration

For information on using the FastTrack benefit for data migration to Office 365, see [Data Migration](#).

# Source environment expectations

Your source environment must have one of the following minimum levels:

- Single or multiple Exchange organizations with Exchange Server 2010 onward.
- A single Google Workspace environment (Gmail, Contacts, and Calendar only).

For information on Multi-Geo Capabilities, see [Multi-Geo Capabilities in Exchange Online](#).

Online client software like Project for Office 365, Outlook for Windows, Outlook for iOS and Android, OneDrive sync client, Power BI Desktop, and Skype for Business must be at a minimum level as defined in [System requirements for Microsoft 365 Office](#).

## Microsoft Teams

### Microsoft Teams core and Teams Premium (including chat, collaboration, and meetings)


FastTrack provides remote guidance for:

- Teams prerequisites:
  - Identities enabled in Microsoft Entra ID for Microsoft 365.
  - Exchange mailboxes are present (online and on-premises in an Exchange hybrid configuration).
  - Users are enabled for SharePoint and OneDrive.
  - Microsoft 365 Groups are enabled.
- Network readiness:
  - Network port and enablement checks.
  - Domain Name System (DNS) settings.
  - Proxy settings.
  - Connection quality checks.
  - Bandwidth checks.
  - Guidance for Call Analytics and Call Quality Dashboard (CQD).
- Security and compliance readiness:
  - Develop governance and compliance policies including hardware security and account security, like multifactor authentication (MFA) guidance and password policies.
- Teams chat and collaboration:
  - Teams basics.
  - Managing and organizing Teams.
  - Presence.
  - Messaging policies.

- Channels (standard, shared, and private).
- Teams meetings and Audio Conferencing:
  - Meeting settings and policies.
  - Service number acquisition.
  - Guidance for conference bridge settings.
  - Assignment of dial-in numbers to meeting organizers.
- Enabling Teams live events, town halls, and webinars:
  - Organizational setup of live events, town halls, and webinar policies.
  - Configuring Microsoft eCDN for large events like town halls and webinars (requires Teams Premium licenses).
- The new virtual desktop infrastructure (VDI) solution for Teams, including prerequisites and configuration for Azure Virtual Desktop, Windows 365, and Citrix.
- Microsoft Places (requires Teams Premium licenses):
  - Reviewing prerequisites for work plans, hybrid RSVP, Places finder (including maps and rooms facilities), room booking enhancements, and space analytics.
  - Providing guidance for configuring buildings, floors, desk pools and workplaces, adding existing Indoor Mapping Data Format (IMDF) floorplans (maps), updating resource mailboxes metadata, and rooms check-in and auto release policies.
  - Enabling Microsoft Places for users including space analytics (users and buildings).
  - Deploying the Microsoft Places app in new Outlook and new Teams clients.

## Microsoft Teams Rooms

FastTrack provides remote guidance for:

- Network, security, and compliance readiness:
  - Validation of network, security, and compliance readiness requirements for Teams Rooms.
- Resource accounts:
  - Creation and configuration of resource accounts needed for supported Teams Rooms devices including license assignment and mailbox configuration.
- Device setup:
  - Guidance on the out-of-the-box experience of a new Teams Rooms device.
- Device management:
  - Device management, including Teams admin center, Microsoft Intune, and Teams Rooms Pro Management service.
- Certified devices:
  - Guidance on using the [Teams Device Catalog](#)  to find and purchase certified devices.

## Microsoft Teams Phone

FastTrack provides remote guidance for:

- Network, security, and compliance readiness:
  - Validation of network, security, and compliance readiness requirements for Teams Phone.
- Teams Phone configuration:
  - Organizational setup for Teams Phone settings.
    - Call queues.
    - Auto attendants.
    - Communications credits.
    - Cloud voicemail.
    - Caller ID.
    - Calling policies.
    - Emergency calling.
  - Shared Calling configuration.
- The Queues app (requires Teams Premium licenses):
  - Configuring and deploying the Queues app.
  - Managing authorized users and setting voice app policies.
  - Integrating with Call queue and Auto attendant authorized users.
- Operator Connect:
  - Enabling Operator Connect.
  - Emergency addresses.
  - Assigning numbers.
- Teams Phone Mobile:
  - Teams Phone Mobile license acquisition and assignment.
  - Enabling a mobile operator.
  - Assigning numbers.
- Calling Plans:
  - Local number porting guidance through user interface (UI) up to 999 numbers.
  - Porting service request (SR) support over 999 numbers.
  - License assignment.
  - Phone number acquisition and assignment.
- Direct Routing:
  - Guidance on Direct Routing.
  - Session Border Controller (SBC) configurations and connectivity.
  - Call routing policies.
  - Media bypass.
  - Local media optimization.
  - Assigning numbers.

## Skype to Microsoft Teams migrations



FastTrack provides remote guidance for:

- Migration from Skype for Business on-premises to Teams.

## Out of scope

- A/V and conference rooms design and installation.
- Device procurement.
- Non-Microsoft integrations (like Cloud Video Interop (CVI)).
- Carrier Session Initiation Protocol (SIP) trunk configuration.
- Session Border Controller (SBC) trunking to carrier or legacy Private Branch Exchange (PBX).
- Troubleshooting existing deployments.
- End-user training.
- Hands-on keyboard support.
- Production of live events or webinars.
- Microsoft Places:
  - Map and floor plan conversion to IMDF and spatial data correlation.
  - Onboarding and integrating non-Microsoft occupancy signals with space analytics.

## SharePoint and OneDrive

FastTrack provides remote guidance for:

- Planning site collections.
- Securing content and managing permissions.
- Configuring SharePoint features, like site creation, site management, site sharing, web parts, search, content types, and site navigation.
- Configuring SharePoint hybrid features, like hybrid search, hybrid sites, hybrid taxonomy, content types, hybrid self-service site creation (SharePoint Server 2013 only), extended app launcher, hybrid OneDrive, and extranet sites.
- Planning for content migration.
- Configuring external sharing settings.
- Deploying Conditional Access.

Further guidance is provided for OneDrive like:

- Redirecting or moving known folders to OneDrive.
- Deploying OneDrive sync clients.

## Data migration

For information on using the FastTrack benefit for data migration to Office 365, see [Data Migration](#).

## Source environment expectations

- The source SharePoint environment must be one of the following on-premises SharePoint Server environments: 2013, 2016, or 2019.
- Data migration services migrate data from these source environments:
  - File shares (Server Message Block (SMB) file shares on devices supporting SMB 2.0 onward).
  - A single Google Workspace environment (Google Drive only).
  - Box (Starter, Business, Enterprise).
  - Dropbox for Teams (Standard and Advanced).

### ⓘ Note

Upgrade of on-premises SharePoint environments to SharePoint Server isn't in scope. Contact a [Microsoft Partner](#) <sup>↗</sup> for assistance. For more information, see [Minimum public update levels for SharePoint hybrid features](#) <sup>↗</sup>.

### ⓘ Note

For information on Multi-Geo Capabilities, see [Multi-Geo Capabilities in OneDrive and SharePoint in Office 365](#) <sup>↗</sup>.

## Microsoft advanced deployment guides

Microsoft provides customers with technology and guidance to assist with deploying your Microsoft 365, Microsoft Viva, and security services. We encourage our customers to start their deployment journey with [these](#) <sup>↗</sup> offerings.

For non-IT admins, see [Microsoft 365 Setup](#) <sup>↗</sup>.

# Windows and Other Services

06/06/2025

## Windows 11

FastTrack provides remote guidance for updating to Windows 11 from Windows 10.

This includes:

- Planning for your Windows 11 deployment.
- Assessing the source environment and the requirements.
- Deploying Windows 11 Enterprise and Microsoft 365 Apps using Microsoft Intune.
- Recommending options to assess Windows 11 app and driver readiness.
- Providing update guidance for Windows 11 Enterprise devices that meet Windows 11 system requirements.
- Providing update guidance for in-place updates from Windows 10 to Windows 11 using Windows Autopatch and guidance for Windows 11 servicing using Windows Autopatch and Microsoft Intune.
- Providing guidance for new Windows 11 device deployment using Windows Autopilot.
- Providing guidance using Endpoint analytics and Windows Autopatch reports to see eligible devices and monitor device deployments.
- Providing guidance for enabling co-management and moving the update workload to Microsoft Intune.
- Providing guidance to help your organization stay up to date with Windows 11 Enterprise and Microsoft 365 Apps.

### Note

PCs must meet [Windows 11 hardware requirements](#) .

## Out of scope for all Windows 11 products

- Upgrading task sequences or software update feature updates from Configuration Manager.
- Upgrading Configuration Manager to Current Branch.
- Creating custom images for Windows 11 deployment.
- Creating and supporting deployment scripts for Windows 11 deployment.
- Converting a Windows 11 system from BIOS to Unified Extensible Firmware Interface (UEFI).

- Enabling Windows 11 security features.
- Configuring Windows Deployment Services (WDS) for Preboot Execution Environment (PXE) booting.
- Using the Microsoft Deployment Toolkit (MDT) to capture and deploy Windows 11 images.
- Using the User State Migration Tool (USMT).

Contact a [Microsoft Partner](#) for assistance with these services.

## BitLocker

FastTrack provides remote guidance for:

- Assessing the Windows 11 environment and hardware for BitLocker configuration.
- Enabling compliance reporting of BitLocker from Microsoft Intune.
- Providing guidance on configuring BitLocker for Windows Autopilot scenarios.
- Providing guidance on BitLocker key recovery best practices.

## Windows Hello for Business

FastTrack provides remote guidance for:

- Assessing the Windows environment and hardware for Windows Hello for Business configuration.
- Enabling Windows passwordless authentication using Windows Hello for Business cloud trust.
- Planning guidance for Windows Hello for Business hybrid key or certificate trust.

## Windows Autopatch

FastTrack provides remote guidance for:

- Assistance in understanding the features of the Windows Autopatch service, validating environment prerequisites, and how the service relates to other Microsoft update tools.
- Assessing company readiness for Windows Autopatch onboarding using the Readiness Assessment tool and addressing issues identified by the tool.
- Understanding the process to enroll into the Windows Autopatch service.
- Registering physical and virtual devices into the Windows Autopatch service.
- Validating device updates and understanding reports.

## Microsoft Defender for Endpoint

For more information, see [Microsoft Defender for Endpoint](#).

## Source environment expectations

The following requirements must be met.

For PC update:

- Source OS: Windows 10 Enterprise or Professional.
- Devices: Desktop, notebook, or tablet form factor.
- Target OS: Windows 11 Enterprise.

## Windows 365

FastTrack provides remote guidance for onboarding to Windows 365 Enterprise, Windows 365 Frontline, and Windows 365 Government. Windows 365 takes the operating system to the Microsoft Cloud, securely streaming the full Windows experience—including all your apps, data, and settings—to your personal or corporate devices. Organizations can provision Windows 365 Cloud PCs (devices that are deployed on the Windows 365 service) instantly across the globe and manage them seamlessly alongside your physical PC estate using Microsoft Intune admin center. This desktop-as-a-service (DaaS) solution combines the benefits of desktop cloud hosting with the simplicity, security, and insights of Microsoft 365.

Remote guidance includes:

- Assigning licenses to users.
- Creating and modifying Azure network connections (ANCs).
- Adding and deleting device images, including standard Azure Marketplace gallery images and custom images. Some guidance might be provided around deploying language packs with custom images using the Windows 365 language installer script.
- Creating, editing, and deleting provisioning policies.
- Assisting with dynamic query expressions for dynamic groups and filtering.
- Deploying Windows Update policies for Windows 365 Cloud PCs using Intune.
- Deploying apps (including Microsoft 365 Apps for enterprise and Microsoft Teams with media optimizations) to Windows 365 Cloud PCs using Microsoft Intune.
- Securing Windows 365 Cloud PCs, including Conditional Access, multifactor authentication (MFA), and managing Remote Desktop Protocol (RDP) device redirections.
- Managing Windows 365 Cloud PCs on Microsoft Intune admin center, including remote actions, resizing, and other administrative tasks.
- Optimizing end user experience.
- Deploying and managing Windows 365 Frontline Cloud PCs.
- Deploying and managing Windows 365 Government Cloud PCs.

- Finding other support for Windows 365.
- Supporting Windows 365 Link, including:
  - Providing an overview of Windows 365 Link, its capabilities, and use cases.
  - Preparing for deployment and requirements, including enabling single sign-on (SSO).
  - Deploying Windows 365 Link.
  - Managing, updating, and securing Windows 365 Link with Microsoft Intune.
  - Providing guidance on troubleshooting Windows 365 Link.

#### ⓘ Note

See [Microsoft Defender XDR](#) and [Microsoft Defender for Endpoint](#) for details about Microsoft Defender for Endpoint and the security baseline scope as it applies to Windows 365.

## Out of scope

- Creation of Azure subscription features including Azure Virtual Networks (VNETs), ExpressRoute, and Site-to-Site (S2S) VPN.
- Support for advanced networking topics.
- Customizing images for a Windows 365 Cloud PC on behalf of customers.
- Standalone use of Configuration Manager for managing Windows 365 Cloud PCs.
- Deploying Windows updates for Windows 365 Cloud PCs using Configuration Manager.
- Migrating virtual desktop infrastructure (VDI) or Azure Virtual Desktop virtual machines to Windows 365.
- Migrating Configuration Manager or Microsoft Deployment Toolkit (MDT) images to Azure.
- Migrating user profiles to or from Windows PCs.
- Configuring network appliances on behalf of customers.
- Programmatic actions using Microsoft Graph API.
- Support for non-Microsoft integrations.
- Support for Windows 365 Business.
- Windows 365 Link:
  - Providing hardware support.
  - Providing support for third-party product and feature integrations.

Contact a [Microsoft Partner](#) or [Microsoft FastTrack for Azure](#) for assistance with items out of scope and/or if source environment expectations aren't met. If facing concerns about app compatibility, contact [Microsoft App Assure](#).

## Source environment expectations

Before onboarding the following is required:

- Windows 365 [licensing requirements](#) must be met.
- If not using a Microsoft-hosted network:
  - An Azure subscription associated with the Microsoft Entra tenant where licenses are deployed must be used.
  - A virtual network is deployed in a region that's supported for Windows 365. The virtual network should:
    - Have sufficient private IP addresses for the number of Windows 365 Cloud PCs in order to deploy.
    - Have connectivity to Active Directory (only for Microsoft Entra hybrid joined configuration).
    - Have DNS servers configured for internal name resolution.

#### Note

FastTrack doesn't provide onboarding assistance for Azure Virtual Desktop. Customers should work with an Azure partner for Azure Virtual Desktop assistance.

## Universal Print

FastTrack provides remote guidance for:

- Onboarding and configuring Universal Print.
- Universal Print connector.
- Universal Print-ready printers.
- Deploying printers with Microsoft Intune.
- Printer and print job management.
- Configuring the Universal Print PowerShell module.

## Out of scope

- Partner integrations.
- Non-Microsoft app virtualization and deployment.
- Creating custom scripts with the Universal Print PowerShell module.
- Universal Print developer features (including API).
- Configuring Windows servers for printing.

## Source environment expectations

- The customer has one of the following licenses:
  - Microsoft 365 Enterprise F3, E3, or E5.
  - Microsoft 365 Education A3 or A5.
  - Microsoft 365 Business Premium.
  - Microsoft 365 G3, G5 - GCC.
  - Microsoft 365 E3, E5 - GCC High.
  - Windows 10/11 Enterprise E3 or E5.
  - Windows 10/11 Education A3 or A5.
  - Windows 10/11 Enterprise E5 Commercial (GCC Compatible).
- Microsoft Entra ID tenant setup (any edition).
- Universal Print connector host and/or Universal Print-ready printers.
- Client devices must be running Windows 11 or Windows 10 version 1903 or later.

## App Assure

App Assure is a service designed to address issues with Windows and Microsoft 365 Apps app compatibility and is available to all Microsoft customers. When you request the App Assure service, we work with you to address valid app issues. To request App Assure assistance, complete the [App Assure service request](#).

FastTrack also provides guidance to customers who face compatibility issues when deploying Windows 365 Cloud PC, Azure Virtual Desktop, and Microsoft Edge and make every reasonable effort to resolve compatibility issues. We provide remediation assistance for apps deployed on the following Microsoft products:

- Windows 10/11 (including Arm64 devices).
- Microsoft 365 Apps, including Microsoft 365 Copilot.
- Microsoft Edge - For deployment guidance, see [Overview of the Microsoft Edge channels](#).
- Azure Virtual Desktop - For more information, see [What is Azure Virtual Desktop?](#) and [Windows 10 Enterprise multi-session FAQ](#).
- Windows 365 Cloud PC - For more information, see [Introducing a new era of hybrid personal computing: the Windows 365 Cloud PC](#).

FastTrack [eligibility criteria](#) doesn't apply to App Assure services and is subject to the discretion of Microsoft.

### ⓘ Note

App Assure supports Microsoft 365 Copilot customers by addressing app compatibility issues encountered when moving to a monthly update channel.



## Out of scope

- App inventory and testing to determine what does and doesn't work on Windows and Microsoft 365 Apps. For more information, see the [Windows and Office 365 deployment lab kit](#). If you're interested in guidance for modernizing endpoints or deploying Windows 11, [request assistance from FastTrack](#).
- Researching non-Microsoft ISV apps for Windows compatibility and support statements.
- App packaging-only services. However, the App Assure team packages Windows apps that we remediated to ensure they can be deployed in the customer's environment.
- Although Android apps on Windows 11 are available to Windows Insiders, App Assure doesn't currently support Android apps or devices, including Surface Duo devices.

## Customer responsibilities

- Creating an app inventory.
- Validating those apps on Windows and Microsoft 365 Apps.

### ⓘ Note

Microsoft can't make changes to your source code. However, the App Assure team can provide guidance to app developers if the source code is available for your apps.

Contact a [Microsoft Partner](#) for assistance with these services.

## Source environment expectations

### Windows and Microsoft 365 Apps

- Apps that worked on Windows 7, Windows 8.1, Windows 10, and Windows 11 also work on Windows 10/11.
- Apps that worked on Office 2010, Office 2013, Office 2016, and Office 2019 also work on Microsoft 365 Apps (32-bit and 64-bit versions).

### Windows 365 Cloud PC

Apps that worked on Windows 7, Windows 8.1, Windows 10, and Windows 11 also work on Windows 365 Cloud PC.

### Windows on Arm

Apps that worked on Windows 7, Windows 8.1, Windows 10, and Windows 11 also work on Windows 10/11 on Arm64 devices.

**ⓘ Note**

x64 (64-bit) emulation is available on Windows 11 on Arm devices.

## Microsoft Edge

If your web apps or sites work on supported versions of Google Chrome or any version of Microsoft Edge, they'll also work on the latest version of Microsoft Edge. As the web is constantly evolving, be sure to review this published list of [known site compatibility-impacting changes for Microsoft Edge](#).

**ⓘ Note**

App Assure helps you configure IE mode to support legacy Internet Explorer web apps or sites. Support for development to modernize Internet Explorer web apps or sites to run natively on the Chromium engine isn't covered under this benefit.

## Azure Virtual Desktop

Apps running on Windows 7, Windows 8.1, Windows 10, Windows 11, or Windows Server (as virtualized apps) also run on:

- Windows 10/11 Enterprise.
- Windows 10/11 Enterprise multi-session.

**ⓘ Note**

Onboarding assistance for Azure Virtual Desktop is provided by [FastTrack for Azure](#)<sup>↗</sup>. Customers should contact [FastTrack for Azure](#)<sup>↗</sup> to check for eligibility since Azure has separate [eligibility requirements](#)<sup>↗</sup>. If the customer doesn't qualify, they should work with an Azure partner.

**ⓘ Note**

Windows Enterprise multi-session compatibility exclusions and limitations include:

- Limited redirection of hardware.
- A/V-intensive apps might perform in a diminished capacity.
- 16-bit apps aren't supported for 64-bit Azure Virtual Desktop.

## Arm Advisory Service

The App Assure Arm Advisory Service is a no-cost service available to Windows on Arm developers where App Assure engineers assist with porting applications to Arm and building Arm-native applications.

FastTrack provides remote guidance for:

- Delivering a technical workshop for developing best practices, including answering specific implementation questions.
- Suggesting which platform features can be used to enhance application experience.
- Providing code review and code samples to enable development.
- Providing break-fix assistance if issues arise while building or porting apps.
- Providing engineering escalation to enable software development efforts and provide product feedback.

To contact App Assure for this service, complete the [Windows Arm Advisory Service](#) enrollment form.

### ⓘ Note

Developers without access to Arm-based hardware can [create a Windows on Arm virtual machine](#) to develop, build, and test applications in a native environment.

### ⓘ Important

Please be aware that Microsoft reserves the right to limit this offer to 15 hours per Arm developer and to waitlist developers due to high volume.


## Microsoft 365 Apps

FastTrack provides remote guidance for:

- Addressing deployment issues.

- Assigning end-user and device-based licenses using the Microsoft 365 admin center and Windows PowerShell.
- Installing Microsoft 365 Apps from the Office 365 portal using Click-to-Run.
- Installing Office Mobile apps (like Outlook Mobile, Word Mobile, Excel Mobile, and PowerPoint Mobile) on your iOS or Android devices.
- Configuring update settings using the Office 365 Deployment Tool.
- Selection and setup of a local or cloud installation.
- Creation of the Office Deployment Tool configuration XML with the Office Customization Tool or native XML to configure the deployment package.
- Deployment using Microsoft Endpoint Configuration Manager, including assistance with the creation of Microsoft Endpoint Configuration Manager packaging. Additionally, if you have a macro or add-in that worked with prior versions of Office and you experience compatibility issues, FastTrack provides guidance to remediate the compatibility issue at no extra cost through the App Assure program.

#### Important

Online client software must be at a minimum level as defined in the [System requirements for Microsoft 365 and Office](#) .

## Network health

Alignment with the Microsoft [principals of network connectivity](#) is vital to the successful onboarding of FastTrack Services. As such, FastTrack provides remote guidance to obtain and interpret data from a customer's environment subject to the terms of the customer agreement to verify this alignment. This highlights a company's network score, which directly impacts migration velocity, user experience, service performance, and reliability. FastTrack also guides our customers through necessary remediation steps highlighted by this data to help improve the network score.

## Source environment expectations

- Microsoft 365 admin center access.
- Up-to-date versions of Microsoft 365 apps are required.
- Location services enabled as per [Network performance recommendations in the Microsoft 365 Admin Center \(preview\)](#).

## Microsoft Edge

FastTrack provides remote guidance for:

- Deploying Microsoft Edge on Windows 10/11 with Microsoft Intune admin center (Microsoft Endpoint Configuration Manager or Microsoft Intune).
- Configuring Microsoft Edge (using group policies or Microsoft Intune app configuration and app policies).
- Migrating web apps or sites from Google Chrome to Microsoft Edge. Additionally, if you have a web app or site that works with Google Chrome and you experience compatibility issues, FastTrack provides guidance to resolve the issue at no extra cost. To request compatibility support for App Assure, sign in to the [FastTrack portal](#) to start an engagement.
- Planning guidance for Microsoft Edge adoption and configuration guidance for Microsoft Search bookmarks.

## Microsoft advanced deployment guides

Microsoft provides customers with technology and guidance to assist with deploying your Microsoft 365, Microsoft Viva, and security services. We encourage our customers to start their deployment journey with [these](#) offerings.

For non-IT admins, see [Deploy and configure Microsoft Edge](#).

# Data Migration

Article • 10/30/2024

FastTrack can help you migrate mail and file data in your source environments to Office 365 (Exchange Online, SharePoint, and OneDrive).

The type of assistance we provide depends on your number of Office 365 licenses:

- **For Office 365 tenants with 150-499 licenses:** FastTrack provides migration guidance only; you're responsible for performing the data migration. We guide you through documentation that helps you plan and use free tools to perform a self-service migration.
- **For Office 365 tenants with 500 or more licenses:** FastTrack provides migration guidance and data migration services. We provide guidance to help you plan your migration, configure your source environments and Office 365 tenant, and use our data migration services to migrate your data. You create and schedule your migration events. We launch migration events in accordance with your schedule, monitor their progress, and provide status reports.

## ⓘ Note

For education plans, your paid faculty/educator licenses are eligible for data migration services. A1 students are only eligible when migrating with paid faculty/educators and when also migrating from Exchange or Google Workspace. For education plans, your paid faculty/educator licenses are eligible for data migration services for content migrations. This includes data within Box, Dropbox, Google Drive, and file share.

## Considerations

- Your source environments must meet specific expectations in order to migrate data to Office 365. For more information, see [Office 365](#) on the source environment expectations for Exchange, SharePoint, and OneDrive.
- We require appropriate access and permissions to your source environments and Office 365 tenant to provide data migration services.
- Our data migration services aren't designed or intended for data subject to special legal or regulatory requirements. As we migrate your data, it can be transferred to, stored, and processed anywhere that we maintain facilities (except as otherwise provided for your FastTrack migration project).

### ⓘ Note

For GCC customers, Gmail, Exchange, and file share migrations are supported. Box, Dropbox, and Google Drive migrations aren't supported.

- We can't guarantee the speed of mail or file migrations.
- Unforeseen issues (like unreadable or corrupt items in the source environment) might prevent our ability to migrate some of your data items.
- External factors beyond our control (like changes to third-party application programming interfaces (APIs)) can result in changes to, delays in, or suspension of our data migration services.

## Migration service availability

- **For Commercial customers:** We provide data migration services 24 hours a day, seven (7) days a week (24x7) (English only).
- **For US Government customers:** We provide data migration services 24 hours a day, five (5) business days a week (24x5).

## Migration to Exchange Online

When you choose to use FastTrack to migrate your email to Exchange Online, we provide migration guidance and data migration services. We provide guidance to help you plan your migration, configure your source environments and Exchange Online, and use our data migration services to migrate your mailboxes. You create and schedule your migration events. We launch migration events in accordance with your schedule, monitor their progress, and provide status reports. When your migration events complete, you can expect mail from appropriately scheduled and eligible source mailboxes of your migrated source environments to Exchange Online.

## Considerations

- Before migration, you must complete FastTrack core onboarding for Exchange Online.
  - If you performed onboarding yourself, you must pass the required checks and prerequisites. Refer to [Exchange Online](#) for details.
- FastTrack migrates only to active Office 365 mailboxes.
- You must satisfy specific requirements if you intend to migrate from an on-premises Exchange environment. Refer to [Hybrid deployment prerequisites](#) [↗](#) for

details.

- Each source environment must be on the latest service pack (SP) and rollup (RU)/cumulative update (CU) level for the respective product in the source environment.
- Distribution lists (*MailEnabledGroup* objects) and external contacts (*MailEnabledContact* objects) that exist in your on-premises Active Directory aren't a part of mailbox data migration. However, you can synchronize them using Microsoft Entra Connect.


## Source environments

Our data migration service migrates data from these source environments:

- A single or multiple Active Directory forests with single or multiple Exchange organizations (each Exchange mail system must be Exchange 2010 or greater).
- Google Workspace environment (Gmail, Contacts, and Calendar only).

The following table presents migration details specific to each source environment:

 Expand table

Source environment	Type of migration	What migrates	What doesn't migrate
Exchange 2010, Exchange 2013, Exchange 2016, Exchange 2019  <b>Note:</b> For on-premises Exchange dependencies, see <a href="#">Hybrid deployment prerequisites</a>  .	Migration with hybrid deployment	<ul style="list-style-type: none"><li>• Emails.</li><li>• Server-side mailbox rules.</li><li>• Delegates.</li><li>• Mailbox contacts.</li><li>• Calendar.</li><li>• Tasks.</li><li>• Rights-managed emails.</li><li>• Encrypted emails.</li><li>• Signatures.</li><li>• Personal archive migrated with the user's mailbox.</li><li>• Recoverable items.</li></ul>	<ul style="list-style-type: none"><li>• Public folders.</li><li>• Any email that exceeds the message size limit.</li><li>• Journaling archive or any third-party archive solution.</li><li>• Blocked or inactive users.</li><li>• Archive data from Personal Storage Table (PST) files.</li><li>• Corrupted items.</li><li>• Inactive mailboxes.</li><li>• Client-side mailbox rules.</li></ul>
Google Workspace environment (Gmail, Contacts, and Calendar only)	Cutover or staged	<ul style="list-style-type: none"><li>• Emails.</li><li>• Mailbox contacts (a maximum of three (3) email</li></ul>	<ul style="list-style-type: none"><li>• Signatures.</li><li>• Any email or attachment that</li></ul>



Source environment	Type of migration	What migrates	What doesn't migrate
<b>Note:</b> Your Google Workspace environment must meet the prerequisites described in <a href="#">Perform a Google Workspace migration</a> .		addresses per contact are migrated). <ul style="list-style-type: none"><li>• Calendar.</li><li>• Labels.</li><li>• Rules.</li><li>• Cloud attachments.</li><li>• Delegates.</li><li>• Tasks.</li></ul>	exceeds the message size limit. <ul style="list-style-type: none"><li>• Blocked or inactive users.</li><li>• Archive data from PST files or any third-party archive solution (for example, Google Vault).</li><li>• Rights managed or encrypted emails.</li><li>• Corrupted items.</li><li>• Google Hangouts.**</li><li>• Google Groups.</li><li>• Resource mailboxes.</li><li>• Inactive mailboxes.</li><li>• Vacation settings and automatic reply settings.</li><li>• Shared calendars, Google Hangout links, and event colors.</li></ul>
			**Hangout conversations saved as label are migrated.

## FastTrack responsibilities for Exchange Online migrations

Our FastTrack Specialists perform standard activities during the migration project. Refer to the data migration responsibilities information in [Exchange Online](#) for details.

Our FastTrack Specialists also perform the following activities, specific to Exchange migrations:

- Provide guidance to help you enable Simple Mail Transfer Protocol (SMTP) mail routing coexistence between your source environments and Exchange Online, if applicable.

## Your responsibilities

You perform standard activities during the migration project. Refer to the data migration responsibilities information in [Exchange Online](#) for details.

You also perform the following activities, specific to Exchange migrations:

- Complete FastTrack core onboarding for Exchange Online. If you performed onboarding yourself, you must pass the required checks and prerequisites. Refer to [Exchange Online](#) for details.
- Install the appropriate level of client software as per Office 365 guidelines.
- Satisfy specific requirements if you intend to migrate from an on-premises Exchange environment. Refer to [Hybrid deployment prerequisites](#) <sup>↗</sup> for details.
- Ensure each source environment is on the latest service pack (SP) and rollup (RU)/cumulative update (CU) level, if applicable.
- Configure and validate SMTP mail routing coexistence between your source environments and Exchange Online, if applicable.
- Ensure your source mailbox size doesn't exceed the target mailbox quota. Depending on the source platform, you might need to limit your source data to 85 percent of the target mailbox quota.
- Migrate client-side data if desired. This includes, but isn't limited to, local address books, data in local PST files, Outlook rules, and local Outlook settings.
- Assist your end-users with remediation of client-side migration issues.

## Migration to SharePoint

When you choose to use FastTrack to migrate your files to SharePoint, we provide migration guidance and data migration services. We provide guidance to help you plan your migration, configure your source environments and SharePoint, and use our data migration services to migrate your files. You create and schedule your migration events. We launch migration events in accordance with your schedule, monitor their progress, and provide status reports. When your migration events complete, you can expect files from appropriately scheduled and eligible sources of your migrated source environments to SharePoint.

## Considerations

- All migrations are subject to SharePoint quotas. Refer to [SharePoint limits](#) <sup>↗</sup> for details.
- We recommend that you limit the overall migration amount to 75 percent (%) of the overall SharePoint storage quota (including any extra storage you purchased

separately).

## Source environment details

Our data migration services migrate data from these source environments:

- File shares (Server Message Block (SMB) file shares on devices supporting SMB 2.0 onward).
- A single Google Workspace environment (Google Drive only).
- Box (Starter, Business, Enterprise).
- Dropbox for Teams (Standard and Advanced).

The following table presents migration details specific to each source environment:

[Expand table](#)

Source environment	Type of migration	What migrates	What doesn't migrate
Any file share device supporting SMB 2.0 onward	Single or multi-pass	<ul style="list-style-type: none"><li>• Documents.</li><li>• File and folder structure.</li><li>• User-level file and folder permissions.*</li><li>• Group-level file and folder permissions.*</li><li>• Files under 250 GB.</li><li>• Basic document and folder metadata:<ul style="list-style-type: none"><li>◦ Created date.</li><li>◦ Modified date.</li><li>◦ Created by.</li><li>◦ Last modified by.</li></ul></li></ul> <p>*Directory synchronization configuration required. Only NTFS permissions exposed to the Windows File Explorer are migrated. Permissions managed directly on file share devices aren't migrated. If data is stored on an SMB 2.0 device, the NTFS-equivalent permissions exposed by the SMB protocol are migrated.</p>	<ul style="list-style-type: none"><li>• Ownership history and previous versions.</li><li>• Conversion of embedded URLs in content.</li><li>• Previous versions.</li><li>• Windows file and folder attributes (like read-only and hidden).</li><li>• Non-Windows New Technology File System (NTFS) and NTFS advanced permissions and special settings:</li><li>• Explicit deny permissions (removed after migration, content subject to parallel permissions or permissions on parent folder).</li><li>• NTFS auditing configuration.</li><li>• More file metadata provided by File Classification Infrastructure (FCI).</li><li>• Inaccessible or corrupted documents.</li><li>• Hidden shares.</li></ul>

Source environment	Type of migration	What migrates	What doesn't migrate
			<ul style="list-style-type: none"> <li>• Sharing (like permissions granted on the share level).</li> <li>• Files or folders exceeding current <a href="#">SharePoint restrictions and limitations</a> <sup>↗</sup>.</li> </ul>
Single Google Workspace environment (Google Drive only)	Single or multi-pass	<ul style="list-style-type: none"> <li>• Google Docs, Sheets, and Slides (files are converted to the equivalent Office format), including files over 10 MB.</li> <li>• File and folder structure.</li> <li>• User-level folder permissions.</li> <li>• Group-level folder permissions.</li> <li>• User-level file permissions.</li> <li>• Group-level file permissions.</li> <li>• Files under 15 GB.</li> <li>• Basic document and folder metadata: <ul style="list-style-type: none"> <li>◦ Created date.</li> <li>◦ Modified date.</li> <li>◦ Created by.</li> <li>◦ Last modified by.</li> </ul> </li> <li>• Shared drives (folders and files).</li> <li>• Shared content owned by the Google Drive account being migrated.</li> <li>• Google Sheets are converted to Excel files, but custom scripts, formulas, and macros <b>aren't</b> migrated.</li> </ul>	<ul style="list-style-type: none"> <li>• Ownership history, previous versions, and comments.</li> <li>• File and folder descriptions, folder colors.</li> <li>• Advanced metadata.</li> <li>• Google Forms.</li> <li>• File lock attributes.</li> <li>• Conversion of embedded URLs in content.</li> <li>• Trashed items.</li> <li>• Inaccessible or corrupted documents.</li> <li>• Blocked or inactive users.</li> <li>• Google Photos, Maps, and other connected apps.</li> <li>• Google Drawings.</li> <li>• Shared content external to your organization.</li> <li>• Content not owned by the Google Drive account being migrated.</li> <li>• Permissions and basic metadata of guests. (<b>Note:</b> Use Google Drive Admin reports to identify content shared with guests. Instruct end users to reshare content with guests after migration.)</li> <li>• Shared Drive membership permissions. (<b>Note:</b> Use Google Drive Admin reports to identify shared drive memberships. Instruct end users to configure these membership settings on</li> </ul>

Source environment	Type of migration	What migrates	What doesn't migrate
			<p>the target before migration.)</p> <ul style="list-style-type: none"> <li>Files marked as restricted or not copyable.</li> <li>Files or folders exceeding current <a href="#">SharePoint restrictions and limitations</a> .</li> <li>Google Shortcuts.</li> </ul>
<b>Box (Starter, Business, Enterprise)</b>	Single or multi-pass	<ul style="list-style-type: none"> <li>Documents.</li> <li>File and folder structure.</li> <li>User-level folder permissions.</li> <li>Group-level folder permissions.</li> <li>User-level file permissions.</li> <li>Group-level file permissions.</li> <li>Files under 15 GB.</li> <li>Basic document and folder metadata: <ul style="list-style-type: none"> <li>Created date.</li> <li>Modified date.</li> <li>Created by.</li> <li>Last modified by.</li> </ul> </li> <li>Shared content owned by the Box account being migrated.</li> <li>Box Notes (converted to Word document format).</li> </ul>	<ul style="list-style-type: none"> <li>Ownership history, previous versions, and comments.</li> <li>File and folder descriptions.</li> <li>Box Tags and advanced metadata.</li> <li>File lock attributes.</li> <li>Conversion of embedded URLs in content.</li> <li>Trashed items.</li> <li>Inaccessible or corrupted documents.</li> <li>Blocked or inactive users.</li> <li>Box Apps, Bookmarks, Favorites, and Workflows.</li> <li>Content not owned by the migrated Box account.</li> <li>Permissions and basic metadata of guests. (<b>Note:</b> Use Box reports to identify content shared with guests. Instruct end users to reshare content with guests after migration.)</li> <li>Files or folders exceeding current <a href="#">SharePoint restrictions and limitations</a> .</li> </ul>
<b>Dropbox for Teams (Standard and Advanced)</b>	Single or multi-pass	<ul style="list-style-type: none"> <li>Documents.</li> <li>File and folder structure.</li> <li>User-level folder permissions.</li> <li>Group-level folder permissions.</li> </ul>	<ul style="list-style-type: none"> <li>Ownership history, previous versions, and comments.</li> <li>File and folder descriptions.</li> <li>Advanced metadata.</li> </ul>

Source environment	Type of migration	What migrates	What doesn't migrate
		<ul style="list-style-type: none"> <li>• User-level file permissions.</li> <li>• Group-level file permissions.</li> <li>• Files under 15 GB.</li> <li>• Basic document and folder metadata: <ul style="list-style-type: none"> <li>◦ Created date.</li> <li>◦ Modified date.</li> <li>◦ Created by.</li> <li>◦ Last modified by.</li> </ul> </li> <li>• Shared team folders and content.</li> <li>• Shared content owned by the Dropbox accounts being migrated.</li> </ul>	<ul style="list-style-type: none"> <li>• File lock attributes.</li> <li>• Conversion of embedded URLs in content.</li> <li>• Trashed items.</li> <li>• Inaccessible or corrupted documents.</li> <li>• Unmounted Dropbox folders.</li> <li>• Deleted or disconnected users.</li> <li>• Dropbox Paper, Showcases, and Spaces.</li> <li>• Dropbox Apps and Favorites (Pins/Stars).</li> <li>• Content not owned by the migrated Dropbox account.</li> <li>• Permissions and basic metadata of guests. (<b>Note:</b> Use Dropbox reports to identify content shared with guests. Instruct end users to reshare content with guests after migration)</li> <li>• Files or folders exceeding current <a href="#">SharePoint restrictions and limitations</a> <a href="#">↗</a>.</li> </ul>

## FastTrack responsibilities for SharePoint migrations

Our FastTrack Specialists perform standard activities during the migration project. Refer to the data migration responsibilities information in [SharePoint and OneDrive](#) for details.

### Your responsibilities

You perform standard activities during the migration project. Refer to the data migration responsibilities information in [SharePoint and OneDrive](#) for details.

You also perform the following activities, specific to SharePoint migrations:

- Provision all SharePoint team sites to be targeted by your migration events.

## Migration to OneDrive

When you choose to use FastTrack to migrate your files to OneDrive, we provide migration guidance and data migration services. We provide guidance to help you plan your migration, configure your source environments and OneDrive, and use our data migration services to migrate your files. You create and schedule your migration events. We launch migration events in accordance with your schedule, monitor their progress, and provide status reports. When your migration events complete, you can expect files from appropriately scheduled and eligible sources of your migrated source environments to OneDrive.

## Considerations

- All migrations are subject to SharePoint quotas. Refer to [SharePoint limits](#) for details.
- We recommend that you limit the overall migration amount to 75 percent of the overall SharePoint storage quota (including any extra storage you purchased separately).
- FastTrack migrates only to active OneDrive drives.

## Source environment details

Our data migration services migrate data from these source environments:

- File shares (SMB file shares on devices supporting SMB 2.0 onward).
- Single Google Workspace environment (Google Drive only).
- Box (Starter, Business, Enterprise).
- Dropbox for Teams (Standard and Advanced).

The following table presents migration details specific to each source environment:

 [Expand table](#)

Source environment	Type of migration	What migrates	What doesn't migrate
Any file share device supporting SMB 2.0 onward	Single or multi-pass	<ul style="list-style-type: none"> <li>• Documents.</li> <li>• File and folder structure.</li> <li>• User-level file and folder permissions.*</li> <li>• Group-level file and folder permissions.*</li> <li>• Files under 250 GB.</li> <li>• Basic document and folder metadata: <ul style="list-style-type: none"> <li>◦ Created date.</li> <li>◦ Modified date.</li> <li>◦ Created by.</li> <li>◦ Last modified by.</li> </ul> </li> </ul> <p>*Directory synchronization configuration required. Only NTFS permissions exposed to the Windows File Explorer are migrated. Permissions managed directly on file share devices aren't migrated. If data is stored on an SMB 2.0 device, the NTFS-equivalent permissions exposed by the SMB protocol are migrated.</p>	<ul style="list-style-type: none"> <li>• Ownership history and previous versions.</li> <li>• Conversion of embedded URLs in content.</li> <li>• Previous versions.</li> <li>• Windows file and folder attributes (like read-only and hidden).</li> <li>• Non-Windows New Technology File System (NTFS) and NTFS advanced permissions and special settings:</li> <li>• Explicit deny permissions (removed after migration, content subject to parallel permissions or permissions on parent folder).</li> <li>• NTFS auditing configuration.</li> <li>• More file metadata provided by File Classification Infrastructure (FCI).</li> <li>• Inaccessible or corrupted documents.</li> <li>• Hidden shares.</li> <li>• Sharing (like permissions granted on the share level).</li> <li>• Files or folders exceeding current <a href="#">SharePoint restrictions and limitations</a> <a href="#">↗</a>.</li> </ul>
Single Google Workspace environment (Google Drive only)	Single or multi-pass	<ul style="list-style-type: none"> <li>• Google Docs, Sheets, and Slides (files are converted to the equivalent Office format including files over 10 MB).</li> <li>• File and folder structure.</li> <li>• User-level folder permissions.</li> <li>• Group-level folder permissions.</li> </ul>	<ul style="list-style-type: none"> <li>• Ownership history, previous versions, and comments.</li> <li>• File and folder descriptions, folder colors.</li> <li>• Advanced metadata.</li> <li>• Google Forms.</li> <li>• File lock attributes.</li> <li>• Conversion of embedded URLs in content.</li> </ul>



Source environment	Type of migration	What migrates	What doesn't migrate
		<ul style="list-style-type: none"> <li>• User-level file permissions.</li> <li>• Group-level file permissions.</li> <li>• Files under 15 GB.</li> <li>• Basic document and folder metadata: <ul style="list-style-type: none"> <li>◦ Created date.</li> <li>◦ Modified date.</li> <li>◦ Created by.</li> <li>◦ Last modified by.</li> </ul> </li> <li>• Shared drives (folders and files).</li> <li>• Shared content owned by the Google Drive account being migrated.</li> <li>• Google Sheets are converted to Excel files, but custom scripts, formulas, and macros <b>aren't</b> migrated.</li> </ul>	<ul style="list-style-type: none"> <li>• Trashed items.</li> <li>• Inaccessible or corrupted documents.</li> <li>• Blocked or inactive users.</li> <li>• Google Photos, Maps, and other connected apps.</li> <li>• Google Drawings.</li> <li>• Shared content external to your organization.</li> <li>• Content not owned by the Google Drive account being migrated.</li> <li>• Permissions and basic metadata of guests. (<b>Note:</b> Use Google Drive Admin reports to identify content shared with guests. Instruct end users to reshare content with guests after migration.)</li> <li>• Shared drive membership permissions. (<b>Note:</b> Use Google Drive Admin reports to identify shared drive memberships. Instruct end users to configure these membership settings on the target before migration.)</li> <li>• Files or folders exceeding current <a href="#">SharePoint restrictions and limitations</a> <sup>↗</sup>.</li> <li>• Google Shortcuts.</li> </ul>
Box (Starter, Business, Enterprise)	Single or multi-pass	<ul style="list-style-type: none"> <li>• Documents.</li> <li>• File and folder structure.</li> <li>• User-level folder permissions.</li> <li>• Group-level folder permissions.</li> <li>• User-level file permissions.</li> <li>• Group-level file permissions.</li> </ul>	<ul style="list-style-type: none"> <li>• Ownership history, previous versions, and comments.</li> <li>• File and folder descriptions.</li> <li>• Box Tags and advanced metadata.</li> <li>• File lock attributes.</li> <li>• Conversion of embedded URLs in content.</li> </ul>

Source environment	Type of migration	What migrates	What doesn't migrate
		<ul style="list-style-type: none"> <li>Files under 15 GB.</li> <li>Basic document and folder metadata: <ul style="list-style-type: none"> <li>Created date.</li> <li>Modified date.</li> <li>Created by.</li> <li>Last modified by.</li> </ul> </li> <li>Shared content owned by the Box account being migrated.</li> </ul>	<ul style="list-style-type: none"> <li>Trashed items.</li> <li>Inaccessible or corrupted documents.</li> <li>Blocked or inactive users.</li> <li>Box Apps, Bookmarks, Favorites, and Workflows.</li> <li>Content not owned by the migrated Box account.</li> <li>Permissions and basic metadata of guests. (<b>Note:</b> Use Box reports to identify content shared with guests. Instruct end users to reshare content with guests after migration.)</li> <li>Files or folders exceeding current <a href="#">SharePoint restrictions and limitations</a> .</li> </ul>
Dropbox for Teams (Standard and Advanced)	Single or multi-pass	<ul style="list-style-type: none"> <li>Documents.</li> <li>File and folder structure.</li> <li>User-level folder permissions.</li> <li>Group-level folder permissions.</li> <li>User-level file permissions.</li> <li>Group-level file permissions.</li> <li>Files under 15 GB.</li> <li>Basic document and folder metadata: <ul style="list-style-type: none"> <li>Created date.</li> <li>Modified date.</li> <li>Created by.</li> <li>Last modified by.</li> </ul> </li> <li>Shared team folders and content.</li> <li>Shared content owned by the Dropbox accounts being migrated.</li> </ul>	<ul style="list-style-type: none"> <li>Ownership history, previous versions, and comments.</li> <li>File and folder descriptions.</li> <li>Advanced metadata.</li> <li>File lock attributes.</li> <li>Conversion of embedded URLs in content.</li> <li>Trashed items.</li> <li>Inaccessible or corrupted documents.</li> <li>Unmounted Dropbox folders.</li> <li>Deleted or disconnected users.</li> <li>Dropbox Paper, Showcases, and Spaces.</li> <li>Dropbox Apps and Favorites (Pins/Stars).</li> <li>Content not owned by the migrated Dropbox account.</li> <li>Permissions and basic metadata of guests. (<b>Note:</b> Use Dropbox reports to</li> </ul>

Source environment	Type of migration	What migrates	What doesn't migrate
			<p>identify content shared with guests. Instruct end users to reshare content with guests after migration.)</p> <ul style="list-style-type: none"> <li>Files or folders exceeding current <a href="#">SharePoint restrictions and limitations</a> <a href="#">↗</a>.</li> </ul>

## FastTrack responsibilities for OneDrive migrations

Our FastTrack Specialists perform standard activities during the migration project. Refer to the data migration responsibilities information in [SharePoint and OneDrive](#) for details.

### Your responsibilities

You perform standard activities during the migration project. Refer to the data migration responsibilities information in [SharePoint and OneDrive](#) for details.

You also perform the following activities, specific to OneDrive migrations:

- Provision all OneDrive sites that are targeted by your migration events.

## Migration to Microsoft Teams and Microsoft 365 Groups

When you choose to use FastTrack to migrate your files to Microsoft Teams and Microsoft 365 Groups, we provide migration guidance and data migration services. We provide guidance to help you plan your migration, configure your source environments and Teams and Microsoft 365 Groups, and use our data migration services to migrate your files. You create and schedule your migration events. We launch migration events in accordance with your schedule, monitor their progress, and provide status reports.

When your migration events are completed, you can expect files from appropriately scheduled and eligible sources of your migrated source environments to Teams and Microsoft 365 Groups. Teams channels and Microsoft 365 Groups must be pre-provisioned by the customer before they can migrate data into these destination types.

Teams and Microsoft 365 Groups impacts your permissions on the file destination location. Teams and Microsoft 365 Groups are built to allow collaboration. The Teams channel or Microsoft 365 groups determine who has access to those files when migrating into those destinations. FastTrack doesn't add end users or groups to any Teams channel or Microsoft 365 Groups permission during migration.

## Considerations


- All migrations are subject to SharePoint quotas. Refer to [SharePoint limits](#) for details.
- We recommend that you limit the overall migration amount to 75 percent of the overall SharePoint storage quota (including any extra storage you purchased separately).

## Source environment details

Our data migration services migrate data from these source environments:

- File shares (Server Message Block (SMB) file shares on devices supporting SMB 2.0 onward).
- A single Google Workspace environment (Google Drive only).
- Box (Starter, Business, Enterprise).
- Dropbox for Teams (Standard and Advanced).

The following table presents migration details specific to each source environment:

 Expand table

Source environment	Type of migration	What migrates	What doesn't migrate
Any file share device supporting SMB 2.0 onward	Single or multi-pass	<ul style="list-style-type: none"><li>• Documents.</li><li>• File and folder structure.</li><li>• User-level file and folder permissions.*</li><li>• Group-level file and folder permissions.*</li><li>• Files under 250 GB.</li><li>• Basic document and folder metadata:<ul style="list-style-type: none"><li>◦ Created date.</li><li>◦ Modified date.</li><li>◦ Created by.</li><li>◦ Last modified by.</li></ul></li></ul>	<ul style="list-style-type: none"><li>• Ownership history and previous versions.</li><li>• Conversion of embedded URLs in content.</li><li>• Previous versions.</li><li>• Windows file and folder attributes (like read-only and hidden).</li><li>• Non-Windows New Technology File System (NTFS) and NTFS</li></ul>

Source environment	Type of migration	What migrates	What doesn't migrate
		<p>*Directory synchronization configuration required. Only NTFS permissions exposed to the Windows File Explorer are migrated. Permissions managed directly on file share devices aren't migrated. If data is stored on an SMB 2.0 device, the NTFS-equivalent permissions exposed by the SMB protocol are migrated. Permissions are impacted by the Microsoft 365 Group and/or Microsoft Teams channel. If the destination is a Microsoft 365 Group or Microsoft Teams channel, the group or channel determines the final permissions profile on migrated files. We recommend not migrating permissions on files migrating to a Microsoft 365 Group or Microsoft Teams channel.</p>	<p>advanced permissions and special settings:</p> <ul style="list-style-type: none"> <li>• Explicit deny permissions (removed after migration, content subject to parallel permissions or permissions on parent folder).</li> <li>• NTFS auditing configuration.</li> <li>• More file metadata provided by File Classification Infrastructure (FCI).</li> <li>• Inaccessible or corrupted documents.</li> <li>• Hidden shares.</li> <li>• Sharing (like permissions granted on the share level).</li> <li>• Files or folders exceeding current <a href="#">SharePoint restrictions and limitations</a> <a href="#">↗</a>.</li> </ul>
Single Google Workspace environment (Google Drive only)	Single or multi-pass	<ul style="list-style-type: none"> <li>• Google Docs, Sheets, and Slides (files are converted to the equivalent Office format including files over 10 MB).</li> <li>• File and folder structure.</li> <li>• User-level folder permissions.*</li> <li>• Group-level folder permissions.*</li> <li>• User-level file permissions.</li> <li>• Group-level file permissions.</li> <li>• Files under 15 GB.</li> <li>• Basic document and folder metadata: <ul style="list-style-type: none"> <li>◦ Created date.</li> <li>◦ Modified date.</li> <li>◦ Created by.</li> <li>◦ Last modified by.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Ownership history, previous versions, and comments.</li> <li>• File and folder descriptions and folder colors.</li> <li>• Advanced metadata.</li> <li>• Google Forms.</li> <li>• File lock attributes.</li> <li>• Conversion of embedded URLs in content.</li> <li>• Trashed items.</li> <li>• Inaccessible or corrupted documents.</li> <li>• Blocked or inactive users.</li> <li>• Google Photos, Maps, and other connected</li> </ul>

Source environment	Type of migration	What migrates	What doesn't migrate
		<ul style="list-style-type: none"> <li>Shared drives (folders and files).</li> <li>Shared content owned by the Google Drive account being migrated.</li> <li>Google Sheets are converted to Excel files, but custom scripts, formulas, and macros <b>aren't</b> migrated.</li> </ul> <p>*Permissions are impacted by the Microsoft 365 Group and/or Microsoft Teams channel. If the destination is a Microsoft 365 Group or Microsoft Teams channel, the group or channel determines the final permissions profile on migrated files. We recommend not migrating permissions on files migrating to a Microsoft 365 Group or Microsoft Teams channel.</p>	<p>apps.</p> <ul style="list-style-type: none"> <li>Google Drawings.</li> <li>Shared content external to your organization.</li> <li>Content not owned by the Google Drive account being migrated.</li> <li>Permissions and basic metadata of guests. (<b>Note:</b> Use Google Drive Admin reports to identify content shared with guests. Instruct end users to reshare content with guests after migration.)</li> <li>Shared drive membership permissions (<b>Note:</b> Use Google Drive Admin reports to identify shared drive memberships. Instruct end users to configure these membership settings on the target before migration.)</li> <li>Files or folders exceeding current <a href="#">SharePoint restrictions and limitations</a> <a href="#">↗</a>.</li> <li>Google Shortcuts.</li> </ul>
Box (Starter, Business, Enterprise)	Single or multi-pass	<ul style="list-style-type: none"> <li>Documents.</li> <li>File and folder structure.</li> <li>User-level folder permissions.*</li> <li>Group-level folder permissions.*</li> <li>User-level file permissions.</li> <li>Group-level file permissions.</li> <li>Files under 15 GB.</li> </ul>	<ul style="list-style-type: none"> <li>Ownership history, previous versions, and comments.</li> <li>File and folder descriptions.</li> <li>Box Tags and advanced metadata.</li> <li>File lock attributes.</li> <li>Conversion of embedded URLs in</li> </ul>

Source environment	Type of migration	What migrates	What doesn't migrate
		<ul style="list-style-type: none"> <li>Basic document and folder metadata: <ul style="list-style-type: none"> <li>Created date.</li> <li>Modified date.</li> <li>Created by.</li> <li>Last modified by.</li> </ul> </li> <li>Shared content owned by the Box account being migrated.</li> <li>Box Notes (converted to Word document format).</li> </ul> <p>*Permissions are impacted by the Microsoft 365 Group and/or Microsoft Teams channel. If the destination is a Microsoft 365 Group or Microsoft Teams channel, the group or channel determines the final permissions profile on migrated files. We recommend not migrating permissions on files migrating to a Microsoft 365 Group or Microsoft Teams channel.</p>	<p>content.</p> <ul style="list-style-type: none"> <li>Trashed items.</li> <li>Inaccessible or corrupted documents.</li> <li>Blocked or inactive users.</li> <li>Box Apps, Bookmarks, Favorites, and Workflows.</li> <li>Content not owned by the migrated Box account.</li> <li>Permissions and basic metadata of guests. (<b>Note:</b> Use Box reports to identify content shared with guests. Instruct end users to reshare content with guests after migration.)</li> <li>Files or folders exceeding current <a href="#">SharePoint restrictions and limitations</a> <a href="#">↗</a>.</li> </ul>
Dropbox for Teams (Standard and Advanced)	Single or multi-pass	<ul style="list-style-type: none"> <li>Documents.</li> <li>File and folder structure.</li> <li>User-level folder permissions.*</li> <li>Group-level folder permissions.*</li> <li>User-level file permissions.</li> <li>Group-level file permissions.</li> <li>Files under 15 GB.</li> <li>Basic document and folder metadata: <ul style="list-style-type: none"> <li>Created date.</li> <li>Modified date.</li> <li>Created by.</li> <li>Last modified by.</li> </ul> </li> <li>Shared team folders and content.</li> <li>Shared content owned by the Dropbox accounts being migrated.</li> </ul>	<ul style="list-style-type: none"> <li>Ownership history, previous versions, and comments.</li> <li>File and folder descriptions.</li> <li>Advanced metadata.</li> <li>File lock attributes.</li> <li>Conversion of embedded URLs in content.</li> <li>Trashed items.</li> <li>Inaccessible or corrupted documents.</li> <li>Unmounted Dropbox folders.</li> <li>Deleted or disconnected users.</li> <li>Dropbox Paper, Showcases, and Spaces.</li> </ul>

Source environment	Type of migration	What migrates	What doesn't migrate
		<p>*Permissions are impacted by the Microsoft 365 Group and/or Microsoft Teams channel. If the destination is a Microsoft 365 Group or Microsoft Teams channel, the group or channel determines the final permissions profile on migrated files. We recommend not migrating permissions on files migrating to a Microsoft 365 Group or Microsoft Teams channel.</p>	<ul style="list-style-type: none"> <li>• Dropbox Apps and Favorites (Pins/Stars).</li> <li>• Content not owned by the migrated Dropbox account.</li> <li>• Permissions and basic metadata of guests. (<b>Note:</b> Use Dropbox reports to identify content shared with guests. Instruct end users to reshare content with guests after migration.)</li> <li>• Files or folders exceeding current <a href="#">SharePoint restrictions and limitations</a> <a href="#">↗</a>.</li> </ul>

## FastTrack responsibilities for Microsoft Teams and Microsoft 365 Groups migrations

Our FastTrack Specialists perform standard activities during the migration project. Refer to the data migration responsibilities information in [Microsoft Teams](#) for details.

### Your responsibilities

You perform standard activities during the migration project. Refer to the data migration responsibilities information in [Microsoft Teams](#) for details. You also perform the following activities, specific to Microsoft Teams and Microsoft 365 Groups migrations:

- Provision all Microsoft Teams channels and Microsoft 365 Groups as targeted by your migration events.

#### ⓘ Note

FastTrack doesn't pre-provision Microsoft Teams channels or Microsoft 365 Groups. FastTrack doesn't add end users or groups to Microsoft Teams channels or Microsoft 365 Groups. You must add your end users or groups to all Microsoft



Teams channels and Microsoft 365 Groups before you migrate data into those destinations so those end users have access to those newly migrated documents

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) 

# Cross-Tenant Migration

Article • 10/30/2024

Cross-tenant migration is the process of migrating workloads from one Microsoft 365 tenancy to another. This process can involve the migration of one or many workloads (including Exchange Online, SharePoint, and OneDrive).

Cross-tenant migrations are normally part of customers considering Mergers, Acquisition and Divestitures (MAD). Beginning in late 2024, FastTrack offers a private preview for cross-tenant migration services to customers migrating Exchange Online, SharePoint and OneDrive.

## ⓘ Note

This service is done on an invitation-only basis and requires a minimum licencing purchase of 500 licenses. A Cross-Tenant User Data Migration SKU is required in order to qualify for the FastTrack cross tenant migration service.

## ⓘ Note

The following products and features aren't supported for this service: Microsoft Teams, Microsoft 365 Groups, Microsoft Planner, Skype, Microsoft Stream, Microsoft Flow, Power Apps, device management, and client configuration.

## Considerations

- We require appropriate access and permissions to your source environments and Microsoft 365 tenant to provide data migration services.
- Our data migration services aren't designed or intended for data subject to special legal or regulatory requirements.

## ⓘ Note

US Government and Education (EDU) customers aren't currently supported.

- We can't guarantee the speed of mail or file migrations.

- Unforeseen issues (like unreadable or corrupt items in the source environment) may prevent our ability to migrate some of your data items.
- External factors beyond our control can result in changes to, delays in, or suspension of our data migration services.

## Migration service availability

**For Commercial customers:** We provide data migration services 24 hours a day, seven (7) days a week (24x7) (English only).

## Migration to Exchange Online

When you choose to use FastTrack to migrate your email from source tenant to target tenant, we provide migration guidance and data migration services. We provide guidance to help you plan your migration, configure your source and target tenant, and use our data migration services to migrate your mailboxes. You create and schedule your migration events. We launch migration events in accordance with your schedule, monitor their progress, and provide status reports. When your migration events are complete, you can expect mail from appropriately scheduled and eligible source mailboxes of your source tenant to have been moved to your target tenant.

## Considerations

- Before migration, you must complete FastTrack core onboarding for Exchange Online.
  - If you performed onboarding yourself, you must pass the required checks and prerequisites Refer to [Exchange Online](#) for details.
- FastTrack migrates only to active Office 365 mailboxes.
- Distribution lists (*MailEnabledGroup* objects) and external contacts (*MailEnabledContact* objects) that exist in your source tenant aren't a part of mailbox data migration. You must pre-create them in the target tenant before the migration.

## Migration details

The following table presents **Exchange Online** tenant-to-tenant migration details:

What migrates	What doesn't migrate
<ul style="list-style-type: none"> <li>• Emails.</li> <li>• Exchange Online server-side mailbox rules.</li> <li>• Exchange Online server-side stored contacts.</li> <li>• Delegate permissions (if both migrated).</li> <li>• Calendar.</li> <li>• Tasks.</li> <li>• Archived mailbox migrated with the user's mailbox.</li> <li>• Recoverable items.</li> <li>• Conference rooms and Equipment mailboxes.</li> <li>• Microsoft rights-managed emails.</li> <li>• Microsoft encrypted emails.</li> </ul>	<ul style="list-style-type: none"> <li>• Public folders.</li> <li>• Any email that exceeds the message size limit.</li> <li>• Journaling archive or any third-party archive solution.</li> <li>• Corrupted items.</li> <li>• Client-side mailbox rules.</li> <li>• Teams messages.</li> <li>• Mailboxes with any kind of hold applied.</li> <li>• Mailboxes with more than 12 auxiliary archives</li> <li>• Outlook profiles.</li> <li>• Microsoft Entra ID permissions.</li> <li>• Send-as emails.</li> <li>• Send-on-behalf emails.</li> <li>• Auto-mapping profiles used for full-access permissions.</li> </ul>

The migration results might be unreadable depending on the source encryption. We recommend the encryption be removed before migration to ensure the readability in the target. For more information, see [Mergers and Spinoffs](#).

## FastTrack responsibilities for Exchange Online migrations

Our FastTrack Specialists perform standard activities during the migration project. Refer to the data migration responsibilities information in [Exchange Online](#) for details.

Our FastTrack Specialists also perform the following activities specific to Exchange Online migrations:

- Provide guidance to help you enable SMTP mail routing coexistence between your source and target tenant if applicable.

## Your responsibilities

You perform standard activities during the migration project. Refer to the data migration responsibilities information in [Exchange Online](#) for details.

You also perform the following activities, specific to Exchange Online migrations:

- Complete FastTrack core onboarding for Exchange Online. If you performed onboarding yourself, you must pass the required checks and prerequisites. Refer to

[Exchange Online](#) for details.

- Install the appropriate level of client software as per Office 365 guidelines.
- Migrate client-side data if desired. This data includes, but isn't limited to, local address books, data in local Outlook Data Files (PSTs), Outlook rules, and local Outlook settings.
- Assist your end-users with remediation of client-side migration issues.

## Migration to SharePoint and OneDrive

When you choose to use FastTrack to migrate SharePoint and OneDrive sites from tenant-to-tenant, we provide migration guidance and data migration services. We provide guidance to help you plan your migration, configure your source and target tenants, and use our data migration services to migrate your data. We launch migration events in accordance with your schedule, monitor their progress, and provide status reports. When your migration events are complete, you can expect files from your source tenant to have been moved to your target tenant.

### Considerations

- All migrations are subject to SharePoint quotas. Refer to [SharePoint limits](#) for details.
- We recommend that you limit the overall amount of migrated to 75 percent (%) of the overall SharePoint storage quota to which you're entitled (including the extra storage you may have purchased separately).
- FastTrack migrates only to active OneDrive sites.

### Migration details

The following table presents **Sharepoint** tenant-to-tenant migration details.

 **Expand table**

What migrates	What doesn't migrate
<ul style="list-style-type: none"><li>• Microsoft 365 group-connected sites, including those sites associated with Microsoft Teams.</li></ul>	<ul style="list-style-type: none"><li>• SharePoint sites with over five (5) TB of content or one (1) million items in total.</li><li>• Inaccessible or corrupted documents.</li></ul>

What migrates	What doesn't migrate
<ul style="list-style-type: none"> <li>• Modern sites without a Microsoft 365 group association.</li> <li>• Classic SharePoint sites.</li> <li>• Communication sites.</li> <li>• Documents.</li> <li>• File and folder structure.</li> <li>• User-level file and folder permissions.</li> <li>• Group-level file and folder permissions.</li> <li>• Sharing links.</li> <li>• Ownership history and previous versions.</li> <li>• Basic document and folder metadata: <ul style="list-style-type: none"> <li>◦ Created date.</li> <li>◦ Modified date.</li> <li>◦ Created by.</li> <li>◦ Last modified by.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Path limits exceeding 400 characters.</li> <li>• SharePoint workflows.</li> <li>• Apps.</li> <li>• Power Apps and automation tasks.</li> </ul>

The following table presents **OneDrive** tenant-to-tenant migration details:

 Expand table

What migrates	What doesn't migrate
<ul style="list-style-type: none"> <li>• Documents.</li> <li>• File and folder structure.</li> <li>• User-level file and folder permissions.</li> <li>• Group-level file and folder permissions.</li> <li>• Sharing links.</li> <li>• Ownership history and previous versions.</li> <li>• Basic document and folder metadata: <ul style="list-style-type: none"> <li>◦ Created date.</li> <li>◦ Modified date.</li> <li>◦ Created by.</li> <li>◦ Last modified by.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Inaccessible or corrupted documents.</li> <li>• OneDrive accounts on legal hold.</li> <li>• OneDrive accounts with over 5 TB of content or one (1) million items in total.</li> <li>• Path limits exceeding 400 characters.</li> </ul>

## FastTrack responsibilities for SharePoint tenant-to-tenant migrations

Our FastTrack Specialists perform standard activities during the migration project. Refer to the data migration responsibilities information in [SharePoint and OneDrive](#) for details.

# Your responsibilities

You perform standard activities during the migration project. Refer to the data migration responsibilities information in [SharePoint and OneDrive](#) for details.

Other activities include:

## For SharePoint tenant-to-tenant migrations

- [Pre-create users, groups, and Microsoft 365 groups on the target tenant.](#)
- [Pre-create Microsoft 365 groups connect to SharePoint sites.](#)
- [Step 5: Identity mapping \(preview\).](#)

## For OneDrive tenant-to-tenant migrations

- [Pre-create users, groups, and Microsoft 365 groups on the target tenant.](#)
- [Create the identity mapping file.](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) 

# Appendix A - FastTrack Center HIPAA Business Associate Agreement

Article • 09/18/2023

If you have a HIPAA Business Associate Agreement (BAA) agreed with Microsoft, all services listed in [Office 365](#) are performed in accordance with that BAA.